BALTIC JOURNAL OF LAW & POLITICS
A Journal of Vytautas Magnus University
VOLUME 15, NUMBER 1, (2022)
ISSN 2029-0454

Cit.: *Baltic Journal of Law & Politics* 15:1 (2022):2042-2055
DOI: 10.2478/bjlp-2022-00131

An Appraisal Of The Nature Of Cybercrimes

Ulisan Mogbitse Ogisi Ph.D[1]
Peter Ikechukwu Gasiokwu Ph.D[2*]
Solomon Chiamaka Ajede LL.M[3*]

[1]Senior Lecturer, Delta State University, Abraka, Nigeria, Faculty Of Law (Oleh Campus), Dept Of Public Law. Email: ulisanmogbitse@gmail.com

[2]*Senior Lecturer, Delta State University, Abraka, Nigeria, Faculty Of Law (Oleh Campus), Dept Of Commercial and Property Law.Email: gasiokwupeter567@gmail.com

3*Doctoral candidate, Delta State University, Faculty of Law (Oleh Campus) Email:ajedepossible@gmail.com

***Corresponding Author: -** Peter Ikechukwu Gasiokwu Ph.D

*Senior Lecturer, Delta State University, Abraka, Nigeria, Faculty Of Law (Oleh Campus), Dept Of Commercial and Property Law. Email: gasiokwupeter567@gmail.com

Abstract
Cybercrime is a type of internet-related crime that has emerged in cyberspace. The typical crimes and problems of poverty, war, corruption, tourism, and the like seem to have rendered the majority of governments ineffective. Cybercrime has become an uncontrollable monster due to the criminal justice system's lack of awareness in both legal and technical matters. What qualifies as cybercrime has grown to be a contentious issue among scholars. The central idea that a computer serves as the main means of committing the crime has not been met with widespread acceptance. We have no choice but to strengthen the approach, knowledge, law, and resources to bring cyber crime under control in order to preserve our economic well-being, personal safety, political stability, and the survival of the nation as a whole. This is due to the general trend, impact, and dimension of cyber crime in law.

Keywords: Cybercrimes, offences, computer, online, Nigeria.

1. INTRODUCTION

Cybercrime is a global phenomenon. [1] A computer that is connected to the internet is all that is required for one to commit such a crime. Due to its lack of boundaries, the cyberspace has evolved into a playground for criminals where they may commit crimes while avoiding detection.[2] Numerous opportunities have been produced by the growth of the internet and computer technology, yet these opportunities have also had some unfavourable effects. [3] Among the effects we frequently experience are privacy violations, online scams, etc. The world's legal history is being confronted by bizarre crimes that have never occurred and are unheard of. [4] In Nigeria

[1]Obanyi, K *CyberCrime Law in Nigeria – Principles and Strategies* (USA. Charleston, SC, 2015) 6.

[2] Brenner SW, "Cybercrime Investigation and Prosecution: the Role of Penal Procedural Law". (2012) Murdoch University Electronic Journal of Law <(austlii.edu.au) http://www5.austlii.edu.au/au/journals/MurU/2001/8.html>accessed 18 October, 2021.

[3]Ankur J. Cybercrime: Nature, Elements and Types (2019), 2 (2) *National* Journal of Cyber Security Law at 1-5.

[4] Wall D *The Transformation of Crime in the Information Age* 1stEdition (USA; Harvard University Press, 2007) 43.

today, cybercrime is on the rise. As a result, Nigeria has turned into a "hideout" for online scammers. The Nigerian government appears to be preoccupied with issues they consider urgent, including poverty, the Boko Haram crisis, corruption, the fuel crisis, political instability, the #ENDSARS agitation, and traditional crimes like murder, kidnapping, rape, theft, and most recently, attacks by headsmen. The effort to combat cybercrime is therefore falling behind.
However, some African nations are making an effort to combat cybercrime. [5]In order to combat the threat of cybercrime, the Nigerian government has introduced cyber legislation since 2015. [6] Many people have criticized the aforementioned regulation for being antiquated and for failing to address the problems posed by cybercrime. [7]

This paper aims to investigate the characteristics of cybercrime. The history, types, categories, and causes of cybercrime will also be considered.

2. HISTORY OF CONCEPTS

Early computers featured certain built-in security benefits, such the Electronic Numeric Integrator and Computer (ENIAC), Binary Automatic Computer (BINAC), Universal Automatic Computer (UNIAC), and other Punch Card Tabulation Machines. Around the 1960s, commercial computers like the Programmed Data Processor (PDP-1) were first developed with a business model of renting the equipment out to businesses and people on a time-sharing basis. This exposed the information and software contained therein to risk, opening the door for hackers. In 1961, not long after receiving its first PDP-1, Massachusetts Institute of Technology (MIT) produced the first hacking collective. [8] Computers were deployed in the 1970s. A peculiar set of individuals known as Phreaks thrived on the notion of breaking it. The Phreaks developed a blue box device that could generate a 2600 hertz signal, enabling them to carry out nefarious activities like shadowing a trunk line and cutting off the operator line that allowed for free long distance calls. The founders of Apple Computer, Steve Wozniak and Steve Jobs,[9] were reported to have participated in the early development and distribution of related gadgets. In the 1970s, the Altair 8800, the first reasonably priced PC, made it possible for people to purchase computers and learn programming.

Some people quickly developed a taste for full-fledged hacking after receiving this knowledge. The introduction of other computers, such as the IMB-PC and Radio Shack's TRS-80, gave users who were eager to discover fresh methods to take advantage of the system's capabilities access to more powerful computing at the same time. With new ideas like peer-to-peer communication standards like the internet, networking technology has significantly advanced and moved beyond the mainframe model, enabling businesses to make suitable solutions that connect computers quickly and affordably. Regrettably, these open standards also made it simpler for hackers to access computers by deciphering the widely used protocol.

There have been attempts to create seamless connection between computers as they have become more affordable and have entered the mainstream. One such project was the ARPA Net, and while it was being designed, security was not a concern for research scientists because they believed that the network's sparse nodes reduced the harm that security branches could provide. Early in the 1990s, when internet connection became commoditized and reasonably priced, attacks increased in quantity and cybercrime began to traverse international borders. Hackers in West Germany who were detained for stealing into US Government and corporate computers and selling operating system source code to the Soviet KGB were among the first cyber-espionage cases to garner international attention. [10] Another instance involved the theft of $10 million from Citibank by Russian Cracker Vladimir Levin, who then transferred the funds to

[5]Other African countries such as Botswana, Kenya, Uganda and Cameroon, etc.
[6]Cybercrime (Prohibition, Prevention, Etc.) Act, 2015.
[7]Vanguard Newspapers of October, 10, 2019 at 9.
[8]Debra LS "Scene of the Cybercrime; Computer Forensics Handbook"< http:// www. syngress.com/catalog/?pid.2250>accessed 10 November 2021.
[9] Stieg, C "Steve Wozniak: When Apple got 'big money' Steve Jobs personality Changed' (February, 6, 2020).
[10]*Ibid*.

several banks throughout the world. [11] For automatic payroll and accounting activities, banks and other financial firms were among the first major private sector [12], computer users. As a result, a computer fraud technique was developed. However, as technology developed, there were more instances of cybercrime. From the beginning, a number of people were actively involved in the fight against computer crime.

Many observers believe Donn B. Parker of the United States to be the father of computer crime expertise and its originator. Beginning in the early 1970s, he worked on studies related to computer security and crime. He was the primary author of the first basic Federal guidebook for law enforcement in the USA [13] and worked as a Senior Computer Consultant at the Stanford Research Institute (SRI) International. This guide soon evolved into an encyclopedia for use by law enforcement outside of the US [14].

3. DEFINITION OF CYBERCRIME

One of the phrases people use frequently in today's culture is "cybercrime." The idea of cybercrime and its growth are relatively recent phenomena made possible by cybercrime activities carried out via globalized information and communication technology and the expansion of global connectivity, cutting across borders and, as a result, transcending earlier recognized computer-related crime.

Understanding the definitions of "Cyber" and "Crime" is necessary in order to comprehend what cybercrimes are. The prefix "Cyber" is used to identify concepts that are a part of the information and computer age. [15] To know what cybercrimes are, it is vital to understand the concepts of "Cyber" and "Crime." Concepts from the information and computer era are designated with the prefix "Cyber." [16] It is important to note that Anah's definition of crime places more emphasis on the need for a criminal motive than it does on the potential harm that a crime can cause. This definition is arbitrary since a person may be held accountable for a crime in a separate jurisdiction even though they did not intend to or even had a criminal purpose.

Crime is related with harm and violence, according to both academic research and popular opinion. However, we cannot agree on the most fundamental issue, "what is crime?". Despite the fact that statutory definitions have been supplied for specific reasons, the term "crime" does not in contemporary criminal law have a straightforward and widely agreed definition. [17] The most common perspective is that anything is only a crime if the law that applies to it declares it to be one. [18] One definition put out states that a crime, also known as an offence or a criminal offence, is an act that is harmful to the community or the State as well as to some specific persons (public wrong). The phrase "Crime is an act that the law makes punished" strikes me as the most palatable definition of a crime. [19] The definition of cybercrime is as follows:

The latest vandals and data thugs don't need to physically interact with their victims in the networked world. Data can be quickly duplicated, sent, changed, or destroyed. As a result, the crime scene is particularly challenging because there are no fingerprints or other evidence, it is

[11]Perera, R. "Transfer of fund" CNN.com. Nov. 26, 2000. Feb. 27, 2001 at 1.
[12]*Ibid.*
[13] Wall DS *The Transformation of Crime in the Information Age* (1st Edition, Harvard University Press, 2007) 23.
[14]*Ibid*.
[15]Anah, BH "Cybercrimes in Nigeria: Causes, Effects and the Way Out"; (August 2012) Vol2. NO.7. *AREN Journal of Science and Technology* 626.
[16]*Ibid.*
[17]Farmer, L "Crime Definitions" in Cane and Conoghan (ed). *The New Oxford Companion to Law*, (UK: Oxford University Press 2008) 263.
[18]Such definitions as provided by Section 243 (2) of the Trade Union and Labour Relations (Consolidated) Act 1992 and by the schedule to the Prevention of Crimes Act 1871. See *Aoko v. Fagbemi*(1961) 1 ALL N. L. R. 400.
[19]Garner,BA Black's Law Dictionary 9th ed., (USA: West Publishing Co., 2009) 427.

difficult to identify the perpetrators, it is even harder to apprehend them, and the judicial system does not adequately provide for justice in cases of this kind of crime. [20]

In light of the aforementioned, several authors have provided numerous definitions of cybercrime. After understanding the dual meanings of "Cyber" and "Crime," this would be explained. Cybercrime is described as "a criminal offence on the internet, a criminal offence involving the internet, a criminal offence committed in relation to the internet, etc." [21] Summer [22] claims that there is no accepted or widely accepted definition of cybercrime and that there are no direct impact evaluations of its scope. Articles 2 to 6 of the Treaty of Budapest, the Council of Europe's cybercrime convention,[23] address "substantive offences," "illegal access," and "misuse of equipment," as well as "system interference," "data interference," and "illegal interception."

It includes "computer-related forgeries" and "computer-related fraud"[24] in addition to "computer-related offenses". [25] Additionally, "unauthorized acts with the aim to impair, or with reckless disregard as to impairing, the operation of computers, e.t.c." are included in the definition of cybercrime.

Any illegal use of computers and networks is considered a form of cybercrime (called hacking). It also encompasses conventional crimes committed online, such as credit card fraud, identity theft, hate crimes, and online fraud. [26] According to Okwunma, cybercrime is a type of cloud crime and shouldn't be limited to crimes committed using computers. Cybercrime should be defined as criminal activities carried out using a computer and the internet because the majority of cybercrimes use the internet as a tool. [27]

The standards used to define the phrase "Cybercrime" or "computer crimes" have caused some confusion. Some assert that any crime involving the use of a computer is unlawful, while others contend that any crime committed when a computer is present is unlawful. [28] However, some people disagree with how cybercrime is classified. Is it accurate to say that utilizing a computer to commit a crime qualifies as "cybercrime"? For instance, in the situation of data entry involving taxable transactions, is it not possible for someone to commit fraud simply by entering inaccurate information onto tax forms that are available in both electronic and physical formats? In 2002, Girasa asserted that the term "cybercrime" is a catch-all term that refers to a wide range of offences with computer use as a central element that are listed in penal codes or laws. According to him, cybercrime is a crime as long as the criminal codes and any other legislation specifically state that it involves not just the use of computers but also the use of computers as the central component. [29]

[20]Duggal, ShriPavan'Cyber Assault and Cybercrime' (August, 2009).<http://Cyber laws. net/ cyberindia/cyberassault.htm>accessed 3 December, 2021

[21]Farlex, "The Free Dictionary", (2014) <www.thefreedictionary.com>accessed 18 December, 2021.

[22] Herman, TT "*Ethics and Technology, Ethical Issue in an Age of Information and CommunicationTechnology",*2nd Edition (USA: John Wiley & sons Inc, 2005) 202.

[23]Council of Europe Cybercrime Convention, 2004. It dates back from 2001 and came into force in 2004 and was ratified by the UK in 2011.

[24]Article 7 of the Council of Europe Cybercrime Convention, 2004.

[25]*Ibid*.

[26]Thisday, Thursday 21 March, 2013.

[27] Okunma, EN "Criticism: Cybercrime Bill", 2013, University of Witwatersrand Johannesburg South Africa 95

[28]*Ibid.*

[29]Girasa, RJ *Cyber Law: National and International Perspectives* 1st Edition **(**New Jersey**:** Prentice Hall Publishers, 2001) 54.

Cybercrime was divided into two categories and defined as follows during a workshop during the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, which was focused on concerns relating to crimes involving computer networks: [30] These are:
a. Cybercrime, in its narrowest form, refers to any illicit activity directed through electronic operations that compromises the security of computer systems and the data they process. [31]
b. Cybercrime, or computer-related crime, is broadly defined as any criminal activity carried out with the aid of or in connection with a computer system or network, including offences like unauthorized possession and the offering or distribution of information via a computer system or network. [32]

This definition, which includes computer crime and criminality related to computers, provides us with an excellent starting point for figuring out what cybercrime actually implies. Computer and crime are the two components of computer crime.
As a result, it entails a crime involving a computer. [33] The connection might, however, also be indirect. For example, a criminal might employ someone to influence a critical computer user in order to alter a computer system rather than just using a computer to do crime. [34] Thus, one involves taking advantage of a technical IT infrastructure's [35] weakness, and the other involves taking advantage of the organization's IT users' social support system. [36]

4. TYPES OF CYBERCRIMES

There are many types of cybercrimes, but this paper will focus on those that are exclusive to Nigeria. They include:
a. Spam/Scam emails: Email scams and spam are among the most disgusting cybercrimes in Nigeria. These con games solicit and advertise fake investments. Nigeria's reputation as a nation has been severely damaged by the cybercrime species, giving rise to a specific sort of email scam known as the "Nigerian E-mail Scam."[37], The email scam can manifest itself in any of the following ways:
i. The offender informs the victim via email that she is the designated beneficiary in an estranged relative's will and is eligible to receive millions of dollars as inheritance.
ii. Online Charities: Here, the criminal asks for money and support from victims through the use of fictitious charitable organizations.
iii. Con artists pose as businesspeople, government officials, or the surviving spouses of former public servants in Nigeria or any other nation where money is temporarily restricted as the bait in this scheme.

They propose to transfer a large sum of money into the account in exchange for the victim paying a "fee" or "taxes" that will allow them to access the funds. The aforementioned is not meant to suggest that only Nigerians have engaged in this kind of criminality. The targets of electronic scams or spam emails are typically foolish people who could be anywhere in the world, despite the fact that the scam is typically associated with Nigeria. The scam is now widespread in many other African nations. These days, communication primarily occurs via Facebook and text messages. Therefore, with the rise in mobile usage, scam emails are increasingly sent to users

[30]Talwant S., 'District and Sessions Judge', *Cyber Law & Technology*, Delhi- India.67.
[31]Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, Vienna A/CONF.187/10, 10-17 April 2000 at 4.
[32]*Ibid*.
[33]*Ibid..*
[34]*United States v. Morris* (1991) 928 F. 2d 504, The accused invaded the security system through a worm as to measure the weakness of MIT which in turn prevented the use of Federal interest computers, thereby causing loss. He was held guilty.
[35]See *S v. Douvenga*case no 111/150/2003, dated 2003/08/19 Northern Transvaal Regional Division 93 Cr APPR 25, 02 Dec2003.
[36]*Ibid.*
[37]*Ibid.*

of mobile devices to entice the victims into their nets. [38]

b. Cyber Stalking: There isn't currently a common understanding of what "Cyber Stalking" means. It is often regarded as stalking or harassing someone via the internet, email, or another electronic communication tool. The term "stalking" refers to persistently bothering or menacing behaviour[39]. In order to pursue their targets, cyber stalkers employ gadgets like cell phones, fax machines, and other modern technologies. The definition of cyber stalking as a crime has changed from one region or country to another, and it is currently illegal in many jurisdictions. A perpetrator's identity might be totally hidden online due to the anonymity of the medium.
Additionally, cyberstalking has contributed to violent criminal instances offline. For instance, an unidentified person followed a South Carolina woman in the USA for several years via email, threatening to kill her, rape her daughter, and posting her home location online for anybody with internet access to see. [40]

c. Cyber-Squatting: According to section 58 of the Nigerian Cybercrime Act, 2015, "Cyber-Squatting" is defined as the purchase of a domain name online in bad faith with the intent to profit, mislead, damage reputation, or prevent others from registering the same as follows: [41]
(a) at the time the domain name was registered, it was similar, identical, or confusingly similar to an already-registered trademark with the relevant government body.
(b) comparable to a name belonging to someone other than the registrant, whether it is identical or not; and
(c) acquired without right or with intellectual property interests in it .

d. Cyber Terrorism: This involves using the internet to carry out terrorist acts or to start terrorist attacks. This is a brand-new technique or method that insurgents or religious extremists (like Boko Haram) employ to enlist new recruits and plan future attacks on other countries.

e. Theft of Communication Services: This is getting an employee's access code fraudulently or utilizing software that is readily available online to access a company's phone switchboard. However, it is conceivable for criminals to target victims in other nations when it is impossible to do personal telephone verification checks. For example, money could be electronically deducted from accounts after business hours when it's impossible to see the transaction right away.

f. Internet Pornography: The use of the internet for sexual assault is still a hot topic for investigation. Internet pornography has been discovered to be a troubling trend, particularly among young people. To prevent online pornography in Nigeria, the usage of web filtering software has been encouraged. Additionally, downloading and sending pornographic images, photos, essays, and other content via the internet is involved. In a similar vein, child pornography is distributed online and used to attract unwary youngsters to pedophiles. Child pornography has been exchanged and sold using the internet as a medium. As a result, prostitutes now use the internet to sell their services by showing internet users their private, sensual, and sensitive areas. Just recently, 200 commercial prostitutes living at the cattle market near the Anambra State border hamlet of Amansea protested against the Anambra State Urban Development Board's demolition of their home (ASUDEB). [42]

g. Impersonation and identity theft: This is the intentional acquisition or possession of another person or entity, whether they are alive or dead, with the goal of misleading or defrauding the general public online. Identity theft is defined as the use of another person's personal information to purchase goods and services through electronic transactions in section 58 of the Cybercrime Act, 2015. [43]

h. Phishing: The phrase was created by hackers who send emails on behalf of reputable businesses to persuade recipients to divulge their passwords or credit card information. This

[38]One of the researchers has within a space of one month, received 10 email scams via facebook from different personsasking him to come and invest in puzzle scheme in order to make more money.
[39]*Ibid.*
[40]Victor T & Olumide, O "E-crime in Nigeria; Trends, Tricks and Treatment"(2005) <www. Openj. gate/search/searchresults/articles> accessed 27 October 2021.
[41]Section 58 (Interpretation Section) of the Nigerian Cybercrime (Prohibition and Prevention, etc) Act, 2015.
[42]Published in Vanguard Newspapers of 18th day of August, 2015.
[43]Section 58 (Interpretation Section) of the Nigerian Cybercrime (Prohibition and Prevention, etc) Act, 2015.

phrase refers to the practice of internal con artists who "fish" for password and financial information from "users" while utilizing increasingly sophisticated lures. According to the Cybercrime Act, "phishing" is the illegal and dishonest act of trying to obtain sensitive data, such as usernames, passwords, and credit card numbers, by impersonating a reliable party in an electronic communication such as email or instant messaging. For example, you might receive an email that purports to be from your bank asking you to change your password or reveal your identity so that the information can later be used. One of the most popular tricks is to create a duplicate page that seems like it belongs on the company's website by copying the HTML code from a popular website. When the user submits their credit card information or password on this page, a bogus email is sent out with a link to it. While the user is still on the computer site, the data is sent to the client. [44]

i. ATM/ Credit Card Fraud: The Automated Teller (ATM) is a cash dispensing device that uses computerized technology to help clients avoid the stress and difficulties they frequently face when trying to check their account balance or withdraw cash from their individual banks. The conventional function indicated above is no longer fulfilled by this machine. One can make online purchases with an ATM card. ATMs and e-transaction systems are used to commit ATM fraud. Each year, consumers lose millions of dollars as a result of the theft of credit card and calling card details from online databases. Criminals occasionally steal users' PINs and use their cards to drain the whole balance of their accounts. The public now has less faith in the technology that is supposed to offer convenience and comfort when withdrawing.

j. Cyber Piracy: Infringing on intellectual property is another way to put it. With the use of digital technology, it is now relatively simple to flawlessly replicate artistic works like music or movies, and the internet offers a free, anonymous way to send or exchange these pirated materials all over the world. [45] Software piracy is a $11.8 billion problem that is only getting worse, according to data from Business Alliance (BSA), an international consortium of top software and e-commerce providers. [46] The cyber security industry has two different definitions of cyber piracy. [47] Cyber piracy is broadly defined as any situation in which a digital document is copied without permission using the internet. A few instances involve copyright, distributing audio or video without the owner's consent, or putting pirated software on a CD.

k. Cyber Hacking: The phrase "cyber hacking" is used to characterize online crimes such eavesdropping, defacing, hijacking, bombing, diddling hyper zapping, and denial of service attacks. [48] Hacking can be a major infringement of privacy and a serious threat to e-commerce, despite the fact that some internet users may find it amusing and even rather clever.

i. Computer Vandalism: This happens when a hacker takes important data from the computer system, denying access to the data to the system's rightful user or owner. [49] This may directly result in a loss of revenue or indicate a significant loss of anticipated revenue. Conley [50] claims that the characteristics of this cybercrime have to do with knowledge of computer use or the technology used to commit the crime; the rate of internet connectivity; internal computer crimes like logic bombs, packet-sniffers, viruses, etc.; hardware and software theft; and telecommunication crimes, among others.

m. Illegal E-lotteries: Online criminals frequently take advantage of Nigerians' desire to become wealthy quickly by sending alluring messages about lottery bonanzas that already exist,[51] in which participants can win a variety of goods and money, including cars, houses, electronics, and laptops, to name just a few. In Nigeria, this kind of cybercrime is widespread. Many Nigerians have been lured to their deaths using even the immigration lottery for the United States and Canada. Due to the high number of young people who are eager to travel overseas, these con artists have created online visa lotteries in order to defraud young people. These days, e-lotteries can also be played on mobile devices. It is typical to get texts like these asking you to

[44] *United States v. Lee* 15 Johns 484 (N.V. 18177) 1998.
[45] Herman note 22 above 35.
[46] *Ibid.*
[47] *Ibid.*
[48] Carter D., "Computer Crime Categories", *FBI Law Enforcement Journal,* Vol. 64, NO. 21 (1995) R.271.
[49] Conley C.H, "CyberCrime" NIJ Reports, Vol. 6 No. 218 (1990) 3.
[50] *Ibid.*
[51] *Ibid*.

answer questions, most of which are quite simple. This encourages the victims to show more interest and maybe earn money. Most of these e-lotteries are run by dubious individuals or organizations whose identities cannot be confirmed. There is no question that this has a detrimental effect on the economy of Nigeria.
Nigeria was listed as the third-largest source of cybercrime worldwide as of 2009 and 2010, respectively, according to the Economic and Financial Crime Commission Report. [52] But Nigeria moved up two spots from the previous quarter's 18th position to the 16th position at the end of the first quarter of 2016 (January - March, 2016). [53] The index is based on threat intelligence gleaned from Check Point's Threat Cloud World Cyber Threat Map, which monitors how and where cyber attacks are occurring globally in real time. Of all the above-mentioned cybercrimes, e-banking fraud/crimes are the most common in Nigeria. As a result, the majority of E-banking users and beneficiaries, particularly those who use the ATM services, have threatened to massively discard their cards if the dishonest act is not stopped. The popularity of online banking has increased the opportunity for cybercriminals. Using wire transfers or account takeovers, money is embezzled. Fraudulent online applications for bank loans are submitted by criminals, who also attack online banking payment systems and disrupt e-commerce by launching denial-of-service assaults. [54]

Identity theft can also happen online, where identity thieves may hijack new accounts, raising questions about the security and stability of financial institutions. Therefore, Nigeria and other countries will continue to serve as worm breeding grounds for cartels engaged in such illicit activities unless crime detection and prevention are addressed jointly. The fight against this crime must be a worldwide one.

5. CAUSES OF CYBERCRIMES IN NIGERIA

According to the 2006 census, there are about 160 million people living in Nigeria. [55] According to a recent report, software piracy costs Nigeria roughly $80 million annually. The study's findings were presented in the report, which was produced by the South African market research firm Institute of Digital Communication. Additionally, the American National Fraud Information Center reported that in 2001, up to 90% of online scams used Nigerian money offers.
Nigeria has an extraordinarily high impact on cybercrime per person, according to the centre. [56] Under this heading, an effort will be made to pinpoint the root causes and driving forces behind people's engagement in cybercrime. These elements include: money/financial gain, fame/recognition, low conviction rates or even being caught, ease of penetration, intellectual arousal, frustration, retaliation, display of wealth by dishonest politicians, "Yahoo, Yahoo boys," laziness, and a lack of moral guidance from parents and guardians.
Awe examined and provided an explicit aspect of the motivational factors in his paper titled "Fight Cybercrime in Nigeria,"[57] when he stated that:

Someone could harbor resentment for a company. If a new company enters his market and you're unhappy about it, you can strive to develop something that will make the services that company is offering useless. Consider the individuals who create software and antivirus programs for profit, such as AVG and Avast. These businesses might create something that the other's antivirus program is unable to handle, rendering antivirus useless. Another driving element is the Yahoo Boys' extraordinary success rate in carrying out their unlawful activity without being apprehended by law authorities, which will only serve to inspire others. The desire to achieve,

[52]EFCC/NBS/(2009), (2010) Business Survey on Crime & Corruption and Awareness of EFCC in Nigeria, Summary Report.
[53]www.Businesstoday.com /Cybercrime: Nigeria ranks 16th on global Threat Index-June 3, 2016/ – accessed 28 August 2021.
[54]Atherton M., "Criminals Switch Attention from Cheques and Plastic to Internet Transactions", *The Sunday Times* March 10, 2010.
[55]During the interaction between the operator of a cyber café (Mr. Uche Otono) and one of the researcher at Asaba, Delta State on the 20th day of April, 2015.
[56]*Ibid.*
[57]Awe, "Fighting Cybercrime in Nigeria", (2008) 26 (5), *the Electronic Library* 716-725.

the get-rich-quick syndrome, vengeance, and occasionally sabotage are additional motivators. [58]

Additionally, a cyber café owner stated that:
The driving forces can vary, but in my opinion, insufficient legislation, financial incentives, low execution costs, a low likelihood of being apprehended and put on trial (as a result of lax laws and enforcement mechanisms), and a relatively low level of stigmatization of cybercriminals have all played significant roles. [59]

During a client interview, Melvin (a suspect in a cybercrime)[60] responded to a question about his motivations for such illicit behaviour by saying:
You've seen how our Nigerian leaders celebrate riches; this has inspired me and other young people to engage in cybercrime. Nigerian culture promotes riches without considering where it comes from. Politicians found guilty of state fraud are appointed to state committees and given prestigious awards, such as the one we just saw. Why won't I discover a means to withstand the financial difficulty so that can also call my name? Corrupt people are invited to start building projects and hold important positions in churches and mosques.

Another cybercrime suspect expressed the following reasons for his involvement in the crime:
The biggest problem is that the software I love to use is typically pricey, and I lack the funds to handle purchasing it. Instead, I'll try to modify the program so I can use it whatever I want and perhaps sell it to make some money. Then, in our peer group, we employ it as a means of establishing reputation; for instance, if one successfully cracks software, they receive the respect of their peers. [61]

Below are x-rayed several more factors that may contribute to cybercrime. They are:

1. Urbanization
One of the main factors contributing to cybercrime in Nigeria is urbanization, which refers to the widespread migration of individuals from rural areas to cities. This ultimately leads to intense competition among the expanding population, especially the elites. As a result, the elites find it profitable to invest in cybercrime because it is a business that requires less cash to invest in, and they are known as "Yahoo Boys." Urbanization will only be advantageous if and only if decent jobs can be established in the cities where population growth is occurring. Meke[62] posited in his article titled "Urbanization and Cybercrime in Nigeria." He stressed that urbanization without good jobs is actually unattainable.
As a result, because cybercrime requires less cash, the elites among them find it profitable to invest in it. The authors modestly disagrees with Omeke's position on the matter because elite and non-elite members of society now make up the cybercriminal population. [63]

2. Unemployment
High rates of unemployment, challenging economic situations, and a deficient educational system have all been linked to cybercrime. [64] The Nigerian National Bureau of Statistics reports that there are about 20 million unemployed persons in Nigeria, and each year, roughly 2 million more people join this depressing group. This demonstrates unequivocally how unemployed many young people are. An old saying goes, "An idle mind is the devil's workshop." As a result, the

[58] *Ibid.*
[59] Vanguard Newspapers, April, 10, 2020.
[60] Johnson, J "African: number of Internet Users in Selected Countries 2020" (25 May, 2021) <http://www.internetworldstats.com .com/stats1.htm> accessed 7 September 2021.
[61] Duggal, ShriPavan note 20 above.
[62] Meke, ESN: "Urbanization and Cyber Crime in Nigeria: Causes and Consequence" (2019) 34(12) *NDIC Quarterly* 34.
[63] Akogwu, S" An Assessment of the Level of Awareness on Cybercrime among Internet users", (2012) Ahmadu Bello University, Zaria.
[64] Malware, "Causes of Cybercrime in Nigeria" (2012) <www.wikipedia.com>assessed 6 October 2021.

majority of our kids will utilize their time and expertise as a platform for their illegal activities in order to better their lot in life and to make ends meet.

3. Quest for Wealth

The need for money is a significant factor in cybercrime. [65] Since there is a significant wealth difference between the rich and the typical person, many people try to move up the social scale as quickly as they can. However, for any firm to succeed, the rate of return on investment must increase at a geometric pace while posing the least amount of risk. The majority of cybercrime only needs a favourable environment and minimal expenditure. Nigeria is such a place, and many online criminals profit from that.

4. Negative Role Models

Most cybercrime merely requires a good setting and minimum investment. Such a location exists, and many cyber criminals take use of it. Meke[66] states that because crime is a sociocultural value that needs to be passed on to the younger generation, many parents nowadays socialize their children with criminal principles. Imagine a scenario in which a child has enough money from cybercrime to acquire houses, live opulently in the community without a work, and be celebrated by society. Most of them will not perceive anything wrong with cybercrime behaviours if this culture is allowed to continue to thrive and the younger generation adopts it. The authors predict that the Cybercrime Act of 2015 would be a mirage until the country's legislation is properly applied. The current researchers believe that an awareness campaign should be run to inform the populace of the penalties and punishments as included in the 2015 Cybercrime Act.

6. EFFECTS OF CYBERCRIME

Cybercrime has the ability to impede socioeconomic development and technology advancement, both of which are essential for increasing productivity. Financial instruments established in Nigeria are viewed with mistrust by international financial institutions. Cheques and drafts from Nigerian banks are no longer accepted as valid foreign payment methods. [67] Nigeria is frequently viewed as an undesirable market by foreign investors. Internet service providers (ISPs) and email providers in Nigeria have already been added to blacklists for email blockage. [68] Some businesses are filtering Nigerian-originating traffic and entire internet network parts.

Over the years, computer crimes have caused significant financial and physical harm to people, private and public corporate organizations within and beyond the nation. [69] Each year, billions of dollars are lost as a result of cybercrime, which also poses a risk to the security and prosperity of a country. Nigeria's current ranking/rating in Transparency International, which lists Nigeria as one of the most corrupt nations in the world, is due to the negative impact cybercrime has had on the country's reputation. [70]

Three Nigerians, Onuoha Nnanna Francis, 34, Valentine O. Anumaka, 28, and Eze Victor, 35, are said to have been detained by India's Central Crime Station (CCS) for defrauding two Indian businessmen of Rs 3. 6 lakh by luring them with an offer to invest $1 lakh in the hotel industry.[71] This is only one of several incidents that have damaged Nigeria's reputation. Most transactions these days take place online, cybercrime also has the effect of scaring away investors. If someone can access your data, he has all the power to render your system redundant. [72]

---

[65] Obono, M "Cybercrimes: Effect on Youth Development", (2008) <http://www.i-genius.org>assessed 30 December, 2021.

[66]Meke note 62.

[67]Ani: L "Cybercrime and National Security: The Role of the Penal and Procedural Law" (2011) <http://www.ejournalofscience.org> accessed 8 December 2021.

[68]*Ibid.*

[69] Ologbodi,K "Fighting Cybercrime in Nigeria" (2010< http// guide2 nigeria. com/news_ articles_About_Nigeria>
accessed 13 November 2021.

[70]Sturgeon, "Global Information and Communications Technology Industry: Where Vietnam Fits in Global Value Chains",

[71]Vanguard of March, 2019, Pg. 45

[72]Premium times. August, 2015. 1

7. EXAMINATION OF THE NATURE OF CYBERCRIME

About a few decades ago, fraud in Nigerian society was known as "419" in reference to the provision of the Criminal Code that makes acquiring money under false pretenses a crime[73]. People who were detained in relation to that law at the time were known as "419ers." It must be remembered that fabrication, impersonation, forgery, and fraudulent fact representation are all connected methods that work together to either aid in or promote advance fee fraud, which is also sometimes referred to as cybercrime in today's society.

The Nigeria Supreme Court had course to entertain an online Advance Fee Fraud in *Mike Amadi v. Federal Republic of Nigeria,*[74] (One Hundred and Twenty Five Thousand United States Dollars). This was done by Fabian Fajans using his email address princemike2001@yahoo.com, the registered domains efccnigeria.com and Reddiff.com, the India Limited multilink telephone number 017946846, and a falsified Central Bank of Nigeria payment schedule with fraudulent pretence. It was committed by asking for money to handle the transfer of $2.5 million USD, which was the agreed-upon amount for generators. Fabio Fajans was deceived into believing that US$125,000 represented the 5 percent processing fee of the total amount of US$2.5 million, in violation of sections 5(1), 8(b), and 1(3) of the Advance Fee Fraud and other Related Offenses Act, which was purported to have been supplied by the Federal Government of Nigeria for the All African Games 2003. He was found guilty by the High Court on May 20, 2005, and given a 16-year prison term. The appellant appealed to the court of Appeal because he was aggrieved with the High Court's ruling. The High Court's decision and the Court of Appeal's sentencing were upheld upon further appeal to the Supreme Court, which dismissed the appellant's appeal while upholding the original rulings.

Due to the proliferation of Internet Service Providers (ISPs) and Cybercafés, Nigeria's telecommunications usage and internet penetration increased dramatically following the liberalization of the country's telecoms industry in the late 1990s. As a result, cybercriminals began using the internet to commit crimes rather than normal mail and fax. [75] Nigeria, one of the nations with the highest rates of cybercrime perpetration in the world, has been identified as a key worldwide hub of cybercriminal activity by both international and domestic reports. The Nigerian government became concerned about how fraudsters were abusing cyberspace, and as a result of this concern, a Presidential committee was established in 2003, followed by other initiatives to look into these fraudsters' online activities and create a legal and regulatory framework to combat the threat of cybercrime. Unfortunately, it took the Nigerian government more than ten years to implement a legal and regulatory framework for cybercrime after becoming aware of the serious negative effects it could have on national economic development, national security, relations with other countries, as well as human rights and human security.
Uptil 2015, Nigeria didn't have any laws that were particularly designed to outlaw and penalize cybercrime. The Nigerian Cybercrime (Prohibition, Prevention, etc.) Act 2015 was enacted by the former President Goodluck Ebele Jonathan[76] in an effort to combat the scourge of cybercrimes in Nigeria. It should be highlighted that the aforementioned law is the first legislative and regulatory framework for cybercrime in Nigeria that has been implemented to control people's activities online. The explanatory note and aim of the Act demonstrate the deterrence theory of punishment and capture the genuine and express intention of the Act.

It is crucial to remember that previous laws existed before the Cybercrime Act of 2015 was signed into law. These laws dealt with situations that may be interpreted to contain cybercrime and attempted, albeit ineffectively, to reduce it. These laws comprise: Economic and Financial

[73]Criminal Code Act Cap. 38, Laws of the Federation of Nigeria.
[74]*Mike Amadi v. Federal Republic of Nigeria* (2008) 12 SC (pt.III) 55 or 36.2 NSCQR 1127. See also *Harrison Odiawa v. Federal Republic of Nigeria* (2003–2010) ECLR 19–99; (2008) All FWLR(pt.439)436;(2008)LPELR-CA/L/124/2006.
[75]The Internet Crime Complaint Center 2003 Internet Fraud Report: January 1, 2003-December 31, 2003 p.9. <http://www.ic3.gov/media/annualreport/2003 _IC3Report.pdf> accessed 18 December 2021.
[76]Punch Newspapers, May 16, 2015.

Crimes Commission (Establishment) Act,[77] Nigeria Criminal Code Act[78] and Advance Fee Fraud and other Related Offences Act,[79]e.t.c. It must be made abundantly apparent that the 2015 Cybercrime Act was enacted as a result of the failure of the previously mentioned laws to address the threat of cybercrime in Nigeria.

The Cybercrime Act of 2015, according to one researcher, was crafted in an inelegant manner since it omitted some key components that can help prosecutors successfully prosecute hackers. The Act, for instance, lacks a futuristic quality because certain offences, such as "Online Publishing Fraud," were not included by it.

The researchers also believed that a prosecutor pursuing an online publishing fraud case against a defendant will simply be on an exploratory journey because it is axiomatically true that no one can be held accountable for an unwritten crime. [80] Cybercrime is an international problem that transcends national borders. Businesses and customers are more at risk from criminals' reach as networked communications and e-commerce spread around the globe. Criminals may conceal their identities, carry out their crimes remotely from any location, and connect with their allies globally thanks to the internet's global reach. Any sort of crime, including violent crime, terrorism, and drug trafficking, as well as the distribution of child pornography, the appropriation of stolen intellectual property, and assaults on online retailers, might involve this. [81]
In four ways, cybercrimes are different from traditional crimes: [82]

1. They readily make decisions;
2. Compared to the potential damage, they only require a limited quantity of resources;
3. They may be committed in any jurisdiction without the offender being required to be present, and
4. They are frequently difficult to categorize as criminals.

Cybercriminals can conduct assaults on people and companies from the comfort of their own homes and from any location in the world. [83] To commit a cybercrime, all a criminal needs is a computer and a modern device that is connected to the internet. It is obvious that committing a crime online is more effective than doing so offline. An identity theft case is a good illustration of this; via the internet, identity thieves may swiftly access the personal information of several people, as well as high-quality phony identification documents (such as licenses, birth certificates, social security cards, and others). [84]

The opportunity to conduct crimes online utilizing scarce resources is immense. [85] Criminal activity is made simple with the aid of computers, computer networks, and related information and communications technology. It is amazing that a thief " can steal more with computers than with a rifle" and "can wreak more harm with a keyboard than with a bomb." [86]
The "Denial of Service Attacks" in February 2000, which temporarily caused severe interruptions to the popular Internet commerce sites like Yahoo, CNN, and E-Bay and forced their closure, are perhaps the most egregious example. [87]

---

[77]Cap. E1, LFN, 2004, hereinafter referred to as EFCC Act.
[78]Cap. C38 LFN, 2004, hereinafter referred to as Criminal Code Act.
[79]Cap A6 LFN 2004, hereinafter referred to as Advance Fee Fraud.
[80]*Aoko v. Fagbemi* note 18 above.
[81]CNN, "Lessons of Love Virus still sinking in …", <http:// news. com. com/ lessons+ of+ love+ virus+ still/2100 3-257095-html>accessed 6 December 2021.
[82]Wall; D note 4 above.
[83]Ferrera, DF *et al, Cyberlaw: Text and Cases* (2001) 298.
[84]Lutkevich B, "Identity Theft", (June, 2020) <What is Identity Theft and How to Prevent it? (techtarget.com>accessed 17 November 2021.
[85]'National Research Council 'Computer at Risk' (1991) <http:// news. com. com/ lessons+ of+ love+ virus+ still/2100 3-257095-html>accessed 22 December, 2021.
[86]Wall, D note 4 above
[87]The President of Cyber Security Experts Association of Nigeria (CSEAN), Remi Afon, in his opening remark stated that there are two significant events that happened this year that

Another such example is the short-lived but destructive "Love Bug" virus that infected thousands of collaborative websites worldwide in May 2000; many businesses were forced to shut down their email systems to block the infection's spread. [88]

Cybercrime, in contrast to traditional crime, does not necessitate any kind of immediate physical contact between the victim and the perpetrator. Cybercrime is a crime without boundaries and without borders. It may be perpetrated against a victim who resides in another city, state, or nation by a person who is anywhere in the world.
The only thing the offender needs is access to a computer with internet connectivity; with this, he can directly cause "damage" to someone by assaulting their computer, or indirectly, by collecting information that allows him to take their identity and exploit it to commit large-scale fraud. [89]

Since a criminal need not be physically present in a country to perpetrate a cybercrime, crime is not restricted by jurisdictional lines in the networked world. Cybercrime is particularly alluring to criminal behaviour since it can be committed against any "computer" user worldwide and from anywhere. It is possible for a criminal to conduct crimes across international borders while maintaining some anonymity, and it is more challenging to locate the crime scene. In the digital world, it may be nearly impossible to track down and identify a, as this may require international cooperation. [90]
The spread of the "Love Bug" virus, which affected more than twenty nations, shows how simple it might be to carry out cybercrimes internationally. Additionally, most nations lack the legal framework necessary to punish cybercrimes, therefore they cannot be covered by the current legislation. [91] In internet, antiquated laws frequently place crime and punishment as distant cousins.
Cybercrime cannot be prosecuted according to the usual categorisation of offences under existing common law. An illustration of this is a denial of service attack, which, despite being a malevolent act that may cause the victim's ability to conduct business to be damaged or even destroyed, cannot be punished as vandalism, trespass, burglary, theft, arson, or extortion. [92]

8. CONCLUSION

It is imperative to examine the incidence and consequences of cybercrime. Nigeria's government, people, system, and approach must all demonstrate a commitment to the need to end cybercrime there. Therefore, in this regard, we advise spreading awareness of the dangers of cybercrime among the general public.
Resources, training, and all other required measures must be put in place to ensure that cybercrime and its effects are diminished, if not entirely eliminated.

REFERENCES

Akogwu, S "An Assessment of the Level of Awareness on Cybercrime among Internet users", (2012) Ahmadu Bello University, Zaria.
Advance Fee Fraud. Cap A6 LFN 2004.
Anah, BH "Cybercrimes in Nigeria: Causes, Effects and the Way Out"; (August 2012) Vol2. NO.7. *AREN Journal of Science and Technology* 626.
Ani: L "Cybercrime and National Security: The Role of the Penal and Procedural Law" (2011) <http://www.ejournalofscience.org> accessed 8 December 2021.
Ankur J. Cybercrime: Nature, Elements and Types (2019), 2 (2) *National* Journal of Cyber Security Law at 1-5.
Aoko v. Fagbemi(1961) 1 ALL N. L. R. 400.

have actually impacted Cyber security awareness. One is global, which is the COVID-19 pandemic, and the other is local, which is the #EndSARS protest. See The Guardian Newspapers on the 2nd ofNovember, 2020.

[88]Geoff, W "Love Bug's creator tracked down to repair shop in Manila". BBC News (2 May 2020).
[89]*Ibid*.
[90] Jonathan C; *Principles of Cybercrime* 1st Edition, (UK; Cambridge Press, , 2018) 34.
[91]CNN.com retrieved 10/4/2019.
[92]Brenner note 2 above.

Atherton M., "Criminals Switch Attention from Cheques and Plastic to Internet Transactions", *The Sunday Times* March 10, 2010.
Awe "Fighting Cybercrime in Nigeria", (2008) 26 (5), *the Electronic Library* 716-725.
Brenner SW, "Cybercrime Investigation and Prosecution: the Role of Penal Procedural Law". (2012) Murdoch University Electronic Journal of Law <(austlii.edu.au) http://www5.austlii.edu.au/au/journals/MurU/2001/8.html> accessed 18 October, 2021.
Carter D., "Computer Crime Categories", *FBI Law Enforcement Journal,* Vol. 64, NO. 21 (1995) R.271.
CNN, "Lessons of Love Virus still sinking in …", <http://news.com.com/lessons+of+love+virus+still/2100 3-257095-html>accessed 6 December 2021.
Conley C.H, "CyberCrime" NIJ Reports, Vol. 6 No. 218 (1990) 3.
Council of Europe Cybercrime Convention, 2004.
Criminal Code Act C38 LFN, 2004.
Cybercrime (Prohibition, Prevention, Etc.) Act, 2015.
Debra LS "Scene of the Cybercrime; Computer Forensics Handbook"<http://www.syngress.com/catalog/?pid. 2250>accessed 10 November 2021.
Duggal, ShriPavan'Cyber Assault and Cybercrime' (August, 2009).<http://Cyber laws.net/cyberindia/cyberas sault.htm>accessed 3 December , 2021.
Economic Financial Crimes Commission Act (EFCC Act). Cap. E1, LFN, 2004.
EFCC/NBS/(2009), (2010) Business Survey on Crime & Corruption and Awareness of EFCC in Nigeria, Summary Report.
Farlex, "The Free Dictionary", (2014) <www.thefreedictionary.com>accessed 18 December, 2021.
Farmer, L "Crime Definitions" in Cane and Conoghan (ed). *The New Oxford Companion to Law*, (UK: OxfordUniversity Press 2008) 263.
Ferrera, DF *et al, Cyberlaw: Text and Cases* (2001) 298.
Garner,BA Black's Law Dictionary 9th ed., (USA: West Publishing Co., 2009) 427.
Geoff, W "Love Bug's creator tracked down to repair shop in Manila". BBC News (2 May 2020).
Girasa, RJ *Cyber Law: National and International Perspectives* 1st Edition **(**New Jersey**:** Prentice Hall Publishers, 2001) 54.
Harrison Odiawa v. Federal Republic of Nigeria (2003–2010) ECLR 19–99; (2008) All FWLR (pt.439) 436; (2008) LPELR-CA/L/124/2006.
Herman, TT "*Ethics and Technology, Ethical Issue in an Age of Information and CommunicationTechnology"***,**2nd Edition (USA: John Wiley & sons Inc, 2005) 202.
Johnson, J "African: number of Internet Users in Selected Countries 2020" (25 May, 2021) <http://www.internetworldstats.com .com/stats1.htm> accessed 7 September 2021.
Jonathan C; *Principles of Cybercrime* 1st Edition, (UK; Cambridge Press, , 2018) 34.
Lutkevich B, "Identity Theft", (June, 2020) <What is Identity Theft and How to Prevent it? (techtarget.com>accessed 17 November 2021.
Meke, ESN: "Urbanization and Cyber Crime in Nigeria: Causes and Consequence" (2019) 34(12) *NDIC Quarterly* 34.
Mike Amadi v. Federal Republic of Nigeria (2008) 12 SC (pt.III) 55 or 36.2 NSCQR 1127.
'National Research Council 'Computer at Risk' (1991) <http://news.com.com/lessons+of+love+virus+still/2100 3-257095-html>accessed 22 December, 2021.
Obanyi, K *CyberCrime Law in Nigeria – Principles and Strategies* (USA. Charleston, SC, 2015) 6.
Obono, M "Cybercrimes: Effect on Youth Development", (2008) <http://www.i-genius.org>assessed 30 December, 2021.
Okunma, EN "Criticism: Cybercrime Bill", 2013, University of Witwatersrand Johannesburg South Africa 95
Ologbodi, K "Fighting Cybercrime in Nigeria" (2010<http//guide2nigeria.com/news_articles_About_Nigeria> accessed 13 November 2021.
Perera, R. "Transfer of fund" CNN.com. Nov. 26, 2000. Feb. 27, 2001 at 1.
*S v. Douvenga*case no 111/150/2003.
Stieg, C "Steve Wozniak: When Apple got 'big money' Steve Jobs personality Changed' (February, 6, 2020).
Talwant S., 'District and Sessions Judge', *Cyber Law & Technology*, Delhi- India. 67.
The Internet Crime Complaint Center 2003 Internet Fraud Report: January 1, 2003-December 31, 2003 p.9. <http://www.ic3.gov/media/annualreport/2003 _IC3Report.pdf> accessed 18 December 2021.
The Nigerian Cybercrime (Prohibition and Prevention, etc) Act, 2015.
Trade Union and Labour Relations (Consolidated) Act 1992 and by theschedule to the Prevention of Crimes Act 1871.
United States v. Lee 15 Johns 484 (N.V. 18177) 1998.
United States v. Morris (1991) 928 F. 2d 504
Victor T & Olumide, O "E-crime in Nigeria; Trends, Tricks and Treatment"(2005) <www.Openj.gate/search/ searchresults/articles> accessed 27 October 2021.
Wall D *The Transformation of Crime in the Information Age* 1stEdition (USA; Harvard University Press, 2007) 43.