International Journal of Law and Societal Studies
ISSN: 3079-2614
DOI: 10.61424/ijlss
Journal Homepage: www.bluemarkpublishers.com/index.php/IJLSS

IJLSS
BLUEMARK PUBLISHERS

| RESEARCH ARTICLE

Cybercrimes in Nigeria: Law and Issues

AKINLOYE RACHEAL BUKOLA
Faculty of Law, Obafemi Awolowo University, Ile-Ife
Corresponding Author: AKINLOYE RACHEAL BUKOLA, **E-mail**: akinloyerachealbukola@gmail.com

| ABSTRACT

This work focused on the general examination of what cybercrimes entail; it identified the legal and institutional framework of the crimes in Nigeria and their implications on the socio-economic and national development of the country. This study also presented a comparative analysis of the Nigerian perspective of the crime and that of other selected jurisdictions, and finally provided strategies to combatting the menace of cybercrimes. The primary sources of materials used in this research work were statutory provisions in relation to cybercrime law in Nigeria; such as the Cybercrime Act of 2015, the Economic and Financial Crime Commission Act 2004, the Nigerian Criminal Code Act 2004, the Advance Fee Fraud and Related Offences Act 2006, etc. and judicial decisions. While textbooks, journals, conference paper, theses, the internet, etc. were used as the secondary source of materials for this study. The study revealed that the problems posed by cybercrime are critical and yet handled most times with levity. It also discovered that people usually abuse the use of computer technology because of the fertile ground created by the internet for false pretenses, which makes the commission of cybercrimes easy for cyber-criminals. Although certain regulatory frameworks have been put in place to regulate online activities by people, however the work has shown that in spite of these, cyber-criminals still hide behind a computer screen to perpetrate evil. Shockingly, some of the law enforcement agents whose jobs are to ensure proper implementation of the extant laws on cybercrimes lack appropriate trainings to carry out their duties effectively. Cyberspace is vast and has no limit; cybercriminals utilize this opportunity to commit crimes anywhere, from anywhere in the world. In this respect, it has been observed in the work that the issue of jurisdiction determination in cases of cybercrime involving different nations has not been adequately addressed. The study concluded that the current legal and institutional frameworks regulating cybercrime in Nigeria have not been sufficient or comprehensive enough to address various menaces of cybercrime, its surrounding issues (such as the determination of jurisdiction in cases of cybercrime involving more than one jurisdiction) and the threats it poses to the socio-economic and technological development of the country. Also, the failure of law enforcement, security, and intelligence agencies to develop requisite institutional capacity for the effective implementation of the provisions of the existing Cybercrimes Act/ laws is quite discreditable.

| KEYWORDS

Cybercrime, Cyber security, Cyberspace.

| ARTICLE INFORMATION

ACCEPTED: 27 September 2020 **PUBLISHED:** 22 November 2020 **DOI:** 10.61424/ijlss.v1.i1.342

1. Introduction

Since the mid-1990s, the Internet has grown to become a fact of life for people worldwide, especially those living in the Western industrialized world. Its relentless expansion, it is claimed, has transformed the spheres of business, work, consumption, leisure, and politics (Castells, 2002). The Internet is undoubtedly seen as part of the globalization process that is supposedly sweeping away old realities and certainties, creating new opportunities and

challenges associated with living in a 'shrinking' world; it is claimed that we now live in a digital world, and that Technology has brought nations together while the world is now deemed a global village. The arrival of Information Communication and Technology (ICT) into many aspects of everyday life has led to the development of the modern concept of the information society (ITU, 2012). We are now said to be in the midst of a 'new industrial revolution', one that will lead us into a new kind of society, an 'information age' (Webster, 2003).

Yet awareness of, and enthusiasm for, these changes have been tempered by fears that the Internet brings with it new threats and dangers to our well-being and security. 'Cyberspace', the realm of computerized interactions and exchanges, seems to offer a vast range of new opportunities for criminal and deviant activities. A decade or so on from the Internet's first appearance in popular consciousness, we can see that the intervening years have been replete with fears about its 'darker', criminal dimensions. Businesses cite threats to economic performance and stability, ranging from vandalism to 'e-fraud' and 'piracy'; incautious web users are being swindled on a regular basis through various means, with the means engendered by reason of gaining access to the victims' personal cum sensitive information on the internet.

The development of the Internet and related communication technologies thus appears to present an array of new challenges to individual and collective safety, social order and stability, economic prosperity, and political liberty. The development of the internet and the widened access to computer technology has not only granted new opportunities for economic activities but has also created opportunities for those involved in illegal activities (Olayemi, 2014). The internet's rapid diffusion and digitization of economic activities have led to the emergence of a new breed of criminals. In recent years, the economic, political, and social impacts of these cyber criminals' activities have received considerable attention. Individuals, businesses, and government rightfully worry about their systems, network, and IT infrastructure. The flourishing connection between organized crimes and the internet has increased the insecurity of the digital world (Kshetri, 2005).

Considering the pattern of cybercrime, it is apparent that many underlying assumptions are flawed, unrealistic, and implausible to explain with this novel form of criminality. The empirical record regarding cybercrime patterns and strategy to avoid and fight the crimes run counter to the functioning of the cyber world. There are various ways to gain access to information in cyberspace. Attackers can exploit vulnerabilities in software and hardware. They can exploit security vulnerabilities by tricking people into opening infected emails or visiting corrupt websites that infect their computers with malicious software. They can take advantage of people who fail to follow basic cyber security practices, such as changing their passwords frequently, updating their antivirus protection on a regular basis, and using only protected wireless networks.

At the turn of the 21st century, Nigerian internet penetration levels took a running jump. Whereas the number used to be less than 5% in 2002- 2003, it stood at over 40% by the end of 2015, and the growth is only poised to accelerate. The advent of mobile telephones on the Nigerian market played a major role and continues to be a key driver in economic advancement (Final report on the Effects of Cybercrime on Foreign Direct Investment in Nigeria, 2017).

However, the rise of the internet in Nigeria has come with an unintended consequence - global notoriety as a haven of cybercrime. Back in the 90s, fraud in Nigerian society was popularly called '419'. At the time, persons who were arrested in connection to that law were labeled '419'. Enforcement and a ponderous criminal justice system meant that the rampant practice of 419 was already a constant source of grief. Then, along came the internet, shortly after which a number of tech-savvy cons successfully "exported" the 419 concept. While the popular 419 reference has since been extended to include cyber criminals, in Nigeria, the name "Yahoo-Yahoo" is the most familiar informal usage that is employed to speak of people who perpetrate scams online.

The internet has indeed offered a lot of platform for useful research purposes; However, Cybercrime is a worldwide problem that's costing countries billions of dollars. According to crime-research.org, as early as 2003, the United

States was already leading the world in percentage of cyber-attacks at 35.4 percent, followed by South Korea at 12.8 percent (Hassan et al., 2012). Countries with high rates of computer piracy, such as Russia, have reacted slowly to cybercrime. As a result, many hackers and other cyber criminals can flourish in countries with few Internet crime laws while attacking richer countries through their computer because they lacks rules and codes of a central authority that governs it; as such, the internet has no geographical demarcation (Lovet & Fortinet, 2009).

Reiterating Cybercrime as a global phenomenon and not one belonging distinctively to Nigeria, it has been argued that cybercrime does not respect geographical boundary, fighting the menace can only be achieved through partnership with other cyber security organizations and institutions across the world (Akano, 2013). Cybercrime has surpassed the illicit drug trade as the global top revenue earner for organized crimes. The cybercrime network has become a highly organized ecosystem with its own value chain, including researchers of stronger attack methods; hackers who compromise account data and make it available to dump vendors (Lemo, 2013).

Arguing further, it is said that the industrialization of cyber fraud poses a great challenge to the cash-less society in Nigeria. And that the prevalence of fraud globally is contributory to the growing technophobia as users were apprehensive about the safety of their funds on electronic payment platforms. The advent and growth of the internet has not only altered how people interact but has also added a new dimension to criminal activities in society. Weber, a writer, canvassing his own views, maintained that the computer and the internet provided an additional cloak of anonymity to the perpetrators of cybercrime and making illicit activities much more attractive (Weber, 2006).

Also, the development of the internet and the widened access to computer technology has created new opportunities for work and business activities, as well as those who engage in illegal activities. The rise of technology and online communication has not only produced a dramatic increase in the incidence of criminal activities, but has also resulted in the emergence of what appears to be a new variety of criminal activities. Both the increase in the incidence of criminal activities and the possible emergence of new varieties of criminal activity pose challenges for legal systems, as well as for law enforcement (Brenner, 2007). Cybercrimes have now been described as one of the fastest growing criminal activities on the planet (Erharbor, 2008). they range from content-related offences, copyright and trademark related offences, computer-related offences, offences against the confidentiality, integrity, and availability of computer data and systems.

While technological advancements have produced radical shifts in the ability to reproduce, distribute, control, and publish information, the internet in particular has radically changed the economics and ease of reproduction (Longe & Chiemeke, 2008). Computer networks have also radically changed the economics of distribution. With transmission speeds approaching a billion characters per second, networks enable the sending of information products worldwide, cheaply and almost instantaneously.

For Nigeria, a nation in the process of saving her face regarding cybercrimes, efforts are now being directed at the sources and channels through which cybercrimes are perpetrated. It is no gainsaying that many internet assisted crimes are committed daily in various forms such as identity theft, desktop counterfeiting, cyber harassment, fraudulent electronic mails, Automated Teller Machine spoofing, pornography, piracy, hacking, phishing, and spamming (Okeshola & Adeta, 2013). The task of re-stigmatizing cybercrime and re-dignifying honesty is not as easy as that of institutionalizing a deterrence mechanism like the code of conduct bureau, Independent Corrupt Practice Commission (ICPC), Economic and financial crime commission (EFCC), and many more. This is after many years at the bottom of the ladder of the corrupt nations of the world, which is based on some index set by Transparency International (TI), an anti-corruption crusader group (Olayemi, 2014). The nature of cybercrime is such which takes the offence beyond the realm of "Crimes against Persons"; Its diverse nature deems it necessary for States to set up both legal and institutional framework potent enough to stifle the growth of the menace called Cybercrime.

Flowing from the above, the increasing rates of cybercrime in Nigeria have now become a strong threat to the country's e-commerce growth and her security as a whole. Thus, giving rise to the imperative need for a very efficient legal framework on cybercrimes in Nigeria, which this study is set to elucidate.

2. Definition of the Term 'Cybercrime'

'Cybercrime' has always been a hot topic not only for academic but also for the public. Nonetheless, cybercrime is seldom clearly described or defined. Despite the fact that many scholars and legislators have proposed dozens of definitions on 'cybercrime', till now none of the definitions has become widely accepted. In other words, a major problem for the study of cybercrime is the absence of a consistent current definition; thus, a generally acceptable definition of the term 'cybercrime' does not exist (Finklea & Theohary, 2015). As earlier said, there has been a debate among scholars and experts on what constitutes a cybercrime and even among law enforcement agencies charged with tackling it (Aldrich, 2000). At the basic analysis, there is no recognizable control mechanism in place in so far as terminology is concerned (McCusker, 2006). Thus, a person may speak of 'cybercrime', 'computer crime', 'digital crime', and 'high tech crime' and be discussing the same and/or different concepts respectively. Consequently, the term 'cybercrime' has become a generic descriptor for any online wrongdoing ranging from spam email and denial of service attacks to malware.

The word 'Cyber-crime' is a hybrid word made up of 'cyber' and 'crime'; thus, it is necessary to explain these words. The word 'cyber' is a combining form, meaning 'computer', 'computer network' or 'virtual reality', used in the formation of compound word (such as: cyber-talk, cyber-art; cyberspace, etc.), and by extension, it means 'very modern'.

The word 'crime', on the other hand, has been defined in section 2 of the Criminal Code of Nigeria as:

'Acts or omissions which render the person doing the act or making the omission liable to punishment under the code or under any other Act of law.'

Various writers have also made attempts to give meanings to the word; for instance, Glanville Williams (1983) defines 'crimes' as:

'A legal wrong that can be followed by legal proceedings which result in punishment'

Also, Okonkwo (1994) explains the word by way of procedures used in hearing criminal and civil matters. The authors conclude crimes or civil actions can only be defined by way of the procedures involved in the hearing of the matter.

'Cybercrime', according to Sackson, M. (1996), has been described as a crime that is committed with the help of a computer through a communication device or a transmission media called cyberspace and a global network called the Internet.

Furthermore, the Commonwealth Organization states that cybercrime includes not only crimes against computer system (such as hacking, denial of service attacks and the setup of botnets) but also traditional crimes committed on electronic networks (e.g. fraud via phishing and spam; illegal internet-based trade in drugs, protected species and arms) and illegal content published electronically,(such as child sexual abuse material). The author states that cybercrime is any offence carried out involving the use of a computer and the internet (Commonwealth Internet Governance Forum).

Additionally, some scholars have also given meanings to the term 'cybercrime'; however, most of these definitions have been identified with one flaw or the other. For instance, computer crime is referred to as a crime where a computer system itself is the target (Clifford, 2001). However, this definition is too narrow; some cybercrimes do not

involve a computer system being the target of the operation. Sometimes, the computer system could just be a mere instrument in the commission of the crime. A scholar, Ferrera (2001), further defines the word as any violation of criminal law that involves knowledge of computer technology for its perpetration, investigation, or prosecution. However, knowledge of computer technology is always, but not necessarily, needed for the commission of cybercrime. Crimes like child pornography do not necessarily require knowledge of computer technology. Loader (2000) is also of the opinion that,

'Cybercrimes are computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks.'

However, Loader's definition is quite flawed in the sense that cybercrimes are not always conducted through global electronic networks. Cybercrimes, like hacking, do not require global electronic networks for them to be perpetrated.

During the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders, it was argued that cybercrimes can either be defined in narrow or broad terms. Thus, two definitions in terms of the narrow and broad sense were developed. Cybercrime, in a narrow sense, was defined as:

'any illegal behavior directed by means of electronic operations that target the security of a computer system and the data processed by them'

While cybercrime in a broader sense (computer-related crimes) is:

'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.'

Furthermore, according to Chik, W.B. (2007), cybercrimes are to be distinguished from computer-enabled crimes. They relate to crimes against computer hardware as well as the digital contents contained within it, such as software and personal data. Computer enabled crimes have an adverse effect on the integrity and trust in information technology infrastructure, such as computer or telecommunications networks, and in the security of transactions conducted through them. "Computer crimes" is often used to define any criminal activities that are committed against a computer or similar device, and data or program therein. According to Chik W.B. and Longe, O. (2005), in computer crimes, the computer is the target of criminal activities.

Criminal-minded individuals carry out acts or omissions which harm individuals every day in cyberspace. Criminal minded individuals who indulge in the advance fee fraud schemes are now popularly called "Yahoo Boys" in Nigeria. Nigeria has therefore carved a niche for itself as the source of what is now popularly called 419-mails, named after Section 419 of the Nigerian Criminal Code Act Cap. C 38, LFN 2004, which forbids advance fee fraud. In fact, Nigeria is ranked first in Africa as the target and origin of malicious cyber activities, and this is spreading from the West African sub-region, with Ghana also gaining prominence in cybercrime, which is popularly referred to as "Sakawa" in Ghana (Ribadu, 2007).

3. History of Cybercrime

How old is the phenomenon of cybercrime? it is safe to say that soon after the first computer networks were built, some people were looking for ways to exploit them for their own illegal purposes. As soon as it was widely recognized that computers store something of value (information), criminals saw an opportunity (Shinder, 2002). But just as it is more difficult to target a robbery victim who stays locked up in his own home every day, the data on closed, standalone systems has been difficult to steal. However, when data began to move from one compute to another over networks, like the robbery victim who travel from place to place, this data became more vulnerable.

Hence, cybercrime didn't spring up as a full-blown problem overnight. In the early days of computing and networking, the average criminal didn't possess either the necessary hardware or the technique expertise to seize the digital opportunity of the day. Computers were million-dollar mainframe monstrosities, and only a few of them were in existence. An aspiring cybercriminal could hardly go out and buy (or steal) a compute, and even if he did, it's unlikely that he would have known what to do with it. There were no "user-friendly" applications; working with early systems required the ability to 'speak'- machine language- that is, to communicate in the calculations that computers understood.

The cybercrime problem emerged and grew as computing became easier and less expensive. Today, almost everyone in the industrialized countries has access to computer technology; children learn to use Personal Computers (PCs) in elementary school, and people who can't afford computers on their own can use PCs in public libraries or on college campuses for free, or they can rent computer time at business centers or internet cafés. Applications are "point and click" or even voice-activated; it no longer requires a computer science degree to perform once-complex tasks such as sending email or downloading files from another machine across the internet. Some of today's cybercriminals are talented programmers (the hacker elite), but most are not. Advanced technical abilities make it easier for cybercriminals to "do their thing" and cover their tracks, but these abilities are by no means a job requirement.

In summary, the concept of cybercrime is historical. With the advent of information and communication technology, massive digitalization and unprecedented interconnectivity provided by the internet has been a boon to students, doctors, teachers, lawyers, businessmen, and criminals. Historical antecedent shows that unauthorized access, damage to property, theft, and distribution of obscene and indecent materials are all considered as familiar cybercrimes (The Communicator, 2018).

Over the years, the alarming growth of the internet and its wide acceptance has led to an increase in security threats. In Nigeria, today, several internet assisted crimes known as cybercrimes are committed daily in various forms such as fraudulent electronic mails, pornography, identity theft, hacking, cyber harassment, spamming, Automated Teller Machine spoofing, piracy, and phishing. Thus, cybercrime is a threat against various institutions and people who are connected to the internet, either through computers or mobile technologies. The exponential increase of this crime in society has become a strong issue that should not be overlooked. The impact of this kind of crime can be felt on the lives, economy, and international reputation of a nation and therefore should be tackled.

4. Factors Which Trigger Cybercrime

A paper presented by N. Rubadu (2007) highlighted some of the factors that trigger cybercrime or the reasons why we have these crimes in Nigeria today. Thus, the followings are excerpts from the discussion; two main factors aided this pattern:

- The free travel protocol, which was granted by the Economic Community of West African State (ECOWAS) treaty; as well as
- The increasingly developed Information Technology (IT) infrastructure in the sub region.

These two factors, together with the poor attitude initially shown towards this fraud because it is presumably preyed on foreign victims, were the factors that aided the commission of cybercrime. The above factors originally provided little incentives to do anything about the scammers, whose boilers rooms were growing by the day in other ECOWAS nations that had now become particularly attracted to the scammers, such as Togo, Benin, Ghana, Burkina Faso, and Cote d'Ivoire, among others.

However, the causes of cybercrime are more than the above mentioned by Rubadu; other contributing factors, such as greed, uncontrollable desire for massive wealth (in other words, the get quick rich syndrome), and mass

unemployment, have been recognized as additional factors. It has also been discovered that the categories of people who practice this nefarious act mostly fell among the followings:

- The perpetrators are youths, and thousands of them are unemployed but highly knowledgeable and skillful in the use of computer; they actually drive the process.
- They are well connected through local insider conspiracy in the financial institutional locally as well as with the Nigerian immigrant community elements abroad.
- Knowing fully well that Nigeria has reinforced her security process, they have migrated to mostly West African and other African nations with weak enforcement mechanisms.
- They also use a mechanism of re-shippers mostly in Dubai, the UK, and the West African way stations.
- They enjoy the fact that there are no cybercrime laws in any of these African jurisdictions that they have chosen as their relay stations.

Furthermore, some other three chief reasons why cyber-criminals commit cybercrime have been identified (Ayofe, 2010). First, cybercrimes can be committed for the sake of recognition. This is basically committed by the youngsters who want to be noticed and feel among the group of the big and tough guys in society. They do not mean to hurt anyone in particular; they fall into the category of the Idealists, who just want to be in the spotlight. Secondly, some cyber-criminals want to make quick money. This group is greed motivated and is career criminals who tamper with data on the net or system especially, e-commerce, e-banking data information, with the sole aim of committing fraud and swindling money off unsuspected customers. Finally, the crime is committed by some cyber-criminals to fight a cause they think they believe in; to cause a threat and most often damages that affect the recipients adversely. This is the most dangerous of all the causes of cybercrime. Those involve believe that they are fighting a just cause and so do not mind who or what they destroy in their quest to get their goals achieved. These are the cyber-terrorists.

5. Categorizing Cybercrime

According to the Council of Europe (COE), 2001, Convention on cybercrime, cyber-crime involves action directed against the confidentiality, integrity, and availability of computer systems, networks, and computer data as well as the misuse of such systems, networks, and data. Also, the Department of Justice ("DOJ") defines computer crimes as any violations of criminal law that involve the knowledge of computer technology for their perpetration, investigation, or prosecution (Dillon, 1998). Thus, cybercrimes have been categorized into three categories, which include: crimes against person, crimes against property, and crimes against the government (Razali).

5.1 Cybercrimes Against Person

These include various crimes like harassment of any one with the use of a computer, such as email phishing. The trafficking, distribution, posting, and dissemination of obscene material, including pornography and indecent exposure, constitute some of the cybercrimes known today. The potential harm of such a crime to humanity can hardly be amplified. This is one cybercrime which threatens to disrupt or undermine the growth of the younger generation and leave irreparable scars and injury on them if not controlled.

5.2 Cybercrimes Against Property

These are kinds of cybercrimes that are against all forms of property and they include: computer vandalization (destruction of other's property), transmission of harmful programmes such as a virus, or denial of the entire service.

5.3 Cybercrimes against the Government

Cyber-terrorism is one distinct kind of crime in this category. The growth of the internet has shown that the medium of cyberspace is being used by individuals and groups to threaten the governments (both internationally and locally) and also to terrorize the citizens of a country. This crime manifests itself into terrorism when an individual cracks into a government or military maintained website (Maitanmi et al., 2013).

Furthermore, there have also been various categorizations of cybercrimes by some scholars. For instance, according to Goodman (1997), cybercrime is in three categories: first is crime where a computer is the target of the crime; secondly, crimes where a computer is a tool of the crime; and lastly, crimes where the computer is incidental.

In the Convention on Cybercrime, another classification can be found which distinguishes between four types of offences: Offences against the confidentiality, integrity, and availability of computer data and systems, computer-related offences, content-related offences, and copy right-related offences. However, it has been argued (Ayofe & Irwin, 2010) that this classification is not wholly consistent, as it is not based on a sole criterion to differentiate between categories. While the first one focuses on the object of legal protection, the remaining three categories focus on the object of the crime.

Finally, Mali (2009) and Poonia (2014) categorize cybercrimes into four different places, which are: cybercrime against individuals, cybercrime against property, cybercrime against organization, and cybercrime against society.

6. Legal and Institutional Framework for the Regulation of Cybercrime in Nigeria

Due to the initial absence of specific laws in Nigeria to combat cybercrimes (Ehimen & Bola, 2010), cyber-criminals freely operated without any legislation fighting their criminal activities. Also, the provision of the section 36(12) of the 1999 Constitution of the Federal Republic of Nigeria (as amended) can be said to have created an ideal environment for these cyber-criminals to freely operate, since it is provided under the section that a person can only be convicted of a codified crime to which the punishment, where breached, is prescribed. The legislatures have, therefore, made efforts to make laws fit to combat cybercrimes in Nigeria (Ani, 2011), hence the enactment of the Cybercrime Act 2015 for the prohibition of cybercrimes and other related matters. Also, the EFCC Act 2004, the Advanced Fee Fraud Related Offences Act, the Nigerian Criminal Code, the Money Laundering Prohibition Act, the Nigerian Evidence Act, among others, are other laws indirectly prohibiting cybercrimes in Nigeria.

6.1 Economic and Financial Crimes Commission (Establishment) Act 2004

The preponderance of cybercrimes involving advance fee fraud (419), money laundering, phishing, among others, has had severe negative consequences on Nigeria, including decreased Foreign Direct Investments in the country and tainting Nigeria's image. The danger of cybercrime and the gravity of the situation led to the passing into law of the EFCC Act. The EFCC Act also establishes the Economic and Financial Crimes Commission (the EFCC) to implement and execute the provisions of the act.

The Economic Financial Crimes Commission (Establishment) Act 2002 was enacted to repeal the Financial Crimes Commission (Establishment) Act 2002. According to section1 of the EFCC Act, a body known as the Economic Financial Crimes Commission (EFCC) was established with the responsibility of the enforcement and the due administration of the EFCC Act. The paper titled "Internet Service Providers and Cybercrime in Nigeria Balancing Services and ICT Developments" has supported that the Economic financial Crimes Commission is the body empowered by the government to fight all forms of financial crimes, including cybercrimes in Nigeria (Lounge et al., 2007). Section 5 of the Act is the basis for the actions of the EFCC as it confers on the Commission, the power to investigate all financial crimes including advance fee fraud money laundering, counterfeiting, illegal charge transfers and also the prosecution all offences connected with or relating to economic and financial crimes, in consultation with the Attorney-General of the Federation.

In the case of FEDERAL REPUBLIC OF NIGERIA V. CHIEF EMMANUEL &ORS., the accused persons were reputed to have carried out the third world biggest single scam with numerous others pending in count. In this case, they were charged to the High Court of Lagos State. A 57 count charge was proffered against the accused persons, including the scamming to the tune of US $181.6 million, and they were all found guilty and sentenced accordingly. In addition to this sentence, their assets were forfeited to the Federal Government of Nigeria, and the sums of money recovered and returned to their owners.

6.2 Advanced Fee Fraud and Related Offences Act 2006

Advance fee fraud is a vexing threat and a major problem in Nigeria today (Chawki, 2009). The term "advanced fee fraud" describes offences in which offenders seek to convince targets to advance a small sum of money in the hope of receiving a much larger sum afterwards (Reich, 2004). In other words, the activities of advanced fee fraud is a medium whereby perpetrators traffic emails requesting the addressee to assist them in wiring or transfer a huge sum of money from one part to the other, thereby involving multiple parties by promising them a share in the percentage.

Thus, the Advanced Fee Fraud and Related Offences Act was enacted to prohibit and punish certain offences pertaining to advance fee fraud, other fraud related offences, and to repeal other Acts related therewith. The Act provides for ways to combat cybercrime and other related online frauds. The Act provides for a general offence of fraud with several ways of committing it, which are by obtaining property by false pretence, use of premises, fraudulent invitation, laundering of fund obtained through unlawful activity, conspiracy, aiding, among other crimes.

Section 2 makes it an offence to commit fraud by false pretence. This Section can be used to prosecute criminals who commit cybercrimes like computer related fraud, where the offender uses automation and software tools to mask criminals' identities, while using the large trove of information on the internet to commit fraud.

The Advanced Fee Fraud and Related Offences Act is currently the only law in Nigeria that deals with internet crime issues, and it only covers the regulation of internet service providers and cybecafés (Maitanmi et al., 2013), it does not deal with the broad spectrum of computer misuse and cybercrimes as cited by Odulaja and Wada (2012).

6.3 Cybercrime Act 2015

The afore-mentioned legislations have proved ineffective in curbing cybercrime, as it is on the increase. In an attempt to put in place a stronger legal framework to curb cybercrimes, a revision of the existing cybercrime law was forwarded by the government in September 2008 (Adesina, 2017). The bill titled "A Bill for an Act to provide for the prohibition of electronic Fraud in all in all Electronic Transactions in Nigeria and for other Related Matters" passed second reading in November 2012 at the Senate. In May 2015, the Cybercrime bill was signed into law, properly defining the Act as unlawful with penalties attached to any disobedience of the law. The Act known as the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 creates a legal, regulatory, and institutional framework for the prohibition, prevention, detention, investigation, and prosecution of cybercrimes and for other related matters.

The Cybercrimes Act is, thus, the first legislation in Nigeria that specifically deals with cybercrimes and cyber security. The application of the provisions of the Act would also apply throughout the Federal Republic of Nigeria. It stipulates that any crime or injury on critical national information infrastructure, sales of pre-registered SIM cards, unlawful access to computer systems, Cyber-terrorism, among others, would be punishable under the new law.

The Cybercrime Act is made up of 59 sections, 8 parts, and 2 schedules. The objectives of the Act are to:

(a) Provide an effective and unified legal, regulatory, and institutional framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes in Nigeria;

(b) Ensure the protection of critical national information infrastructure; and

(c) Promote cyber security and the protection of computer systems and networks, electronic communications, data, and computer programs, intellectual property, and privacy rights.

7. Comparative Study Of Cybercrime Legislation

7.1 Cybercrime In The United States

The United States has widely been known as one of the forerunners of attempting to use criminal law to regulate cyber wrong doings or cybercrimes, not only to use the then existing criminal law, but also to promulgate new laws. Such attempts can be traced back to the 1970s. The US has certain federal laws that relate to computer crimes. In the early 1980s, law enforcement agencies in the US faced the dawn of the computer age with developing issues about the lack of criminal laws available to fight emerging computer crimes.

CFAA was a cyber-security law that protects federal computers and computers connected to the Internet. It protects them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud. It is not a statute which is broad in scope, but instead it fills cracks and gaps in the protection afforded by other federal criminal laws. The offences provided for by the Act include obtaining national security information, accessing a computer and obtaining information, trespassing in a government computer, accessing a computer to defraud and obtain value, intentionally damaging by knowing transmission, recklessly damaging by intentional access, negligently causing damage and loss by intentional access, trafficking in passwords, and extortion involving computers.

The federal **Wiretap Act** is another US law for fighting computer crimes. This Act, as amended in 1986 by the **Electronic Communications Privacy** Act, protects the privacy of wire, oral, and electronic communications, a broad term that includes computer network communications (Jarret & Bailie). It is both procedural and substantive. It prohibits not just law enforcement, but 'any person' from making an illegal interception or disclosing or using illegally intercepted material.

The **Identity Theft and Assumption Deterrence Act of 1998** is another federal law in the US relating to computer crime. Section 1028 of the Act criminalizes certain types of conduct involving fraudulent identification documents or the unlawful use of identification information. Another US law is the **Access Device Fraud**. Prosecutors commonly bring charges under Section 1029 in many types of 'phishing' cases, were a defendant uses fraudulent emails to obtain bank account numbers and passwords, and 'carding' cases, where a defendant purchases, sells, or transfers stolen bank account, credit card, or debit card information.

7.2 Cybercrime In France

The French suffer more from cybercrime than any other Europeans; this is according to the report made by the computer security company Symantec. The company also reported that 41% of French Smartphone users have been victims of criminal acts in the past years, compared to 29% in Europe and 38% worldwide. Some factors affecting the rise of cybercrime in France have been identified (Chawki, 2005).

France has adopted an extensive legal framework on cybercrime and computer related offences, starting with the **Law No. 88-19 on computer fraud ('Godfrain Law')** and its amendments, as it is codified by **Art. 321-1a323-7 of the Penal Code.** The legal framework was developed by the following legislative texts, especially the **Law On Confidence** In **The Digital Economy** (LCEN Law) of 21 June 2004.

The Art **321-1 2323-7 of the Penal Code** defines as crimes all offences against the confidentiality, integrity, and availability of computer data and systems, including illegal access, data interference, system interference, as well as misuse of devices. Offences related to child pornography are covered by Art. 222-23 to 222-31; 223-13; 22-14, 25-7-1;227-26.

7.3 Cybercrime In England And Wales

The **Computer Misuse Act (CMA) 1990** (now amended by the Police and Justice Act 2006) focuses mainly on computers and is the only legislation that explicitly tackling computer crime. The Act creates three main offences: (i) unauthorized access to computer material, (ii) unauthorized access to a computer system with intent to commit or

facilitate further offences, and (iii) unauthorized modification of computer material. Maximum sentences for these offences range from six months imprisonment and/or a 500 Euros five to ten years imprisonment and/or an unlimited fine.

In 2001, the United Kingdom signed the Convention on Cybercrime. To implement this Convention and to respond to the pressure from the (England) All **Party Internet Group**, legislators promulgated the (England) **Police and Justice** Act **2006** and amended the **CMA** 1990. In other words, the current **Police and Justice Act** contains an amendment to the **CMA** under the Section called 'Miscellaneous Part 5 Computer Misuse amendments'.

7.4 Cybercrime In Canada

Cybercrime in Canada is an evolving international phenomenon. People and businesses in a country or another countries may be affected by computer crimes that or may not originate within the borders of their country. Canada has been recognized as one of the first countries to enact criminal laws in the area of computer crime. Canada is also ahead of nearly two-thirds of the 52 countries surveyed in enacting laws to crack down on cybercrimes, this is according to a study by a United Nations-sponsored network of internet policy officials.

Canada is a signatory to the *Convention on Cybercrime*. It requires that each state party prosecute cybercrimes committed within its territory. This translates that a country could claim territorial jurisdiction in a case where the computer system attacked is on its territory, even if the perpetrator of the attack is not.

The **Criminal Code of Canada,** as last amended 2005, makes provisions of crimes relating to the use of computer and computer networks. In Canada, a crime is a computer crime if it falls under **Section 430 or 342.1** of the Canadian Criminal Code, that is, where a computer or data is the object of the crime.

8. Effects Of Cybercrimes On Foreign Direct Investment And Economic Development

The cost of cybercrime to any nation is enormous and can completely ruin the country's economy if the proper security strategies are not put in place. Foreign Investments into that economy can begin to dwindle. Several governments of the world are continuously carrying out research to improve their cybercrime attacks counter-measures. For instance, the Nigerian Government set up the cybercrime committee, which formed the Nigerian Cybercrime Working Group (NCWG), so as to accelerate the implementation of its Cybercrime research efforts; the Nigerian National Assembly has also passed the Cybercrime Bill into law.

Nigeria, as part of the nations classified under developing countries, has benefited immensely from Foreign Direct Investments since the middle 1990's. It goes without saying that the country's economy in recent times has had advancements in Information and Communications Technology, which can be seen in every facet of its industries. This growth has also attracted innumerable crimes which have directly and otherwise affected the influx of Foreign Direct Investments, especially in the form of Cybercrime (Final report on the Effects of Cybercrime on Foreign Direct Investment in Nigeria, 2017).

8.1 Adverse Effects Of Cybercrime On Foreign Direct Investment

The cost of cybercrime to a society can be both qualitative and non-qualitative. These are the financial losses to individuals and organizations (figures rarely made public), as well as the sizable expense of security software and personnel to protect against possible digital incursions. Then there is also damage to brand image where a country be the unfortunate victim of online crimes.

a) Reduces the competitive edge of organizations

Cybercrimes over the years have cost a lot of havoc to individuals, private and public business organization within and outside the country, causing a lot of financial and physical damage. Due to cybercrimes, there has being a global loss of billions of dollars annually. Cybercrimes may threaten a nation's security and financial health. Sensitive

company information can be stolen and sold to a competitor company; this will automatically reduce the competitive strength of the company.

b) Time wastage and slows financial growth
A lot of time is required by the professionals to constantly stay ahead of cyber criminals. Nations spend a huge amount of money to fortify their information systems and ward off any attack by cyber criminals. These resources could have been channeled into other, more productive sectors of the business or nation.

c) Loss of revenue
Loss of revenue can be caused through identity theft, unauthorized access to important information like trade secrets, and by scams in which the victims willingly pay for undelivered services. Recent statistics show that cybercrime fraud is over $559 million annually. Furthermore, research has shown that companies hit by cybercrime attacks lose revenue through a decline in stock prices by between 1 - 10%.

d) Reduced Productivity
There is an unquantifiable loss through reduced productivity, especially when people find themselves spending more time preventing, troubleshooting, or protecting themselves from the effects of cybercrime, rather than engaging in more productive activities.

e) Damaged reputation
High level of cybercrime in a country brings that country's name into disrepute within the international community. Nigeria is viewed by some countries in a negative manner when it comes to cybercrime.

f) Unemployment
The issue of cybercrime and its impact on the Nigerian economy in relations to FDI inflow has increasingly become worrisome and has been an increase in the unemployment rating of the country, where FDIs and their parent companies flee the country and in some instances cut their staff strength due to cyber-attacks that has led to fall in profit.

8.2 Benefits Of Foreign Direct Investment To Nigeria
The underdeveloped nature of the Nigerian economy, that essentially hindered the pace of her economic development, has necessitated the demand for Foreign Direct Investment (FDI) into the country. J.A. Aremu (1997) noted that Nigeria, as one of the developing countries of the world, has adopted a number of measures aimed at accelerating growth and development in the domestic economy, one of which is attracting FDI into the country. Foreign Direct Investments are often seen as an important catalyst for economic growth in developing countries because it affects economic growth by stimulating domestic investment, increase in capital formation, and also facilitating the technology transfer in the host countries.

Also, Foreign Direct Investment has emerged as the most important source of external resource flows to developing countries over the years and has become a significant part of capital formation in these countries, though their share in the global distribution of FDI continued to remain small or even declining. The role of FDI has been widely recognized as a growth-enhancing factor in developing countries. Speaking on the effects and advantages of FDI to the host economy, it was noted that the effects are normally believed to be: an increase in employment, augmenting the productivity, a boost in exports, and an amplified pace of transfer of technology (Ugochukwu et al., 2013).

9. Poverty As An Instigator Of Cybercrimes In Nigeria
Poverty is one major factor adduced for the rise in various crimes, most especially cybercrime in Nigeria. It is thus important, while examining the relation between cybercrime and poverty, to define the two terms "cybercrime" and "poverty". The definitions of the word 'poverty' have been given in many ways by different scholars. Some of these

scholars have defined it in relations to income, many treat poverty as multidimensional, using indicators such as (i) low income, (ii) low levels of education and health, (iii) vulnerability (to health or income loss natural disaster, crime and violence, and education curtailment) and (iv) voicelessness and powerlessness (feeling discrimination, lacking income earning possibilities, mistreatment by state institutions, and lacking status under the law).

According to Fields (1994), he defines poverty as:

the inability of an individual or a family to command sufficient resources to satisfy the basic needs, such as food, clothing, shelter, health care, and other necessities of life.

In 1998, a United Nations Statement on poverty, signed by the heads of all UN agencies, stated on the meaning of poverty as thus:

Fundamentally, poverty is a denial of choices and opportunities, a violation of human dignity. It means a lack of basic capacity to participate effectively in society. It means not having enough to feed and cloths a family, not having a school or clinic to go to, not having the land on which to grow one's food or a job to earn one's living, not having access to credit. It means insecurity, powerlessness, and exclusion of individuals, households, and communities. I means susceptibility to violence, and it often implies living on marginal or fragile environments, without access to clean water or sanitation.

The issue of poverty in Nigeria is a paradox. While Nigeria is a leading oil-producing nation and highly endowed in terms of various natural resources, most of its people are economically poor. As national data shows, over one-third of Nigerians (35%) live in extreme poverty, while 54% are relatively poor. For instance, the Nigeria Poverty Profile 2010 Report of the National Bureau of Statistics provides an insight into the level of poverty in the country. More than half of the Nigerian population lives on less than a dollar a day.

Thus, there is a magnitude of unemployment in Nigeria. These unemployed youths have time on their hands and have easy access to the internet to perpetuate cybercrimes. Even if they do not have access to the Internet at home, cyber-cafés are readily available throughout the country at relatively low rates for Internet access. All these factors combine to create a new generation of local hackers and cyber-criminals (Olowu, 2009). Although they may not have deep programming knowledge like experienced hackers who can create their own malware or viruses, they take advantage of many websites available for free that help them understand the basics behind hacking techniques, with links to underground hacking sites and even free tools to use.

10. Combating Cyber Crime in Nigeria

The increasing use of the Internet has also led to an increase in cybercrime. The FBI and other law enforcement agencies in Canada, Europe, Asia, and Africa spend countless hours fighting cybercrime each day, but everyone can help combat cybercrimes. Learning the different types of cyber-crimes and ways that can help combat these crimes is an important step in helping to catch these cyber criminals and keep them from continuing to commit cybercrimes against others.

Cybercrime cannot be easily and completely eliminated, but can be minimized. However, collaborative efforts of individuals, corporate organization, and the government could go a long way to reduce it to a minimal level. Firms should secure their network information. The followings are ways to combat cybercrime.

1. Laws to enforce property rights work only when property owners take reasonable steps to protect their property in the first place. As one observer has noted, if homeowners fail to buy Locks for their front doors, should towns solve the problem by passing more laws or hiring more Police? Even where laws are adequate, firms' dependent on the network must make their own Network, Information, and computer systems secure.

2. Governments should ensure that their laws apply to cybercrimes. African countries are bedeviled by various socioeconomic problems such as poverty, AIDS, fuel crisis, political and ethnic instability, and other related crimes. This limits their strength to effectively combat cybercrime. Nevertheless, it is important that Nigeria, as a nation, take measures to ensure that its penal and procedural laws are adequate to meet the challenges posed by cybercrimes.
3. Individuals should observe simple rules. Individuals on their part should ensure proper anti-malware protection on their computer systems, they should be encouraged to avoid pirated software, never to share their Personal Identification Number (PIN), bank account, email access code to unknown persons, never disclose any confidential information to anybody as none of these networks were designed to be ultimately secure.

11. Conclusion

Cybercrime is a global practice today, particularly in Nigeria, where it has become a predominant practice, whereby the regulations to these crimes are newly established for the purpose of tackling cybercrime threats. The menace of crime has eaten deep into the fabrics of our society and poses threats to the socio-economic development of the country. It is pertinent to state here that although cybercrime is a global phenomenon, the vulnerabilities and their impacts on societies tend to differ depending on the strength of the measures, such as cyber laws and cyber protection technologies, each country put in place to combat the crime.

In Nigeria, cybercrime has become a huge menace threatening foreign investment, socio-economic, and technological advancement of the nation. Socially, cybercrime activities such as cyber stalking, harassment, blackmail, and cyber terrorism are dangerous to an individual's right to privacy and fundamental freedom. Similarly, cybercrimes like pornography, child predation, online gambling, online prostitution undermines morality in society and puts society at risk of a breakdown of social norms and values.

The prevalence of cybercrime has also created a bad image for Nigeria amongst the committee of nations as one of the most corrupt nations in the world. This tarnished national image affects the way Nigerians and Nigerian businesses are treated abroad with suspicion and extreme caution, as Nigerians are stereotyped to be fraudulent and hence not to be trusted. Private companies around the world are beginning to take steps geared towards blocking e-mails originating from the country, while financial instruments are accepted with extreme caution.

With each passing day, we witness more and more alarming cases of cybercrimes in Nigeria, with each new case more shocking than the one before. Ironically, the prosecution of the offenders of this heinous crime has remained relatively low, as many people who are secretly engaging in cybercrime are going all over society scot-free. It could be said that over the past years, cybercrime laws have served to be deterrents to cyber-criminals; however,, these laws are still grossly inadequate.

Therefore, flowing from the above, it can be concluded that the current legal and institutional frameworks regulating cybercrime in Nigeria have not been sufficient or comprehensive enough to address various menaces of cybercrime, its surrounding issues (such as the determination of jurisdiction in cases of cybercrime involving more than one jurisdictions) and the threats it poses to the socio-economic and technological development of the country. Also, the failure of law enforcement, security, and intelligence agencies to develop requisite institutional capacity for the effective implementation of the provisions of the existing Cybercrimes Act is quite discreditable.

12. Recommendations

Expanding the rule of law into Cyberspace is an essential technique to ensure a reliable environment for business and people. Since that extension is a work in progress, corporate bodies presently must first and foremost safeguard their personal information and systems from attack, be it from within or outside. To ensure this self-protection, corporate bodies must concentrate on executing the plans of cyber security by addressing the process,

people, and technology cases. Apart from all these, the following are the various recommendations (Ezeifekwuaba, 2019) for the government of the country.

12.1 Issue Of Cyber-Security Should Be Prioritized By The Government

The defense of any country has moved from physical to the technology space; thus, the problem posed by cybercrime in Nigeria, for instance, may persist until there is a framework for digital sovereignty in the country. Also, lack of data encryption, poor awareness, under reporting of breaches, etc., would continue to fuel the menace in the country. Therefore, government and business organizations should not take cyber-security issues with levity.

12.2 Governments Should Assure That There Are Laws Specifically Applying To Cybercrimes

National governments remain the dominant authority for regulating criminal behavior in most places in the world; some nations have struggled from, and ultimately improved, its legal authority after a confrontation with the unique challenges presented by cybercrime. It is crucial that other nations can copy this lesson and examine their current laws to discern whether they are composed in a technologically neutral manner that would not exclude the prosecution of cyber criminals.

12.3 Proper Training Of The Law Enforcement Agencies

For Section 24(3) of the Cybercrime Act, which provides for the training of law enforcement agencies to be more efficient, the agencies, either through workshops or specialized training abroad on cyber forensics, should be properly trained to investigate and prosecute cybercrimes. There is also a need for an over-arching legislation which would clearly specify the duties and boundaries of all these law enforcement agencies in most nations.

12.4 Initiation Of An Africa-Wide Cybercrime Treaty By Nigeria

First, ratification and domestication of the Budapest convention on cybercrime is paramount. This would enhance international cooperation in the fight against cybercrime and go a long way in resolving issues of jurisdiction when a cybercrime is committed and has to be prosecuted. However, the Convention on cybercrime might be good, but not be totally applicable to the peculiar situations of cybercrime in Africa and in Nigeria. Hence, Nigeria can initiate an Africa-wide Cybercrime Treaty, which would cover the peculiarities embedded in the commission of cybercrime in African countries.

12.5 Firms Should Secure Their Networked Information

The laws to enforce property rights will work only when property owners take reasonable steps to protect their property in the first place. For instance, if homeowners failed to buy locks for their front doors, should towns solve the problem by passing more laws or hiring more police?. Even where laws are adequate, firms dependent on the network must make their own information and systems secure.

12.6 Establishment Of A Framework Of International Cooperation

While law is always territory-based, the tool, the scene, the target, and the subject of cybercrime are all boundary-independent. Domestic measures will certainly be of critical importance, but not sufficient for meeting this worldwide challenge. Therefore, to combat cybercrimes, international coordination and cooperation is very crucial due to the trans-national nature of the crime.

12.7 Enlightenment Of The Public

There is a need to enlighten the public on the dangers that come with using the internet. Ignorance that cybercrimes have a similar effect with real world crimes makes people not to adopt measures to protect themselves from cybercriminals. Such measures may include using computer anti-viruses/internet protection for computers and or smart phones, accepting only people you know as your friends on social media, and avoiding unnecessary publicity of private lives, as through this, a cybercriminal may stalk and later kidnap a victim.

12.8 Establishment Of A Centralized Online Cybercrime Reporting Mechanism

Finally, there is a need for the commission responsible for the implementation of the provisions of the Cybercrime Act to put a centralized online cybercrime reporting mechanism in place, which provides victims of cybercrime a convenient and easy-to use reporting mechanism that alerts authorities to suspected cybercriminals.

References

[1] Adesina, O. S. (2017). The Cybercrime and Poverty in Nigeria, *Canadian Social Science*, Vol. 13(4), 19-29.

[2] Akano, T. (2013). Cyber crime: Nigeria redeems image, *The Punch*.

[3] Aldrich, R. (2000). Cyber-terrorism and computer crimes: issues surrounding the establishment of an international legal regime', *Information Operation Series* USAF, Paper 32.

[4] Ani, L. (2011). Cybercrime and National Security: The Role of the Penal and Procedural Law, *Law and Security in Nigeria*, 197-232.

[5] Aremu, J.A. (1997). Foreign Private Investment: Issues Determinant and Performance', Paper presented at a Workshop on Foreign Investment Policy and Practice, organized by the Nigerian Institute of Advance Legal Studies, Lagos.

[6] Ayofe, A.N. & Irwin, B. (2010). 'Cyber Security: Challenges and the Way forward', *Computer Science and Telecommunications*, Vol. 6(29), 58.

[7] Brenner, S. (2007). *Law in an Era of Smart Technology*, Oxford: Oxford University Press.

[8] Castells, M. (2002). *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford: Oxford University Press.

[9] Chawki, M. (2005). 'Cybercrime in France: An Overview', *Computer Crime Research Center*.

[10] Chawki, M. (2009). 'Nigeria tackles advance fee fraud', *Journal of Information, Law & Technology*, Vol. 1.

[11] Chik, W.B. (2007). "Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore", *Icfai lawbooks*.

[12] Clifford, R. (2001). *Cybercrime: The Investigation, Prosecution and Defence of a Computer-Related crime*, Caroline Academic Press.

[13] Commonwealth Internet Governance Forum. "Commonwealth Cybercrime Initiative".

[14] Dillon, S.A. (1998). 'Note, Computer Crimes', *American Criminal Law Review*, 35, 503-505.

[15] Ehimen, O.R. & Bola, A. (2010). 'Cybercrimes in Nigeria', *Business Intelligence Journal*, Vol. 3(1), 93-98.

[16] Erharbor, M. (2008). 'Cybercrime and the Youths', Unpublished PGDE Thesis, Department of Education, Ambrose Ali University, Ekpoma, Nigeria.

[17] Ezeifekwuaba, T. (2019). 'Cybercrimes and Legislation in the Globe: Nigeria as a case study', *Journal of legal methodology, policy and governance*, Vol. 1(1), 1-7.

[18] Ferrera, G. et al. (2001). *Cyber law: Texts and Cases*, Southwestern College Publishing Co.

[19] Fields, G. (1994). Poverty changes in developing countries. In R. Van Der Honven & R. Anken (Eds.), *Poverty monitoring: An international concern*. New York: St. Martins Press.

[20] Final report on the Effects of Cybercrime on Foreign Direct Investment in Nigeria (2017). Nigerian Communications Commission (Dept. of New Media and Information Security).

[21] Finklea, K. & Theohary, C. (2015). 'Cybercrime Conceptual Issues for Congress and U.S. Law Enforcement', *Congressional Research Service*.

[22] Goodman, M. (1997). 'Why the Police don't care about Computer Crime', *Harvard Journal of Law and Technology*, Vol. 10(3), 465-494.

[23] Hassan, A.B., Lass, F.D. & Makinde, J. (2012). 'Cybercrime in Nigeria: Causes, Effects and the Way Out', *ARPN Journal of Science and Technology*.

[24] ITU (2012). 'Understanding Cybercrime: Phenomena, Challenges and Legal Response', September Report.

[25] Jarret, M. & Bailie, M. 'Prosecuting Computer Crimes', Published by Office of Legal Education, Executive Office for United States Attorneys.

[26] Kshetri, N. (2005). 'Pattern of Global Cyber War and Crime: A Conceptual Framework', *Journal of International Management*, Vol. 11(4), 541-562.

[27] Lemo, T. (2013). 'Cyber crime: Nigeria redeems image', *The Punch*.

[28] Loader, B. & Douglas, T. (2000). *Cybercrime: Security and Surveillance in the information Age*, Routeledge.

[29] Longe, O.B. & Chiemeke, S.C. (2008). 'Cybercrime and criminality in Nigeria - What roles are internet access paints in playing?', *European Journal of Social Sciences*, 6(4), 133-139.

[30] Longe, O. et al. (2005). 'Implications of the Nigeria Copyright Law for Software Protection', *the Nigerian Academic Forum Multidisciplinary Journal*, Vol. 5(1), 7-10.

[31] Lounge, O.B. et al. (2007). "Internet Service Providers and Cybercrime in Nigeria: Balancing Services and ICT Development", 1-11.

[32] Lovet, G. & Fortinet (2009). "Fighting Cybercrime: Technical, Juridical and Ethical Challenges", *Virus Bulletin Conference*.
[33] Maitanmi, O., Ogunlere, S., Ayinde, S. & Yinka, A. (2013). "Cybercrimes and Cyber Laws in Nigeria", *The International Journal of Engineering And Science (IJES)*, Vol. 2(4), 19-25.
[34] Mali, P. (2009). 'Classification of Cybercrimes', *Lawyers Club India*.
[35] McCusker, R. (2006). "Transitional Organised Cyber Crime: Distinguishing Threat from Reality", *Crime, Law and Social Change*, 257-273.
[36] Odulaja, G.O. & Wada, F. (2012). "Accessing Cybercrime and its Impacts on E-Banking in Nigeria Using Social Theories".
[37] Okeshola, F. & Adeta, A. (2013). 'The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria', *American Journal of Contemporary Research*, Vol. 3(9), 98-114.
[38] Okonkwo & Nalsh (1994). *Criminal Law in Nigeria*, 2nd ed. Spectrum Law Publications, Ibadan.
[39] Olayemi, O. (2014). 'A socio-technological analysis of cybercrime and cyber security in Nigeria', *Academic Journal*, Vol. 6(3), 116-125.
[40] Olowu, D. (2009). Cyber-crimes and the boundaries of domestic legal responses: Case for an Inclusionary Framework for Africa, *Journal of Information, Law and Technology (JILT)*, 1-18.
[41] Poonia, A. (2014). 'Cyber Crime: Challenges and its Classification', *International Journal of Emerging Trends and Technology in Computer Science*, Vol. 3(6), 119-121.
[42] Reich, P.C. (2004). 'Advance Fee Fraud Scams In-Country and Across Border', *Australian Institute of Criminology International Conference*, Hilton on the Park, Melbourne, Australia.
[43] Ribadu, N. (2007). 'Cybercrime and Commercial Fraud: A Nigerian Perspective', Modern Law for Global Commerce, *Congress to celebrate the fortieth annual session of UNCITRAL Vienna*.
[44] Sackson, M. (1996). Computer Ethics: Are Students Concerned?", *First Annual Ethics Conference*.
[45] Shinder, D.L. (2002). 'Scene of the Cybercrime Computer Forensics Handbook', *Syngress Shinder Books*.
[46] The Communicator (2018). 'A Summary of the Legislation on Cybercrime in Nigeria', December.
[47] Ugochukwu, U.S., Okore, O.A. & Onoh, J.O. (2013). 'The Impact of Foreign Direct Investment on the Nigerian Economy', *European Journal of Business and Management*, Vol. 5(2), 25-33.
[48] Weber, J. (2006). 'The Cloak of Anonymity'.
[49] Webster, F. (2003). *Theories of the Information Society*, 2nd edition, London: Routledge.
[50] Williams, G. (1983). *The Text Book of Criminal Law*, 2nd edition, Stevens & Sons, London.