# Legal and Ethical issues in Curbing Cybercrime in Nigeria

By

**Ojuawo, O.O[1]& Abibu, A.A[2]**

[1]Department of Computer Science, The Federal Polytechnic, Ilaro
[2]Department of General Studies, The Federal Polytechnic, Ilaro

PRESENTED AT
THE 13TH NATIONAL CONFERENCE,
ACADEMIC STAFF UNION OF POLYTECHNICS (ASUP)
VENUE: HOSPITALITY MANAGEMENT HALL, SCHOOL OF TECHNOLOGY ANNEX,
KANO STATE POLYTECHNIC, KANO.
DATE: MONDAY 7TH – THURSDAY 10TH, NOVEMBER 2016.

## Abstract

*The Internet is one of the fastest-growing areas of technical infrastructure development. Over the past decades, the growth of the internet and its use afforded everyone this opportunity. The internet makes boundless open doors for business, social, and educational activities. Internet has been an instrument in aiding crimes ranging from bank fraud, unauthorized access to confidential information, sabotage of data in computer networks of some organizations. Cybercrime occurs by the use of computer and internet by attackers to commit crime. Types of cybercrime are identified as spamming, cyber terrorism, cyber stalking, and identity theft amongst others. With Nigeria approaching a cashless society, cybercrime should be minimized, if not eradicated. In preventing cybercrime, citizens as well as police are required to be involved. The police force lack specialists in its investigating unit to deal with cybercrime. This paper discusses about the different types of cybercrime, review of cybercrime laws, the challenges in enforcing cybercrime laws in Nigeria and the legal framework for enforcing cybercrime laws that provide an effective, unified, regulatory and institutional framework for the comprehensive, legal, prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria*.

**Keywords:** *Cybercrime, internet, laws, attackers, Cyber ethics.*

## 1.0 Introduction

In the society of today, the word Cybercrime is one of the words popularly used by individuals. Cybercrime can also be tagged as computer crime which can beexplained as a criminal activity which involves the use of information technology facilities to have illegal access or unauthorized access, illegal interception that involves technical means of non-public transmissions of computer data to, from or within a computer system (Ehimen, O, R&Bola, A, 2010). Most times it is being described as the means of using computer system to perpetrate fraud. This has affected a lot of people in Nigeria in many ways, ranging from the misuse of devices, forgery or identity theft, electronic fraud, manipulating data on the computer system. The advent of digital technology brought forth cutting edge correspondence web access, hardware and intense PC frameworks for data processing.

The cyberspace has been a platform for the internet, which has made geometric development and opened the windows of opportunities for organizations in the aspect of businesses and the expulsion of monetary hindrances up to this point confronted by countries of the world. Individuals from different background and regions can now unreservedly get to and use the focal points offered by the internet platform.

A very few criminally minded youths in the country, who are mostly not educated or graduates, are stealing and committing atrocities through the aid of the internet online business transactions. The web online business administrations, which conventionally expected to be a blessing as it opens one to a considerable measure of chances in a different field of life is quickly turning into a wellspring of distress and stress because of the atrocities being executed through it. Cybercrime has come as an astound and an odd marvel that until further notice lives with us in Nigeria. Computer crimes incorporate a wide scope of conceivably unlawful exercises.

In general, cybercrime are grouped into two major categories. The first category are crimes thattarget computer networks or devices directly while the second group are crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device. According to the Guardian (2008), Nigeria was as of late recognized as the pure and unmindful passive player in the internet learning Olympiad. The safety of Nigeria's national cyberspace was in doubt when the Al Quaeda used Nigeria websites and email systems to broadcast information. In Nigeria, the most common name for cyber criminals is "yahoo boys". This category of internet fraud stars has caused so many havoc in the society and dented the image of the country.

The country is yet to put in place proper mechanism in controlling activities of internet fraud stars and has cut down the country's economy especially in the online stock exchange market trading of Nigeria. Without legitimate security strategies set up, it is much the same as building a house without locks. Any individual can get entrance. The class and nature of cybercrime in Nigeria is unending. Cybercrime is a worldwide exceptional that is undermining the economy of countries.

This paper discusses about the different types of cybercrime, types of cybercrime laws, investigation of critical review of cybercrime laws, the challenges of enforcing cybercrime laws in Nigeria and a legal framework in enforcing cybercrime laws in Nigeria.

## 2.0 Cybercrime

According to Halder, D& Jaishanker, K (2011), Cybercrimes are offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards

and groups) and mobile phones.Cybercrime can be defined as an act committed or omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction (Saini, H., Rao, Y. S & Panda, T, 2012).

Cybercrime has been an evading variable in the cyberspace transactions in Nigeria, where cybercrimes and PC related crimes are endemic. The mix of computer technology as a global issue, the economy of most countries in the world is open using Information communication and technology and at stake (Sauwala, M. A& Abubakar, M, 2004).

Cybercrime in a narrow sense (computer crime) covers any illegal behavior directed by means of electronic operations that target the security of computer systems and the data processed by them. Cybercrime in a broader sense (computer-related crimes) covers any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network (Gercke, M, 2009).

In Nigeria, individuals, ranging from the young to the old, perform cybercrimes, however, in most instances the youths. So many youths engage in cybercrime with the aim of emerging as the best hacker or as a profit making venture since the tools for hacking in our modern world has become affordable by many (Hassan et. al, 2012). In quest of Nigeria battle against cybercrimes, efforts put in placeare directed through the sources and channel which cybercrimes perpetrates.InNigeria are generally targeted at individuals and via the computer systems, hence less technical expertise on the part of the criminals is required(Sauwala, M.A& Abubakar, M, 2004).

As of late, a report demonstrated that Nigeria is losing about $ 80 million dollars yearly to software piracy. This report was the finding of a study led by Institute of Digital Communication, is a market research situated in South Africa. Additionally, the American National Fraud Information Center (ANFIC) reported Nigerian cash offers as the fastest online scam, up to 90 % in 2001. ANFICalso positioned Nigeria cybercrime impact per capita as being outstandingly high. Email scams and spam are the most horrendous wonders among the cybercrime, these are ways used to display false money related investments. Nigeria's image is being referred to and has been dented as a consequence of her nationals' inclusion in the cybercrime. The internet fraud stars send an email that the victim is the named recipient to a will of alienated relative and stands to profit the bequest. In some cases, they utilized online philanthropy; the culprits send an email to the victims, soliciting for funds and help to charitable organizations that don't exist.

## 3.0 Types of Cybercrime

An attack to carry out a Cyber Crime can be called as a Cyber Attack. With regards to the Internet, it certain to obtain some malware, if a user visits malicious websites without proper protection. An antivirus and a firewall is required. Additionally, the user need to stay clear and avoid distinctive sorts of cybercriminals attempting to make profit at any cost. The following are different types of cybercrimes.

### 3.1 Fraud - Identity theft

Identity theft and fraud is one of the most common types of cybercrime. Fraud can be described as a criminal activity in which someone puts on a show to be some individual with the aim to get

some vital information about someone (Hassan, A. B, Funmi, D. L & Makinde, J, 2012). When this is done online on the Internet, it is called Online Identity Theft. For instance, making a false bank website page to get the account details of an individual. This is an easy concept;somebody gain access your personal information and utilizes it for his own advantage. This could go from a black-hat hacker stealing online banking account login and password to accessing ATM and utilizing such individuals can make themselves a great deal of cash with individual information. In Nigeria, criminals design web link forms requesting users to fill in their personal information which includes, unique details like pin numbers and passwordsso as to use it to commit crimes. The most common source to steal identity information of others, are data breaches affecting government or federal websites. It can be data breaches of private websites too, that contain important information such as – credit card information, address, email ID's, etc.

### 3.2 Ransomware

This is one of the terrible malware-based assaults. Ransomware enters your PC network and encrypts your documents utilizing public key encryption, and unlike other malware, this encryption key stays on the hacker's server. Attacked clients are then requested to pay huge ransoms to get this private key.This is a PC malware that installs secretly on a victim's PC, executes a crypto virology attack that affects it, and requests a payoff installment to decrypt it or not publish it. Basic ransomware may lock the system in a way which is easy for a learned individual to switch, and show a message asking for payment to unlock it. Ransomware is an extortion scheme whereby attackers hijack and encrypt the victim's computer files and then demand a ransom from the victim for these files in original condition.

### 3.3 Distributed Denial of Service Attacks (DDoS attacks)

DDoS assaults are utilized to make an online service inaccessible and bring it down, by besieging or overpowering it with traffic from numerous locations and sources. Botnets are produced by planting malware on the victim's PCs. The motive is typically to attract victims for the DDOS attack, and permit the hacker to hack into a system. Another motive could be blackmail and extortion.

According to Simon, F. L& Rubin, S. H (2000), a denial of service attack is characterized by an explicit attempt by an attacker to prevent legitimate users of a service from using the desired resources and the distributed format adds the “many to one” dimension that makes these attacks more difficult to prevent.

### 3.4 Spamming and Phishing

Spamming and phishing are two extremely common types of cybercrimes. There is very little you can do to control them. Spam is essentially undesirable emails and messages that utilize Spambots while Phishing is a technique where cyber criminals offer a bait with the goal that you take it and give out the information they need.A spambot is a program designed to collect, or harvest, e-mail addresses from the Internet in order to build mailing lists for sending unsolicited e-mail, also known as spam. The bait can be in form of a business proposal, announcement of a lottery to which you never subscribed, or anything that promises you money for nothing or a small favor. Spamming and phishing messages are sent by random individuals whom you didn't ever know about. You ought to avoid any such offers particularly when you feel that the offer is too good. Do not get into any sort of agreements that guarantee something too good to be true. Most times, they are fake offers intending to get your information and to get your cash directly or indirectly.

According to Kratchman, S., Smith, J. L & Smith, M (2008), phishing occurs when the perpetrator sends fictitious emails to individuals with links to fraudulent websites that appear official and thereby cause the victim to release personal information to the perpetrator. Spam is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, television advertising and file sharing network spam (Hassan, A. B et al, 2012).

### 3.5 Social Engineering

The term 'social engineering' is found to have its underlying foundations from the early twentieth century political science field where it intended to speak to brilliant techniques that take care of the social issues. Because of the positive meanings of "engineering", it was appropriated for different social issues of the time (Ivaturi, K& Janczewski, L, 2011).Social engineering is a strategy where the cyber criminals contact you utilizing emails or telephones, generally the last mentioned. They attempt to gain your confidence and once they prevail at it, they get the information they require. This information can be about you, your cash, your organization where you work or anything that can bear some significance with the cyber criminals.

Basic information about individuals from the Internet is easy to discover. Utilizing this information as the base, the cyber criminals attempt to become a close acquaintance with the victim and once they succeed, they will vanish, leaving you prone to different financial injuries directly and indirectly. They can offer the information acquired from the victim or utilize it to

secure things like credits in the victim's name. It can also be in form of identity theft. Users should be extremely careful when dealing with strangers on phone or on the internet.

### 3.6 Cyber Terrorism

Cyber terrorism occurs when terrorists cause virtual destruction in online computer system (Kratchman, S. et al, 2008).A cyber terrorist can be portrayed as someone who dispatches assault on government or organization keeping in mind the end goal to contort and additionally access stored information stored on the computer and their networks. Wikipedia describes a cyber-terrorist as someone who intimidates the government or to propel his or her political or social goals by launching PC based attack against computers, networks, and the information stored on them.

### 3.6 Cyber Ethics

Cyber ethics entails the healthy and responsible use of the internet without compromising the safety and integrity of the information of other users. It promotes the positive and the good use of the cyberspace. Cybercrime is a deviation from the norm on the acceptable use of the computer

### 3.7 The Nature of Cybercrime

The world around us today with the help of information technology is now becoming a global community. Access to information is in real time at a click of a button. In spite of its immense benefit, it has however has produced new challenges as access to information is without borders (Fortinet, G.L, 2009). Safety of private information could be disrupted thereby creating security

risks of far reaching proportions. The social media and the transition of many businesses to the online platform has created a new meeting point with new opportunities, responsibilities and peculiar challenges**.** Unlike conventional crimes, which requires the physical presence in the locus of the crime before it can be consummated, the theatre of internet crime has been moved online. The anonymity created by the use of the internet has produced mutations in crimes due to the technicalities involved and makes it more difficult for law enforcement agents to trail.It does not usually leave a crime scene, unlike non electronic crimes, evidence of computer based crimes are track across many locations as cybercrime could be carried out from any part of the world. Almost all crimes with the exception of few e.g. rape could be done online. It therefore becomes imperative to create a robust legal framework that would address the problems.

## 4.0 Legal Frame work for Combating Cybercrime in Nigeria.

Prior to the enactment of the cybercrime law in Nigeria in 2015 the traditional legal framework for combating cybercrime includes: The Nigerian Criminal Code (1990) nowCap C38 LFN 2004,Advanced Fee Fraud and other Related Offences Act(1995) now 2006, Economic and Financial Crimes Commission Act Cap E1 LFN2004.

## 4.1 The Nigerian Criminal Code

The most famous provision of the criminal code is section 419 which criminalized the act of obtaining by false pretense and anyone found guilty is liable to 3 years imprisonment.Also notable are section 418 which defines fraud and section 421 which provides that anyone who obtains by fraud or trick from any other person anything that can be stolen is guilty of a misdemeanor and is liable to imprisonment for two years.Anyone who commits these offences through the use of computer would equally be liable.In the case of **Federal Republic of Nigeria**

V. **Chief Emmanuel & Ors**. The accused were charged under the Criminal Code and the Advance Free Fraud and Other Related Offences Act for defrauding Banco Noroeste S. A of Sao Paulo, Brazil. The employee of the company (Banco Noroeste ), Mr Nelson Sakaguchi was promised 40% of the contract sum. The victim was deceived into a meeting in London for the purported contract for the construction of the Abuja International Airport. The defendants also represented that they were acting on behalf of the Federal Government of Nigeria. The defendants demanded several sums from the victim as payment for taxes to the Nigerian Government. Over $ 190 Million was obtained from the victim due to repeated demands in the pretext that the contract sum had been increased thereby requiring additional payment of taxes.

### 4.2 Economic and Financial Crimes Commission Act

Due to the limited nature of the applicability of the criminal code and the increase in fraud the Economic and Financial Crimes Commission Act was enacted to addresseconomic crimes and has powers to investigate and prosecute same pursuant to section 6 of the Act. The commission is saddled with the following responsibilities:

i. The enforcement and the due administration of the provisions of the Act;
ii. The investigation of all economic crimes including advance fee fraud, money laundering, counterfeiting, illegal charge transfer, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, contract scam etc.
iii. The coordination and enforcement of all economic and financial crime laws and enforcement functions conferred on any other persons or authority.

Also, section 48offers an extensive meaning for the expression "Economic and financial crimes" to includenon-violent crimes and illicit activities committed with the motive of receiving moneyillicitlywhich ranges from fraud, narcotic drug trafficking, money laundering, embezzlement, bribery, looting and any form of corrupt practices, illegal arms dealing, smuggling, human trafficking and child labour, illegal oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of ceremony, theft of intellectual property and piracy, open market abuse etc. The above definition accommodates cybercrimes that constitute economic crimes. In an unreported case, **EFCC** V **Chime Larry Okonji suit No. Id/864/2007.** Where a 500 Level student defrauded an American to the tune of N 97 million. He was sentenced to 45 years for impersonating the Chairman of the EFCC.

### 4.3 The Evidence Act

The Evidence Act of 2011 is also noteworthy of mention, section 84 has introduced novel provision of the admissibility of electronically generated evidence. This provision has helped to redefine the law of Evidence in Nigeria.

### 4.4 The Cybercrimes Prohibition, Prevention Act 2015

The Act is divided into 8 parts and 59 sections. The Act which came into force on the 5$^{th}$of May 2015 is a long awaited legislation on cybercrime. It is the first dedicated Act to address the menace of cybercrime in Nigeria. The provisions of the Act are considered below:

### 4.5 Object and Application of the Act (Part 1)

Section 1 of the Act espouses the objective of the Act to provide a unified legal framework forthe prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. It also promotes the protection of critical national information infrastructure. The objective further encapsulates the protection of computer systems and networks, cyber security, data and computer programs, electronic communications, intellectual property and privacy rights.The Act contains copious provisions that prohibit and sanction cybercrime. What appears to be lacking are the necessary infrastructure to aid the detection and prevention of cyber and electronic crimes. For example, the permanent secretary in the Ministry of Information claimed to have shut down the illegal transmission of Biafra radio. The radio was used to for propagating falsehood and secessionist ideology.However, few days after the public statement, the radio transmission of the group persisted (Premium Times, 2015). Section 2 states that the Act applies throughout the Federal Republic of Nigeria.

### 4.6 Protection of Critical National Information Infrastructure (Part 2)

The combination of Sections 3 and 4 empowers the President upon the recommendation of the National Security Adviser vide an order published in the gazette to designate specific computer systems or network as critical to national information infrastructure.

### 4.7 Offences and Penalties (Part 3)

Section 5 to 35 states various offences under the Act and it also impose appropriate punishment for the offences. Section 5 sets the punishment for the persons who commit an offence against critical national information infrastructure. The person who commits this offence is liable to imprisonment of not more than 10 years and not more than 15 years without an option of fine

where the offence result into bodily harm, where the offence results into death, the offender shall be convicted to life imprisonment.

Section 6 punishes unlawful access to computer which is punishable for a term not more than 5 years or a fine not more than N 5,000,000.00. Where the intention is to access industrial or classified information, uses any device to avoid detection, the imprisonment shall not be less than 7 years or a fine not exceeding N 7,000,000.00 or to both. Anybody who traffics in password or similar information shall be liable to a fine not more than N 7,000,000.00 or a term not more than 3 years.

Section 7 makes it mandatory for the registration of every cybercafé and shall keep a register of user through a sign in register. Section 7(2) prohibit electronic fraud using cybercafé shall be guilty of an offence and sentenced to a term of 3 years or a fine N 1,000,000.00 or both.Where there is a connivance by owners of a cybercafé they shall be liable to a fine of N 2,000,000.00 or 3 years jail termor both.Section 8 criminalizes system interference to a term not more than 2 years or a fine not 5,000,000.00. Section 9 criminalizes the act of the destroying or intercepting electronic messages, emails and money transfer. Anyone found guilty of the offence shall be liable to a term of 7 years in the first instance and 14 years in the second instance. Section 10 prohibits tampering with critical infrastructure and section 11 punishes willful misdirection of electronic messages, the violation the sections attracts a punishment of a fine of N 2,000,000.00 or an imprisonment of 3 years and a term of 3 years or a fine of N 1,000,000.00 respectively.

Section 12 criminalizes acts of unlawful interception of non- public transmission data. Subsection (2) further sanctions anyone who by false pretence induces a government worker to deliver electronic message which are confidential. Subsection (3) sanctions anyone who hides or

detains electronic messages or mails or receives such message in error with the knowledge that he ought not to receive such message.

Section 13 and 14 prohibits all forms of computer related forgery and computer related fraud respectively. Theft of electronic devices is prohibited by section 15, it criminalises stealing of financial institutions or public infrastructure terminal and Automated Teller Machine. All acts of unauthorized modification of computer systems, network data and system interference is criminalized by section 16. Section 17 provides for electronic signature, and that all electronic signature in respect of purchases of goods and other transactions are binding. If anyone questions an electronic signature, the burden of proof is on the contender and not on the originator. Forgery of and electronic signature of another or a company's mandate is an offence punishable for 7 years or a fine of 10,000,000.00 section 17(1)(c). Section 17(2) excludes certain transactions or declarations from being valid by virtue of electronic signature, these documents includes; creation and execution of wills, codicils or other testamentary documents, death certificate, birth certificate, matters of marriage, divorce, adoption or related matters, issuance of court orders etc.

Section 18 criminalise cyber terrorism. Section 19 imposes the duty protects sensitive information on financial information. Section 19(3)imposes the responsibility on financial institutions to provide adequate counter fraud measures to protect customer's information. Section 20 states that any employee of a financial institution who issues fraudulent instructions would be liable to a term of 7 years.

Section 21 makes reporting cyber threats imperative and section 22 prohibits identity theft. Child pornography and related offences is prohibited by section 23. Section 24 also outlaws cyber stalking. Cybersquatting is prohibited by section 25. Section 26 and 27 criminalises racist, xenophobic offencesand attempts, conspiracy, aiding and abetting respectively. Section 28

criminalises the importation and fabrication of E- Tools for the purpose of committing an offence. Breach of confidence is an offence under the Act by virtue of section 29. Section 30 criminalises the manipulation of ATM machine or point of sale terminal. Section 31 makes it a responsibility of an employee to surrender codes or access rights after leaving the employment. Phishing and spamming, spreading of computer virus, or electronic card related fraud is criminalized by section 32 and 33 respectively.

Section 34, 35, 36 prohibits dealing in card of another, purchase or sale of card of another and use of fraudulent device attached to E-mails and Websites.

### 4.8 Duties of Financial Institutions/ Duties of Service Providers (Part 4)

Section 37 imposes a duty of financial institutions to verify the identity of its customers before issuing electronic cards while sections 38, 39 and 40places responsibility on service providers to retain and protect data, to intercept electronic communications by order of court, and duty to assist law enforcement agencies.

### 4.9 Administration and Enforcement (Part 5)

Section 41 gives the National Security Adviser charge over co-ordination ofenforcement agencies under the Act. It also creates the National Computer Emergency Response Team (CERT) in Nigeria. The Cybercrime Advisory Council was established by section 42. Section 43 stipulates the function and the powers of the council which includes the duty to advice of ways of preventing cybercrime and computer related offences. Subsection (1) (d)states that the council shall establish award grants to institution of higher learning to establish cyber security research

centers. Sub section (1) (e) also mandates graduate traineeship in cybersecurity, computer and network security research and development.

The provisions of the above sections are quite commendable, however the provision of section 43(1) (d) and (e) are yet to be implemented in Nigeria, it is instructive to say that the provisions of these sections are mandatory as the word 'shall' was used, therefore leaving the council with no option than to comply with the provisions of the Act.The cyberspace has been utilised for different types of criminal exploits. However, in recent times it has been used for espionage, terrorism and cyber warfare. The introduction of the Stuxnet worm (the world's first digital weapon) into the Iranian nuclear plant by the Israeli mossad in collaboration with the US is an example of state sponsored cyber warfare's made possible through the use of information technology (Available at https://en.wikipedia.org/wiki/Stuxnet accessed 15th October 2016).

Stuxnet, was a unique virus different from any other virus that existed before it. It was the first virus that manipulated operations of equipment, as opposed to recognised form of virus attacks. (Available at https://us.norton.com/stuxnet accessed 16 October 2016).It certain that without research, adequate knowledge and an unsecured cyberspace, Nigeria will remain helplessly vulnerable and an easy target for cyber espionage or cyberwar and other forms of cyberattacks.

Section 44 creates the National Cyber Security Fund which is a levy of 0.005 of all electronic transactions by the businesses specified in the second schedule of the Act, which must be deposited with the central bank by the affected businesses within 30 days. The businesses listed in the second schedule includes all telecommunications companies, Banks and other financial institutions, insurance companies, internet service providers and the Nigerian Stock Exchange.

Subsection (3) exempts the all funds accruing from income tax. The National Security Adviser is empowered to keep a record of accounts in respect of the fund.

### 4.10 Arrest, Search, Seizure and Prosecution (Part 6)

Section 45 provides that law enforcements agents may apply exparte to a Judge for the purpose of issuing a warrant in order to obtain electronic evidence, it also give law enforcements agent the power to arrest, search, seize and remove evidence which shows the commission of an offence under the Act. The obstruction of a law enforcement and refusal to release or comply with instructions is an offence contrary to section 46. Law enforcement agencies have power to prosecute offences under this Act save for offences committed under section 19 and 21 which requires the approval of the Attorney General before the commencement of prosecution. Section 48 gives the court the discretionary power to order forfeiture of assets, money of property traceable to the proceed of an offence under the Act. Where a convicted person under this Act has a property abroad, such properties subject to treaties be forfeited to the Federal Government of Nigeria. The court is also empowered to order restitution section 49.

### 4.11 Jurisdiction and International Co-operation (Part 7)

The Federal High Court is vested with the jurisdiction to try offences under the Act. The offences under the Act is extraditable under the Extradition Act, Cap E 25 Laws of the Federation of Nigeria, 2004. Section 52 give the Attorney General the power to collaborate with other nations in the investigation, detection, prevention and assist in the prosecution of offences under the Act. Evidences acquired pursuant to request in the investigation or proceeding of a foreign court, if verified can be used in a court proceeding in Nigeria. Section 54 states the

method through which a request from a foreign state can be made. Section 55 provides for preservation of computer data. To ensure international cooperation, the office of the National Security Adviser must designate and maintain a contact point to be available at all times section 56.

### 4.12 Miscellaneous

The Attorney General is empowered to make regulations for proper implementation of the Act, Section 57.Sections58, 59 provides definition sections and citation respectively.

## 5.0 Criticisms

Computer based crimes are complex and technologically advanced therefore to effectively combat cybercrime, there is a need for a dedicated agency that will be adequately trained in fighting cybercrime. Sadly, the Act has failed to specify the law enforcement agency that would be saddled with the responsibility of fighting cybercrime in Nigeria. This could lead to conflict among the different law enforcement agencies.

While good legislative framework provides a virile springboard upon which the fight against cybercrime could be fought, legislation is not a one fit all solution to the problem of cybercrime. Nigeria lacks the hardware to track computer related crimes, there is urgent need to adopt policies, acquire forensic equipment and improve human skills through adequate and regular training of security agents in order to keep pace with the ever changing dynamics in the cyber world.

## 6.0 Conclusion

The provisions of section 43 (1)(d) and (e) respectively should be implemented in other to improve research and expertise on cyber security and to equip the nation with technical know-how on how to prevent and combat cybercrimes.

There should be collaboration between the various agencies in the area of information sharing to ensure effective, efficient and coordinated fight against cybercrime. Centralized databank should be maintained in order to provide law enforcement agencies with information on individuals.

**References**


Advanced Fee Fraud and other Related Offences Act (1995) now 2006.

Available athttps://en.wikipedia.org/wiki/Stuxnet (accessed 15th October 2016)

Available athttps://us.norton.com/stuxnet(accessed 16 October 2016).

Economic and Financial Crimes Commission Act Cap E1 LFN 2004

Ehimen, O. R., & Bola, A. (2010). Cybercrime in nigeria. *Business Intelligence Journal-January,* , 93-98.

Extradition Act, Cap E 25 LFN, 2004

Federal Republic of Nigeria V. Chief Emmanuel & Ors Suit No: CA/245/05 www.cenbank.gov.ng/419/cases.asap.

Fortinet, G. L, (2009). Fighting Cybercrime: Technical, Juridical and Ethical Challenges. *Virus Bulleting Conference*.

Gercke, M. (2009). Understanding cybercrime: A guide for developing countries. *International Telecommunication Union (Draft), 89*, 93.

Halder, D., Jaishankar, K., & Jaishankar, K. (2012). *Cybercrime and the victimization of women: Laws, rights and regulations* Information Science Reference.

Hassan, A. B., Funmi, D., & Makinde, J. (2012). Cybercrime in nigeria: Causes, effects and the way out. *ARPN Journal of Science and Technology, 2*(7), 626-631.

Ivaturi, K., & Janczewski, L. (2011). A taxonomy for social engineering attacks. *International Conference on Information Resources Management, Centre for Information Technology, Organizations, and People (June 2011),*

Kratchman, S., Smith, J. L., & Smith, M. (2008). The perpetration and prevention of cybercrimes. *Available at SSRN 1123743.*

Premium Times July, 15 2015 Available at http://www.premiumtimesng.com/news/headlines/186692-nigerian-govt-lied-radio-biafra-still-broadcasting.html

Saini, H., Rao, Y. S., & Panda, T. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications, 2*(2), 202-209.

Saulawa, M. A., & Abubakar, M. (2004). Cybercrime in Nigeria: An overview of cybercrime act 2013. *Economic Times,* , 1.

Simon, F. L., & Rubin, S. H. (2000). Distributed denial of service attacks.

The Evidence Act of 2011.

The Guardian Wednesday, July 9, 2008 Pg.39.

The Nigerian Criminal Code (1990) now Cap C38 LFN 2004.