JILS (JOURNAL *of* INDONESIAN LEGAL STUDIES)
NATIONALLY ACCREDITED JOURNAL (SINTA 2)
Published by Faculty of Law, Universitas Negeri Semarang, Indonesia
Volume 5 Issue2, November 2020 ■ ISSN (Print) 2548-1584 ISSN (Online) 2548-1592

RESEARCH ARTICLE

CYBER CRIME MANAGEMENT AMONG STUDENTS

An Evaluation of Legal Correlates of Cyber Crime Management among Tertiary Institutions Students in Nigeria (A Case Study of Delta State)

Ngboawaji Daniel Nte[1], Urowayinor Kelita Esq[2], Bribena Kelvin Enokie[3], Onyeka Bienose[4]✉
[1, 2] Dept. of Intelligence & Security Studies, Novena University, Nigeria
[3] Faculty of Law, Niger Delta University, Nigeria
[4] Global Intelligence, Peace and Security Institute, Nigeria

✉ bienoseonyeks@gmail.com

Submitted: March 7, 2020 **Revised**: June 12, 2020 **Accepted**: October 20, 2020

ABSTRACT

This study investigated examined the legal correlates of cybercrime management amongst higher institution students in Nigeria with special reference to some selected tertiary institutions in Delta State, Nigeria. A correlation approach of survey research design was adopted in this study. In order to address the problem of this study, seven research questions were raised and seven research hypotheses were formulated and tested at a .05 level of significance. This study revealed that the law can provide solutions to Cyber Crime management in Nigeria. Poverty is a factor responsible for cybercrime in Nigeria. The law can promote intellectual property and ensure privacy rights. There are existing laws that adequately address challenges relating to cybercrimes. The study revealed that youths who are mostly male are the major perpetrator of cyber-crimes and the crime can be committed at any time of the day. The study found that

unemployment, poverty, absence of effectual law, and corruption are the major causes of cyber-crime in the study area. Based on the findings of this study, it was therefore recommended that collective vigilance detect and report to law enforcement agencies anyone suspected to be involved in cyber-crime. The Federal Government should empower the youths in terms of job creation and regularly engage the IT organizations to develop strategies to curtail cyber-crime.

Keywords: Law; Cyber-crime; Cyber-crime Management; Nigeria; Higher Institutions

TABLE OF CONTENTS

Copyright © 2020 by Author(s)
This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License. **All writings published in this journal are personal views of the authors and do not represent the views of this journal and the author's affiliated institutions.**

HOW TO CITE:
Nte, N. D., Esq, U. K., Enokie, B. K., & Bienose, O. (2020). Cyber Crime Management among Students. *JILS (Journal of Indonesian Legal Studies)*, 5(2), 295-334. https://doi.org/10.15294/jils.v5i2.34005

INTRODUCTION

With the profound advancement of technology in this 21st century, the world has now become more or less a digital world. Technology has brought together nations and the world has now become a global village. The economy of most nations in the world is accessible through the aid of

electronic via the internet.[1] 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. Currently, there are nearly 2 billion internet users and over 5 billion mobile phone connections worldwide. According to a report given by the International Telecommunications Union (ITU), as at 2011, there were more than 45 million internet users in Nigeria, which is 26.5% of the population.[2]

The economic activities and national security depend largely on a secured cyberspace. Through cyberspace, one is able to communicate with virtually everyone in the world and economic transactions have now become relatively easier. Goods and services are routinely purchased and delivered electronically leading to significant changes in industries like journalism, travel and banking. Notwithstanding these advantages, it is through this same cyberspace that the economy, privacy and social interactions have become unsecured. The growing convenience of the cyberspace comes at a cost.

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.[3] The flourishing connection between organized crimes and the internet has increased the insecurity of the digital world. The arrival of the internet has been pointed as the remote cause for lots of ingenious crimes hitherto unknown to our criminal law like the online credit card scheme. Some scholars have interestingly argued that 'in the internet nobody knows you are a dog'. Internet connected activities are susceptible to crime and can lead to victimization as effectively as common physical crime.

As a result of this development, criminal and other harmful acts aimed at computers – so called 'cyber-crimes' are on the rise. Crimes like online fraud and hacking attacks are just some example of cybercrimes that

---

1 A. AJEWOLE, *Curbing Cybercrime in Nigeria. Fighting the Masked Enemy and Promoting Productive Alternative for the Youth* 2010 [hereinafter as AJEWOLE]; F. OYESANYA, *Nigerian Internet 419 On The Loose* 2004 [hereinafter as OYESANYA]; A.S. OYEWOLE & A. OBETA, *An Introduction to Cyber Crime* 2002 [hereinafter as OYEWOLE & OBETA].

2 *Id.*, at. 57; O. AYANTOKUN, *Fighting Cyber-Crime in Nigeria, Information-System*, 2006 [hereinafter as AYONTAKUN]; R. IMHOF, *CYBERCRIME AND TELECOMMUNICATION LAW*, 115-117 (Rochester Institute of Technology USA, Information and Communication Technology, 2010).

3 D. MORLEY, and C. S. PARKER, *UNDERSTANDING COMPUTERS, TODAY AND TOMORROW* 312-313 (11th Edition, Published by Thomson Course Technology, USA, 2007) [hereinafter as MORLEY & PARKER].

are committed in a very large form every day. The internet has now created a fertile ground for false pretences, fraud and other fraud related crime. And one reason why the issue of cybercrime remains challenging is the constant technical development, and also the changing means and ways in which the offences are committed. Cybercrimes have been described as one of the fastest growing criminal activities on the planet. Cybercrimes 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.[4]

In Nigeria today, 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. Some perpetrators of the online fraud in Nigeria usually referred to as 'yahoo boys' are taking advantage of e-commerce system available on the internet to defraud unsuspected victims. To underscore the high rate of cybercrime in Nigeria, Nigeria is the third jurisdiction after China and United States of America, where the world records the highest number of cybercrimes. The increasing rates of cybercrime in the society have now become a strong threat to Nigeria's e-commerce growth and the security of Nigeria as a whole. Thus, giving rise to the imperative need for a very efficient legal framework on cybercrimes in Nigeria.[5]

The law provides rights and duties and defines crimes such as cybercrimes and punishment or provides for establishments of institutions etc. or procedural law which provides mechanism for enforcement of such rights/ duties or how to enforce laws that bother on cybercrimes. Cybercrime on the other hand involves a reference to a crime related to the cyberspace, computers, computer networks and the internet.[6]

---

4 AJEWOLE, *supra note* 1, at. 58; MORLEY & PARKER, *supra note* 3.

5 A. A. AHMED, *HACK NO MORE, INTERNET SECURITY: ATTACKS AND* DEFENCE 71 (Ahmadu Bello University Press Limited, Nigeria, 2010); K. KUMAR, *CYBER LAWS, INTERNATIONAL PROPERTY AND E-COMMERCE* SECURITY 74-76 (Dominant Publishers and Distributors, New Delhi, 2003); T. SALIHU, Impact of Computer Appreciation in Military Technology, *A Commandant's Paper submitted to Nigerian Army School of Military Police, Nigeria,* (School of Postgraduate Studies, 2006); G. SESAN, *The New Security War*, 2010.

6 McConnell, *Cybercrime and Punishment*, ARCHAIC LAWS THREATEN GLOBAL INFORMATION (2010); MORLEY & PARKER, *supra note* 3.

Cybercrimes include: various conducts relating to the use of computers in criminal behaviour, including conduct relating to the obtaining and communicating of restricted information; the unauthorized accessing of information from financial institutions, the Nigerian government, and "protected computers"; the unauthorized accessing of a government computer; fraud; the damaging of a protected computer resulting in certain types of specified harm; trafficking in pass words; and extortionate threats to cause damage to a "protected computer".[7]

Until 15th May 2015, when the Nigerian Cybercrime Act 2015 was signed into law, there was no specific adjectival law on cybercrime in Nigeria. The situation was like the Philippines' in 2000 when the 'Love Bug virus' spread throughout the world, and the suspect could not be effectively prosecuted due to the lacunae in the Philippines' cyber-criminal legislation. The only relevant legislation was municipal laws, like the Economic and Financial Crimes Commission Act, the Criminal Code (as applicable in the southern Nigeria) and Penal Code (which is operational in the northern Nigeria). Unfortunately, this traditional legislation had little or less to offer in respect of cyber-related offences. This made it almost impossible to secure convictions on offences relating to cybercrime in Nigeria, except in the few situations where confessional statements are extracted from the offenders by the investigating officers and/or prosecution.

Nigerian Cybercrime Act 2015 provides an effective, unified and comprehensive legal, regulatory and institutional Framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. This Act also ensures the protection of critical national information infrastructure, and promotes cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.[8]

Laws on cybercrime became necessary considering the fact that cybercrime has become one of the great legal frontiers in Nigeria and the world over. Between 2000 and 2012, the internet expanded at an average rate of 566.4% on a global level, while an estimated 2.4 billion people are "on the Net", six trillion web pages are accessible, 2.2 billion Google searches per month and 12% of all global trade happens online, with about

---

7 AYANTOKUN, *supra note* 2.

8 K. HIDAYATULLAH, K *Cyber Crime and Its Consequences*, (National Law University Raipur, Chhattisgarh, New Raipur, 2000); McConnell, *supra note* 6, at. 15.

$240 million lost from global cyber-crime. In other words, the rapid growth of computer technology carries with it the evolution of various crimes on the internet.

In recent years, there has been considerable focus within the criminal justice system on computer-related crime, as cybercrime has garnered increased attention because computers have become so central to several areas of social activity connected to everyday life. Internet users especially those in tertiary institutions in Delta State, Nigeria innovate freely on various platforms, reaching out to more people, aiding ubiquity of internet features and with attendant high utility and pecuniary returns.[9]

Although the internet has been a double-edged sword providing opportunities for individuals and organizations, it brings with it an increased information security risk. Cybercrime has in recent time become a crucial threat to many countries including Nigeria which has necessitated many governments from around the world to enact sturdy legislation and also put in place coherent procedural measures to tackle cyber-criminals; which involve putting effective task forces, efficient legislation and tough sentencing regimes in place for those convicted of acts involving cybercrime. It is a truism that the cyber world has no definite territorial boundaries; it is not restricted to Local Government or States in Nigeria. Cybercrime offences know no limits to physical geographic boundaries and have continued to create unprecedented issues regarding to the feasibility and legitimacy of applying traditional legislations based on geographic boundaries. These offences also come with procedural issues of enforcement of the existing legislations and continue to subject nations with problems unprecedented to its sovereignty and jurisdictions.[10]

In Nigeria today, numerous internets assisted crimes are committed daily in tertiary institutions in Delta State, Nigerian various forms such as identity theft, desktop counterfeiting, internet chat room, cyber harassment, fraudulent electronic mails, Automated Teller Machine spoofing, pornography, piracy, hacking, phishing, and spamming. Usually, these crimes are committed in forms like sending of fraudulent and bogus

---

[9] For further reading, please also see E. ROGER, E. *Diffusion of Innovation*, 1995; M. K. ROGERS M.K., *A SOCIAL LEARNING THEORY AND MORAL DISENGAGEMENT ANALYSIS OF CRIMINAL COMPUTER BEHAVIOUR. AN EXPLORATORY STUDY*, (University of Manitoba, Winnipeg, Manitoba, 2010).

[10] J. R. FISCHER, E. HALIBOZEK, & G. GREEN, *INTRODUCTION TO SECURITY* 229-441 (Linacre House, Jordan Hill, Oxford, 2008).

financial proposals from cyber criminals to innocent internet users. The increasing rates of cyber crime in Nigeria today have become a strong threat to the country's e-commerce growth and has led to ill- reputation intentionally and consequently denied some innocent Nigerians certain opportunities abroad.[11]

In the further context, cyberspace has provided a safe haven for internet platform, which has created geometric growth and accelerated windows of opportunities for businesses and the removal of economic barriers hitherto faced by nations of the world. People from diverse areas of human endeavor can now freely access and utilize the advantages offered by internet platform.[12] In addition, the internet has brought some positive impact to the world such as facilitation of job search and employment, accessibility to research information for education and businesses, rural integration, enhancement of trade and commerce, sharing of resources and ideas, and enhance communication. [13]

Considering the limitless advantages of the internet, one can easily subscribe to the fact that it is an important tool for national development in a developing country like Nigeria. However, despite the development trend associated with the internet, it has brought about a new wave of crime which is threatening the social order in the society. The internet online services, which are ordinarily supposed to be blessings as they exposes one to a lot of opportunities in various field of life are fast becoming sources of discomfort and worry due to the atrocity being perpetrated through it. Cybercrimes cover a wide range of illegal activities on the cyber space by individuals in tertiary institutions in Delta State.

Cyber-crime simply means the use of computers and internet as tools to conduct criminal activity such as financial fraud, identity theft, phishing and copyright violations amongst others. Some individuals in Nigeria have embraced cyber-crime as a way of life. Many have become rich

---

[11] AHMED, *supra note* 5; E.J. AGHATISE, *Cyber-crime Definition*, Computer Crime Research Centre 2006. For comprehensive and comparative reading, please also see KUMAR, *supra note* 5; P. PATI *Cybercrime*, 2003; PLANETINDIA, *Introduction to Cyber Crime*, 2001.

[12] O.R. EHIMEN, & A. BOLA, *Cybercrime in Nigeria*, 3 BUSINESS INTELLIGENCE J. 85, 98-99; F.F. AKANDE, *ISSUE IN HUMANITIES AND TECHNOLOGY*, (Integrity Publication, Ilorin, 2007).

[13] M. YAR, *CYBERCRIME AND SOCIETY*, (London, Sage Publication Ltd, 2006). Also see Young Media Association, *The Internet: Benefits, Danger and strategies*. Australia Young Association, 2007.

while some others have been caught by the law. [14]This new crime is denting and drilling holes in the economy of the nation. For example, in a recent report by the Internet Crime Complaint Center which is a partnership between the FBI and America's National White Collar Crime Center, revealed that Nigeria now ranked third among the list of top ten sources of cybercrime in the world.[15]

Also, the Central Bank of Nigeria (CBN) in its banking sector supervision report revealed that the Nigeria banking sector lost 7.2 billion naira to internet fraud.[16] Losing 7.2 billion naira in a developing economy such as ours is not something to be proud about. Apart from the destruction cyber-crime does to the economy, it also is leads to the erosion of confidence in genuine Nigerian commercial credibility and today many western countries with France taking the lead have moved to deny Nigerian businessmen and women who are legitimate the rewards of e-commerce. France today requires web camera verification for most online business transactions from Nigeria.[17]

This study therefore examines the correlates of the Nigerian legal system and the challenges of cybercrime management in Nigeria with special reference to tertiary institutions in Delta State, Nigeria. Tertiary institutions include universities, polytechnics, colleges of education and colleges of technology. In most tertiary institutions in Delta State, Nigeria, various form of crimes are being witnessed ranging from examination malpractices, falsification of admission, rape, robbery and stealing, sexual abuse, assault, cultism amongst others. But in recent time cyber-crime, a new form of crime now exists in tertiary institutions in Delta State, Nigeria. Students of tertiary institution now engage in cloning of websites, false representations, internet purchase and other e-commerce kinds of fraud such as credit card fraud. It is for this reason, that this study is conceived to examine legislative drafting and the challenges of cybercrime

---

[14] O. TADE, & I. ALIYU, *Social Organization of Internet fraud among University Undergraduates in Nigeria*, 5 *INTL J. CYBER CRIM*, 860, 860-875 (2011).

[15] S. M. ABDULHAMID, HARUNA C., & A. ABUBAKAR, *Cybercrimes and the Nigeria Academic Institution Networks*, 7 *THE IUP JOURNAL OF INFORMATION TECHNOLOGY* 1, 11-12 (2011); Internet Crime Complaint Center, *Internet crime report*, 2010.

[16] AJEWOLE, *supra note* 1.

[17] O.S. LONGE & S. C. CHIEMEKE, *Cyber Crime and Criminality in Nigeria. What Roles are Internet Access Points in Playing?* 6 *EUROPEAN JOURNAL SOCIAL* SCIENCES 127, 132-139 (2008); KUMAR, *supra note* 5.

management in Nigeria with special reference to tertiary institutions in Delta State, Nigeria and to suggest possible solutions to the identified challenges.[18]

Although the internet has been a double-edged sword providing opportunities for individual, tertiary institutions in Delta State, Nigeria and other organizations, it brings with it an increased information security risk. Cybercrime has in recent time become a crucial threat to many tertiary institutions in Delta State, Nigeria which has necessitated many Federal Government to enact Nigerian Cybercrime Act 2015 and also put in place coherent procedural measures to tackle cyber-criminals in Nigeria; which involve putting effective task forces, there is however the need for Federal Government to initiate more strategies to curb the menace of cybercrime which threatens the security of businesses, tertiary institutions in Delta State, Nigeria.

Nigeria is not the only Nation where cybercrimes are being perpetrated. The incident can rightly be said to be on the increase in the country due to lack of security awareness and under reportage respectively. Although some undergraduate and post graduates students' level of knowledge of the internet is observably just for chatting with their friends and may be get information there from, most of them may not be in the position to protect their data or information and computer from malicious, programmers.

The contribution of internet to the development of the nation Nigeria especially the tertiary institutions in Delta State, Nigeria has been marred by the evolution of new waves of Cybercrime. The internet has also become an environment where the most lucrative and safest crime thrives.

Internet has become a stubborn mouth sore which causes us a lot of pain and shame because criminally minded individuals in tertiary institutions in Delta State and the country at large are stealing and committing atrocity through the aid of the internet online business transactions. The undergraduate and post graduates students in tertiary institutions in Delta State, Nigeria who are mostly youths in every society is of great importance and concern to that society because they are looked

[18] N. RIBADU, Cybercrime and Commercial Fraud: A Nigerian Perspective, *A paper presentation at the Modern Law for Global Commerce*, Vienna 9-12 July 2007; KUMAR, *supra note* 5, ABU, REGULATIONS GOVERNING HIGHER DEGREE STUDIES, NIGERIA (ABU Press Limited, Nigeria, 2010).

upon as the leaders of tomorrow. Olaide & Adewole observed that a sizeable number of criminals in tertiary institutions in Delta State, Nigeria fall within the youthful age as earlier stated. The undergraduate and post graduates students in Delta State, Nigeria at present have discovered different ways of using the internet in doing different types of criminal activities and these age brackets are also found in other tertiary institutions in Nigeria.[19]

Concerted attempts to address cybercrime by various governments and international organizations have not been successful owing to the fact that the identities of the perpetrators of this crime have often remained inadequate. A study by Zero Tolerance indicates that cybercriminals are usually within the age of 18 and 30 years and they indulge in the crime in order to survive and have a taste of good life. Noting these observations, there is need to identify more attributes these cyber criminals possess and identify other motivating factors since it have been acknowledged that a good taste of life is a major factor.[20]

According to Vladimir internet is a global network which unites millions of computer. The contribution of internet to the development of the nation has been marred by the evolution of a new wave of crime.[21] The internet has also become an environment where the most lucrative and safest crimes thrive. There are indications that cyber-crime is rising. For example, a 2005 YouGov poll of UK Internet users found that 1 in 20 had lost money in online scams. Also a 2001 survey revealed that 52 per cent of companies interviewed said internet fraud posed real problems for them.[22] These are clear indications that cyber-crime is on the increase and as such, it is beginning to gain recognition at the global level and there is dearth of study in the area of this burgeoning criminal act in Nigeria.

The internet create unlimited opportunities for commercial, social and educational activities, however, it has introduced its own peculiar risks that pose danger to the economy. This danger could affect many sectors of the society and put the development of the country into peril. Some of

---

[19] M. OLAIDE, & R. ADEWOLE, *Cyber Crime Embarrassing for Victims*, 2004.

[20] Zero Tolerance, *The Portrait of a Yahoo Boy*, 1 ECONOMIC AND FINANCIAL CRIME COMMISSION 36, 38-39 (2006).

[21] G. VLADIMIR, *International Cooperation in Fighting Cyber Crime, 2005;* D.S. WALL, D.S, CRIME AND THE INTERNET, London Routledge Publisher, 2005) [hereinafter as WALL, 2005].

[22] D. S. WALL, D.S, CYBERCRIME: THE TRANSFORMATION OF CRIME IN THE INFORMATION AGE, (Polity Press, Cambridge, UK, 2007) [hereinafter as WALL, 2008].

these possible adverse effects could include the destruction of the country's image both at home and abroad, insecurity of both life and properties, fear of doing business with Nigerian's citizen, economic loss of spending substantial amount of money on the prevention and control of cybercrime amongst others.[23] For example, a survey on cyber-crime conducted in 2001 by Confederation of British Industry (CBI) and other parties including Price water house Coopers, states that cyber-crime could hinder the growth of e-business because it makes people to be.[24] In essence, what other menace does cyber-crime poses to the society.

Consequently, many countries have intensified efforts in curbing the excesses of cyber-criminals. Nevertheless, efforts have been made by the Federal Government of Nigeria to curb the menace of the crime too. For instance, according to Awe,[25] the government of President Olusegun Obansanjo in 2003 set up a working group known as the Nigeria Cyber Crime Working Group (NCWG) to address this phenomenon since the loss suffered by both consumers and investors creates serious credibility and image problem to the country. Similarly, according to Abdulhamid et al, in Nigeria, a bill title "Cyber Security and Critical Infrastructure bill" is presently been prepared to deal specifically with the menace of cyber-crime.[26]

The Economic and other Financial Crime Commission (EFCC) and the Nigerian Police Force (NPF) have also played vital roles in curbing this menace.[27] To support their efforts, Microsoft and other internet related organizations like PARADIGM Initiative Nigeria, Background Check International (BCI) and the Internet safety, Security and Privacy Initiative for Nigeria (ISSPIN) have also assisted to curb the maladies (Awe, 2009).[28] In spite of all these efforts, cyber-crime in tertiary institutions in Delta State, Nigeria is still on the increase. The situation raises a question on the

---

[23] A.B. DAMBAZAU, M.M. JUMARE, & A. M. YAKUBU, A.M, *ISSUES IN CRIME PREVENTION AND CONTROL IN NIGERIA*, (Baraka Press and Publishers Ltd Kaduna, Nigeria, 1996).

[24] R.G. BROADHURST & and P.N. GRABOSKY, *CYBER-CRIME: THE CHALLENGE IN ASIA* 15-81, (Hong Kong University Press, Hong Kong, 2005).

[25] J. AWE, *Fighting Cybercrime in Nigeria*, 2009.

[26] ABDULHAMID, HARUNA, & ABUBAKAR, *supra note* 15, at. 11; S. McQuade, S., *THE ENCYCLOPEDIA OF CYBERCRIME*, (Green Wood Press, Westpoint Connecticut, London, 2009).

[27] E.F. OGBUNWEZEH, E.F., *EFCC and Cybercrime The True Lesson*, 2006.

[28] AWE, *supra note* 5. See also J. UMAR-AJIJOLA, *Microsoft Combats Cybercrime in Nigeria*, 2010a. J. UMAR-AJIJOLA, *Fighting Cybercrime in Nigeria*, 2010b.

place of the law in curbing cybercrime in Nigeria, the challenges of cybercrime management in Nigeria, the type of cyber-crime that is on the increase in tertiary institutions in Delta State, Nigeria and remedy to solve the menace. Consequently, the research work was designed to provide answers to the research questions raised and also to suggest solutions to the challenges of cybercrime management in Nigeria.

METHOD

I. OBJECTIVES OF THE STUDY

The main aim of this study is to examine the law and crime management in Nigeria. The specific objectives of this study therefore are:

1. To determine the provisions of the Nigerian Cybercrime ACT 2015
2. To determine the causes of Cyber Crime in Nigeria
3. To determine the Types of Cyber Crime often committed by individuals in tertiary institutions in Delta State, Nigeria
4. To determine the consequences of Cyber-Crime in Nigeria
5. To determine the relevance of Nigerian Cybercrime ACT 2015?
6. To determine the challenges of cybercrime management in Nigeria
7. To suggest appropriate solutions to the challenges of cybercrime management in Nigeria.

II. RESEARCH HYPOTHESES

This study in the quest of finding solution to the menace of cybercrime in Nigeria, seek to test the following research hypotheses:

1) H0: The law cannot provide solution to Cyber Crime management in Nigeria.
   H1: The law can provide solution to Cyber Crime management in Nigeria.
2) H0: Poverty is not a factor responsible for cybercrime in Nigeria.
   H1: Poverty is a factor responsible for cybercrime in Nigeria.
3) H0: The law cannot promote intellectual property and ensure privacy rights.

H1: The law can promote intellectual property and ensure privacy rights.

4) HO: The law does not provide mechanism for the enforcement of the rights, duties and laws that bother on cybercrimes.
   H1: The law does provide mechanism for the enforcement of the rights, duties and laws that bother on cybercrimes.
5) HO: Cybercrime does not consists of various conducts (communicating of restricted information; the unauthorized accessing of information from financial institutions, the Nigerian government etc) relating to the use of computers in criminal behaviour.
   H1: Cybercrime does consists of various conducts (communicating of restricted information; the unauthorized accessing of information from financial institutions, the Nigerian government etc) relating to the use of computers in criminal behaviour.
6) HO: There is no existing law to adequately address cybercrimes (Hacking, Theft of Intellectual Property and Computer Related Fraud etc).
   H1: There are existing law to adequately address cybercrimes (Hacking, Theft of Intellectual Property and Computer Related Fraud etc).
7) HO: Cybercrimes cannot lead to loss of revenue to financial institutions and multinational companies.
   H1: Cybercrimes can lead to loss of revenue to financial institutions and multinational companies.

III. RESEARCH QUESTIONS

The following research questions will serve as guide to the study:

1. What are the laws guiding cybercrimes in Nigerian?
2. What are the causes of Cybercrime in Nigeria?
3. What are the Types of Cyber Crime often committed by individuals in tertiary institutions in Delta State, Nigeria?
4. What are the consequences of Cyber-Crime in Nigeria?
5. What are the relevance of Nigerian Cybercrime ACT 2015?
6. What are the challenges of cybercrime management in Nigeria?

7. What are the solutions to the challenges of cybercrime management in Nigeria?

IV. RESEARCH DESIGN

The design of this study is the correlational survey design. Correlational survey research design is used when the focus of a study is to find out whether or not there is a relationship between two or more variables. In this study the researcher is interested examining the law and cyber crime management in Nigeria with special reference to some selected tertiary institutions in Delta State, Nigeria. Therefore, this design is considered appropriate because the data that will be collected will be used to describe the direction and the magnitude of the relationship between the variables with respect to the population of the study.[29]

a. Population of the study

The target population in this research will comprise of all the 208 staff of all the forty (40) online businesses centers and cyber cafes in all the 28 tertiary institutions in Delta State, Nigeria. The following are the list of tertiary institutions in Delta State, Nigeria:

1. Federal University of Petroleum Resources, Effurun

---

[29] I.I. AKPABIO, & F.S. EBONG, *RESEARCH METHODOLOGY AND STATISTICS IN HEALTH AND BEHAVIOURAL SCIENCES 91*, (UNICAL Printing Press, Calabar, Nigeria, 2009); L. ERINOSHO, I. N. OBASI, & A. MADUEKWE, *INTERDISCIPLINARY METHODOLOGIES IN THE SOCIAL SCIENCES* (Auscon Fireseed and Co Ltd, Abuja, Nigeria, 2009); J.E. GYONG, Basic Component of a Research Project in Sociology, *A Paper Presentation at the In-House Training, Department of Sociology*, (ABU, Nigeria, 2011). This research also uses multidisciplinary perspective between law, security studies, social, and sociology. *Please also see* M. HARALANBOS, M. HOLBORN, & R. HEALD, *SOCIOLOGY: THEME AND PERSPECTIVES*, (Harper Collins Publishers, London, UK, 2008); National Population Commission, 2006 Population and Housing Census of the Federal Republic of Nigeria (National population Commission, 2006). A.O. OLAYIWOLA, *PROCEDURES IN EDUCATIONAL RESEARCH* 106, (Hanijam Publications, Ahmadu Bello Way, Kaduna, Nigeria, 2007); E.C. OSUALA, *INTRODUCTION TO METHODOLOGY*, (African Fep Publishers Limited, Nigeria, 1992).

2. Delta State University (Abraka Campus, Oleh Campus, Asaba Campus)
3. Delta State Polytechnic, Ogwashi-Uku
4. Delta State Polytechnic, Otefe-Oghara
5. Delta State Polytechnic, Ozoro
6. The Film and Broadcast Academy, Ozoro
7. College of Education, Agbor
8. College of Education, Warri
9. Federal College of Education Technical, Asaba
10. College of Physical Education, Mosogar
11. School of Health Technology, Ughelli
12. Petroleum Training Institute, Effurun
13. Western Delta University, Oghara
14. Novena University, Ogume-Amai
15. National Open University of Nigeria, Asaba Study Center, Asaba
16. National Open University of Nigeria, Emevor Study Center, Emevor
17. Delta State School of Marine Technology, Burutu
18. Nigerian Maritime University, Okerenkoko, Warri
19. Conarina School of Maritime & Transport Technology, Oria-Abraka
20. University of Information and Communication Technology, Agbor
21. State School of Midwifery, Asaba
22. School of Nursing, Agbor
23. School of Nursing, Warri
24. Baptist School of Nursing, Eku
25. Edwin Clark University, Kiagbodo
26. Eagle Heights University, Omadino, Warri
27. Nigerian Naval School, Sapele
28. Nigerian Navy Maritime University, Ibusa

b. Sample Size

The sample for the study shall consist of two hundred (200) staff of 20 online businesses centers and cyber cafes out of Two Hundred and eight (208) online business staff drawn from a total of forty the (40) online businesses centers and cyber cafes in tertiary institutions in Delta State, Nigeria. The following were the 10 tertiary institutions where 20 cyber

cafes out of forty (40) online businesses centers and cyber cafes (with 200 staff) were selected and used as sample:

1. Federal University of Petroleum Resources, Effurun
2. Delta State Polytechnic, Otefe-Oghara
3. College of Education, Agbor
4. College of Education, Warri
5. Federal College of Education Technical, Asaba
6. College of Physical Education, Mosogar
7. School of Health Technology, Ughelli
8. Petroleum Training Institute, Effurun
9. Western Delta University, Oghara
10. Novena University, Ogume-Amai

c. Sample technique

Two hundred (200) online business staff out of Two Hundred and five (208) of them will be selected from 20 online business centers / cyber cafes in tertiary institutions in Delta State, Nigeria using simple random sampling technique. This represents 76% of the population of online business staff in tertiary institutions in Delta State, Nigeria.

d. Instruments

The instrument that will be used for this study is titled: "The Law and the Cyber Crime Management in Nigeria Survey Scale" (TLCCMINNSS). The Questionnaire was adopted from Bethran and part of it was adapted. The instrument will be made up made of 30 items split into six sections A, B, C, D, E and F; each section is made up of 6 items. Section A was used to measure" legislative drafting and cyber crime" section B was used to measure "relationship between law enforcement and cyber crimes", section C was used to measure "attitudes and cyber crimes", section D was used to measure "ethics and cyber crimes", section E will be used to measure "Challenges of cyber crime management" and section E will be used to measure "solutions to the identified challenges" The research instrument will be based on four Likert scale: Positive worded items will be scored thus: "Strongly agree" – 4 points, "Agree"- 3 points, "Disagree" 2 points, and

Strongly Disagree -1 point while negative worded items will be scored thus "strongly Agree" 1 point, "agree" 2 points, "Disagree" 3 points and "Strongly disagree" 4 points.

e. Justification of the statistical test or technique

The following are the reasons for using Pearson product moment correlation statistics for the test of hypothesis:

1) Pearson product moment correlation statistics not only indicates the presence or absence of correlation between any two variables but also, determines the exact extent, or degree to which they are correlated.
2) Under this method, the researcher will also ascertain the direction of the correlation like whether the correlation between the two variables is positive, or negative.
3) Pearson product moment correlation statistics enables the researcher to estimate the value of a dependent variable with reference to a particular value of an independent variable through regression equations.
4) This method has a lot of algebraic properties for which the calculation of co-efficient of correlation, and a host of other related factors viz. co-efficient of determination, are made easy.
5) Fisher-Z Statistics is employed whenever it can be argued that a test statistic follows a normal distribution under the null hypothesis of interest. Many non-parametric test statistics, such as U statistics, are approximately normal for large enough sample sizes, and hence are often performed as Fisher-Z Statistics tests.

f. Data Analysis

Hypotheses 1 to 3 was tested using Pearson Product Moment Correlation Statistics and Fisher-Z Statistics. All hypotheses will be tested at a 0.05 alpha level of significance.

DATA PRESENTATION AND ANALYSIS OF FINDINGS

I. PRESENTATION OF DATA

Table 1 Distribution and Return of Questionnaire

Number of Questionnaire Administered on sample subjects	208
Number of Questionnaire that were duly completed and returned questionnaire	200
The percentage of questionnaire returned	100%

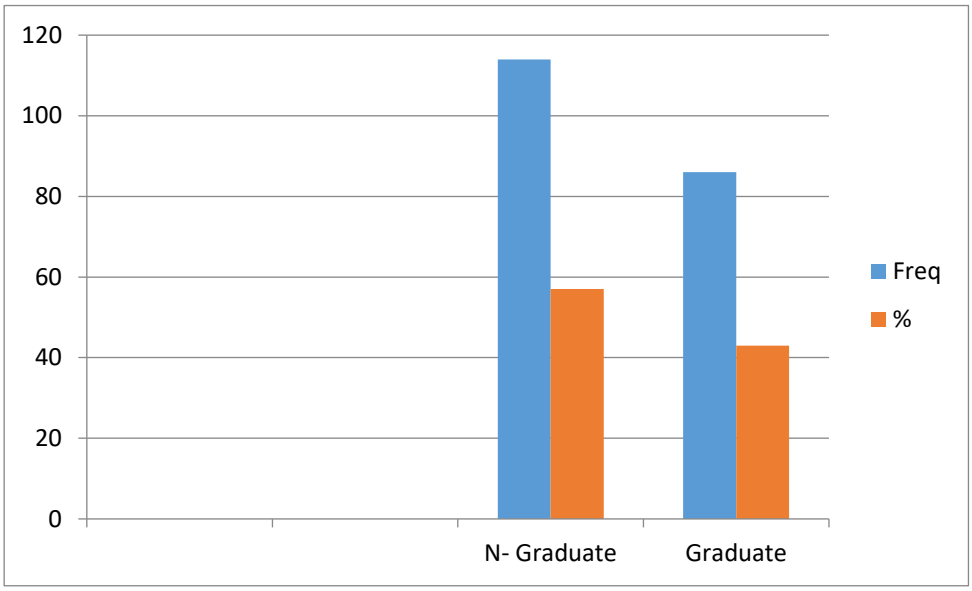
Source: Fieldwork, 2018

Table 1 shows that out of a total of 208 questionnaires administered on 200 sample elements, comprising of online staff, 200 copies were duly completed and returned questionnaire. This shows a response rate of 94%, implying a very good response rate for the study and considered adequate for comprehensive analysis and generalization of research findings.

Table 2 Distribution of Respondents by Level of Education

Level of Education of the respondents	Frequency	%
Non-Graduate	114	57
Graduate	86	43
Total	**200**	**100**

Source: Fieldwork, 2018

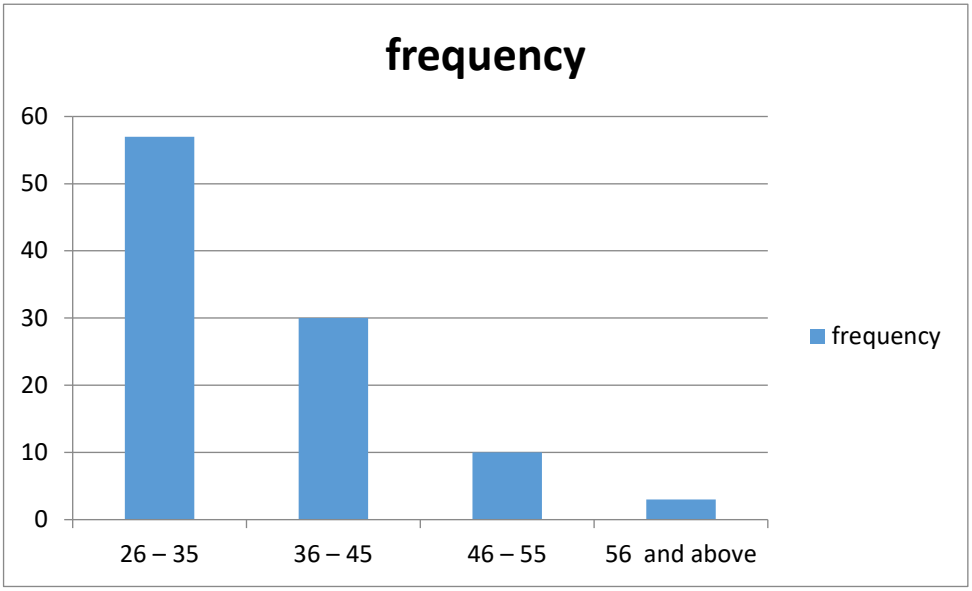


The graph above shows that 114 representing 57% of the respondents are on line staff who are non-graduates while 86 representing 43% of the staff of the cyber cafes or on line staff who are graduates; this demographic data reveals that the respondents are more of non-graduates.

Table 3 Distribution of Respondents by Age

Age of the respondents	Total Frequency	%
26 – 35	114	57
36 – 45	60	30
46 – 55	20	10
56 and above	6	3
Total	**200**	**100**

Source: Fieldwork, 2018



The age distribution of the respondents as revealed in the questionnaire indicates age ranges from 26 – 35; 36 – 45; 46 – 55 and 56 and above respectively. Since majority of the respondents are within the age bracket of 26-35 years and 36 – 45 years, this denotes a productive workforce of on line staff in terms of age.

II. ANALYSIS OF DATA

a. Research Question one

Table 4 The Laws guiding Cybercrime in Nigeria

No	ITEMS	SA	%	A	%	SD	%	D	%	TOTAL
1.	Economic and Financial Crimes Commission (Establishment) Act	5	2.5%	65	32.5%	127	63.5%	127	63.5%	200
2.	Advanced Fee Fraud and other Fraud Related Offences Act	140	70%	40	20%	10	5%	10	5%	200
3.	Nigerian Criminal Code	163	81.5%	32	16%	2	1%	3	1.5%	200
4.	Money Laundering	105	52.5%	73	36.5%	10	5%	12	6%	200

	Prohibition Act									
5.	The Nigerian Evidence Act and the Cybercrime Act 2015	40	20%	20	10%	35	17.5%	105	52.5%	200

Source: Field Survey by Research, 2018.

Table 4. above shows that economic and financial crimes commission (Establishment) Act, Advanced Fee Fraud and other Fraud Related Offences Act, Nigerian Criminal Code, Money Laundering Prohibition Act and The Nigerian Evidence Act and the Cybercrime Act 2015 are the Laws guiding Cybercrime in Nigeria.

b. Research Question Two: What are the causes of Cyber Crime in Nigeria?

Table 5 The causes of Cyber Crime in Nigeria

No	ITEMS	SA	%	A	%	SD	%	D	%	TOTAL
1.	Poverty	154	77%	36	18%	3	1.5%	7	3.5%	200
2.	Defective socialization	140	70%	40	20%	10	5%	10	5%	200
3.	Unemployment	163	81.5%	32	16%	2	1%	3	1.5%	200
4.	Weak laws/absent of existing law on cyber-crime	105	52.5%	73	36.5%	10	5%	12	6%	200
5.	Easy accessibility to the internet	40	20%	20	10%	35	17.5%	105	52.5%	200

Source: Field Survey by Research, 2018.

Table 5shows that majority of the respondents agreed 163 (81.5%) that unemployment is the major cause of Cyber Crime in Nigeria.

c. Research Question Three

Table 6 What are the Types of Cyber Crime often committed by individuals in tertiary institutions in Delta State, Nigeria?

No.	ITEMS	SA	%	A	%	SD	%	D	%	TOTAL
1.	Cyber-stalking	105	52.5%	73	36.5%	10	5%	12	6%	200

2.	Malicious program/Virus dissemination	40	20%	20	10%	35	17.5%	105	52.5%	200
3.	Cyber/identity theft	88	44%	45	22.5%	30	15%	37	18.5%	200
4.	Cyber defamation	180	90%	10	5%	6	3%	4	2%	200
5.	Cyber identity theft	170	85%	25	12.5%	2	1%	3	1.5%	200

Source: Field Survey by Research, 2018.

The above table 6 showed that Cyber defamation is the major type of Cyber Crime often committed by individuals in tertiary institutions in delta state, Nigeria.

Table 7 What are the consequences of Cyber-Crime in Nigeria?

No.	ITEMS	SA	%	A	%	SD	%	D	%	TOTAL
1.	Loss of revenue	40	20%	20	10%	35	17.5%	105	52.5%	200
2.	Loss of employment	140	70%	40	20%	10	5%	10	5%	200
3.	It is inimical to progress and development of the country	163	81.5%	32	16%	2	1%	3	1.5%	200
4.	Tarnishing the country's reputation internationally	105	52.5%	73	36.5%	10	5%	12	6%	200
5.	Loss of life	40	20%	20	10%	35	17.5%	105	52.5%	200

Source: Field Survey by Research, 2018.

The above table showed that the major consequence of Cyber-Crime is that it is inimical to progress and development of the country, with 163 (81.5%) agreeing to it.

Table 8 What are the relevance of Nigerian Cybercrime ACT 2015?

No	ITEMS	SA	%	A	%	SD	%	D	%	TOTAL
1.	Provide an effective and unified legal, regulatory and institutional framework for the **prohibition of cyber crime**	140	70%	40	20%	10	5%	10	5%	200
2.	Provide an effective and unified legal, regulatory and institutional framework for the **detection of cyber crime**	163	81.5%	32	16%	2	1%	3	1.5%	200
3.	Provide an effective and unified legal, regulatory and institutional framework for **prosecution of cyber crime**	105	52.5%	73	36.5%	10	5%	12	6%	200
4.	Provide an effective and unified legal, regulatory and institutional framework for **punishment of cybercrimes in Nigeria**	40	20%	20	10%	35	17.5%	105	52.5%	200
5.	Ensure the **protection of critical national information infrastructure**	88	44%	45	22.5%	30	15%	37	18.5%	200

	and the protection of computer systems									

Source: Field Survey, 2018.

The table above shows majority of the respondent strongly agreed the major relevance of Nigerian Cybercrime ACT 2015 is that it helps to provide an effective and unified legal, regulatory and institutional framework for the detection of cybercrime.

d. Research Question Six

Table 9 What are the challenges of cybercrime management in Nigeria?

No	ITEMS	SA	%	A	%	SD	%	D	%	TOTAL
1.	Poor security network in Nigeria	163	81.5%	32	16%	2	1%	3	1.5%	200
2.	Poor funding of the Police, EFCC and other relevant agencies	105	52.5%	73	36.5%	10	5%	12	6%	200
3.	Corruption among the Police, EFCC and other relevant agencies	40	20%	20	10%	35	17.5%	105	52.5%	200
4.	High level of Illiteracy in Nigeria	88	44%	45	22.5%	30	15%	37	18.5%	200
5.	Poverty of the mind	180	90%	10	5%	6	3%	4	2%	200

Source: Field survey 2018/2019.

In table above shows majority of the respondent strongly agreed the major challenge of cybercrime management in Nigeria is poor funding of the Police, EFCC and other relevant agencies.

e. Research Question Seven

Table 10 What are the solutions to the challenges of cyber crime management in Nigeria?.

No	ITEMS	SA	%	A	%	SD	%	D	%	TOTAL
1.	Redefine our ethical standards.	8.		170	85%	25	12.5%	2	1%	3
2.	Arrest and	163	81.5%	32	16%	2	1%	3	1.5%	200

	immediate prosecution of cyber-criminals									
3.	Introduce cyber-crime as a course in the curriculum of secondary school Students.	105	52.5%	73	36.5%	10	5%	12	6%	200
4.	Enlighten young ones about the consequences of such actions under law.	40	20%	20	10%	35	17.5%	105	52.5%	200
5.	Report to the police or other concerned authorities anyone we might suspect of engaging in cybercrime.	88	44%	45	22.5%	30	15%	37	18.5%	200

Source: Field Survey, 2018.

In table above shows majority of the respondent strongly agreed the best solutions to the challenges of cybercrime management in Nigeria is Arrest and immediate prosecution of cyber-criminals.

III. TEST OF HYPOTHESES

Hypothesis 1: The law cannot provide solution to Cyber Crime management in Nigeria.

Table 11 Fishers' Z of the law and Cyber Crime management in Nigeria

Sex	N	R	Zr	Z-cal.	Z-table
Male	85	.187	.189		
				3.215	1.96
Female	112	.217	.221		

α = .05

Table 11 shows a calculated Z value of 3.215 and a table value of 1.96, testing at an alpha level of .05, the calculated value falls within the rejection region, so, the null hypothesis which states that "The law cannot provide solution to Cyber Crime management in Nigeria" is rejected. Meaning the law cannot provide solution to Cyber Crime management in Nigeria.

Hypothesis 2: H0: Poverty is not a factor responsible for cyber crime in Nigeria.

Table12 Fishers' Z of poverty is not a factor responsible for cyber crime in Nigeria.=

Sex	N	R	Zr	Zcal	Z-table
Male	85	.161	.162		
				2.510	1.96
Female	112	.168	.170		

α = .05

Table 12 shows a calculated Z value of 2.510 and a table value of 1.96, testing at an alpha level of .05, the calculated value falls within the rejection region, so, the null hypothesis which states that "poverty is not a factor responsible for cybercrime in Nigeria" is rejected. Meaning poverty is not a factor responsible for cybercrime in Nigeria.

Hypothesis 3: H0: The law cannot promote intellectual property and ensure privacy rights.

Table 13 Fishers' Z of the law and promotion of intellectual property and ensuring of privacy rights

Sex	N	R	Zr	Zcal	Z-table
Male	85	.159	.160		
				2.078	1.96
Female	112	.170	.172		

α = .05

Table 13 shows a calculated Z value of 2.078 and a table value of 1.96, testing at an alpha level of .05, the calculated value falls within the rejection region, so, the null hypothesis which states that "The law cannot promote intellectual property and ensure privacy rights" is rejected. Meaning the law can promote intellectual property and ensure privacy rights.

Hypothesis 4: HO: The law does not provide mechanism for the enforcement of the rights, duties and laws that bother on cybercrimes.

Table 14 Fishers' Z of the law and provision of mechanism for the enforcement of the rights, duties and laws that bother on cyber crimes

Age	N	R	Zr	Z	Z-table
Under 20years	110	.211	.214		
				2.036	1.96
21years and above	90	.216	.219		

α = .05

Table 14 shows a calculated Z value of 2.036 and a table value of 1.96, testing at an alpha level of .05, the calculated value falls within the rejection region, so, the null hypothesis which states that "The law does not provide mechanism for the enforcement of the rights, duties and laws that bother on cybercrimes" is rejected. Meaning the law does provide mechanism for the enforcement of the rights, duties and laws that bother on cybercrimes.

Hypothesis 5: HO: Cyber crime does not consists of various conducts relating to the use of computers in criminal behaviour.

Table 15 Fishers' Z of Cybercrime consisting of computers in criminal behaviour

Age	N	R	Zr	Z-cal	Z-table
Under 20years	110	.188	.190		
				2.328	1.96
21years and above	90	.142	.143		

α = .05

Table 15 shows a calculated Z-cal value of 2.328 and a table value of 1.96, testing at an alpha level of .05, the calculated value falls within the rejection region, so, the null hypothesis which states that "Cybercrime does not consists of various conducts (communicating of restricted information; the unauthorized accessing of information from financial institutions, the Nigerian government etc) relating to the use of computers in criminal

behaviour." is rejected. Meaning Cybercrime does consists of various conducts (communicating of restricted information; the unauthorized accessing of information from financial institutions, the Nigerian government etc) relating to the use of computers in criminal behaviour.

Hypothesis 6: HO: There is no existing law to adequately address cybercrimes (Hacking, Theft of Intellectual Property and Computer Related Fraud etc).

Table 16 Fishers' Z of No existing law that adequately addresses cybercrimes (Hacking, Theft of Intellectual Property and Computer Related Fraud etc).

Age	N	R	Zr	Z	Z-table
Under 20years	110	.142	.143		
				2.515	1.96
21years and above	90	.214	.217		

α = .05

Table 16 shows a calculated Z value of 2.515 and a table value of 1.96, testing at an alpha level of .05, the calculated value falls within the rejection region, so, the null hypothesis which states that "There is no existing law to adequately address cybercrimes (Hacking, Theft of Intellectual Property and Computer Related Fraud etc)" is rejected. Meaning There are existing law to adequately address cybercrimes (Hacking, Theft of Intellectual Property and Computer Related Fraud etc).

Hypothesis 7: H0: Cybercrimes cannot lead to loss of revenue to financial institutions and multinational companies.

Table 17 Fishers' Z of Cyber crimes and loss of revenue to financial institutions and multinational companies

Sex	N	R	Zr	Zcal	Z-table
Male	85	.159	.160		
				2.078	1.96
Female	112	.170	.172		

α = .05

Table 17 shows a calculated Z value of 2.078 and a table value of 1.96, testing at an alpha level of .05, the calculated value falls within the rejection region, so, the null hypothesis which states that "Cybercrimes cannot lead to loss of revenue to financial institutions and multinational companies." is rejected. Meaning Cybercrimes can lead to loss of revenue to financial institutions and multinational companies.

IV. DISCUSSIONS OF FINDINGS

This section discusses the key findings from the objectives of the study in relation to other scholar's findings. As to the pattern and consequences of cyber-crime in tertiary institution in Nigeria, the study revealed that youths in tertiary institutions and graduates seeking for employment are mostly the perpetrators of this criminal activity. This result is found to have similarity with past studies. For instance, the report of EFCC (2012), on cyber-criminals caught and penalized shows a large number of the involvement of students and graduates as the main perpetrator of the crime. For example, a 25-year-old student of the University of Ilorin, Imonina Kingsley, was sentenced on four-count of impersonation, possession of fraudulent documents and attempt to obtain money by false pretences and was sentenced 20 years jail term. He was said to have used the false identity of one Mr. Thomas Duke, with the email address given as thomasduke4luv@yahoo.com to send fraudulent mails with intent to defraud unsuspecting victim.[30]

Also, Abayomi Lawal Adekunle Nurudeen, a final-year student of Survey and Geo-Informatics Engineering at the University of Lagos, sentenced to 19 years jail term for obtaining $47,900 from Pee Loo Rosalind Summer, an Australian lady. Similarly, Ferdinand Iheasirim, a 1993 graduate of Accountancy of Abia State University had claimed to Rev Robert McArdle, an Australian and that he was Ben Agwu, a security adviser to Nigeria's president. He was sentenced to 10 years imprisonment. All this are report of EFCC (2012).[31]

The research has shown that hacking, software piracy, credit card fraud, phishing, pin fraud and the use of social network are the commonest

[30] D. THOMAS, D, *Cybercrime in Nigeria*, 2011
[31] OGBUNWEZEH, *supra note* 27.

types of cyber-crime being perpetrated in tertiary institutions in Nigeria. This statement corroborate with past studies on the types of cyber-crime common in Nigeria. For instance, Olugbodi states that the most prevalent forms of cyber-crime in Nigeria are Website Cloning (phishing), Financial Fraud, Identity Theft, Credit Card fraud, Cyber-theft, Cyber-harassment, Fraudulent Electronic Mails, software piracy and Virus / Worms / Trojans.[32] In addition, Ribadu stated that the prominent forms of cyber-crime in Nigeria are cloning of websites, false representations, internet purchase and other e-commerce kinds of fraud.[33]

Findings from the study showed that youths who are involved in cyber-crime are within the ages of 18-30years who are motivated by the quest for quick luxurious comfort, greed, reputation, vengeance and low chances of being caught. The result of the finding agrees with past studies on the ages of cyber-criminals and motivating factor. For instance, a study by Zero Tolerance, indicates that cyber-criminals are usually within the age category of 18 and 30 years and they indulge in the crime in order to survive and have a taste of good life. The study further identified the sexes that are involved in cyber-crime. The study showed that males are mostly involved in cyber-crime.[34] This finding can be corroborated with that of Olaide and Adewole which states that cyber-crimes are male dominated, however, and that female are tender-hearted, feared being caught in evil act, humble, submissive, gentle, emotional and quiet while men are strong and daring. [35]

The theoretical deduction showed that an individual becomes a cyber-criminal if the following three conditions are met: if the individual had learned the requisite skills and techniques for committing the crime, if the individual had learned excess of definitions favourable to crime over definition unfavourable to crime and finally, if the individual had the objective opportunity to carry out the crime. In addition to the theory used, other push factors such as economic, socio-political and cognitive factors were identified which could lead an individual to be involved in cyber-crime.

Findings from the studies had shown that those individuals involved in cyber-crime associate with other cyber-criminals either through chat

[32] K. OLUGBODI, *Fighting Cyber Crime in Nigeria*, 2010.
[33] RIBADU, *supra note* 18.
[34] Zero Tolerance, *supra note* 20.
[35] OLAIDE & ADEWOLE, *supra note* 19.

channels (communication) or physically (interaction) in order to perfect their skills and to keep abreast of new techniques and potential targets. The study also revealed, that through these means, the individual develop a rationalization for cyber-crime. This fact tallies with assumption 1 - 4 of differential association theory. That state; Criminal behavior is learned, Criminal behavior is learned in interaction with other persons in a process of communication, The principal part of the learning of criminal behavior occurs within intimate personal groups, and When criminal behavior is learned.[36]

In addition, cyber-criminals have come to realized that corruption thrives in the society and it is uncheck by law enforcement agencies and the law enforcement agencies have not also done much to arrest and prosecute these cyber-criminal due to lack of legislature on cyber-crime, this gives them the opportunity to operate freely without fear of being arrested. This fact also tallies with fifth and sixth assumption of differential association theory, States that an individual will be pushed into deviant behavior depending on their view of the legal code as being favorable or unfavorable. A person becomes delinquent because of an excess of definitions favorable to violation of law over definitions unfavorable to violation of the law. According to the seventh factor of Differential Association, the finding revealed that the more time an individual spend with cyber-criminals, the more the increase in the frequency that they engage in deviant behavior.[37]

As to the causes of cyber-crime in Nigeria, the findings showed that unemployment, corruption, poverty, peer group influence, easy accessibility to the internet and weak laws are the causes of cyber-crime in the study area. Other studies also agreed with the findings, For instance Okoro, identified the following as the causes of cyber-crime in Nigeria; unemployment, negative role models, lack of adequate policing facilities and knowledge of cyber crime and social gratification.[38] Similarly, Awe stated that widespread of corruption, harsh economic climate, high unemployment, disregard for the rule of law and lack of transparency and

[36] R.L. MATSUEDA, *DIFFERENTIAL ASSOCIATION THEORY* (Seattle, WA, University of Washington, 2010).

[37] *Id*.., at. 117-119; see also McQuade, *supra note* 26.

[38] S. ARASE, & A. OBAEDO, *POLICING NIGERIA IN THE 21ST CENTURY* 298-302 (Spectrum Book, Ibadan, Nigeria, 2009).

accountability in governance are the main causes of cyber-crime in Nigeria.[39]

Regarding the negative consequences cyber-crime has on the society, it was discovered that such include loss of life, tarnishing the country's reputation internationally, loss of revenue and employment, denial of innocent Nigerians certain opportunity abroad. Similarly, past studies also agreed with this findings for example, Ringwelski listed the consequences cyber-crime has on the economy to include loss of revenue, wasted time, damaged reputation and reduce productivity.[40] The study adopted differential association theory which provided the relevant perspective in the study through its nine assumptions. It helped to explain why an individual becomes a cyber-criminal.

V. INTERPRETATION OF FINDINGS

The findings of the study revealed that:

1) The law can provide solution to Cyber Crime management in Nigeria.
2) Poverty is a factor responsible for cybercrime in Nigeria.
3) The law can promote intellectual property and ensure privacy rights.
4) The law provides mechanism for the enforcement of the rights, duties and laws that bother on cybercrimes.
5) Cybercrime consists of various conducts (communicating of restricted information; the unauthorized accessing of information from financial institutions, the Nigerian government etc) relating to the use of computers in criminal behaviour.
6) There are existing laws that adequately address cybercrimes (Hacking, Theft of Intellectual Property and Computer Related Fraud etc).
7) Cyber crimes cannot lead to loss of revenue to financial institutions and multinational companies.

[39] AWE, *supra note* 25; B.H. SCHELL & C. MARTIN, *CYBERCRIME: A REFERENCE HANDBOOK* 4-5, (ABC-CLIO Inc, Santa Barbara, California, 2004). D.L. SHINDER, *SCENE OF THE CYBERCRIME: COMPUTER FORENSICS HANDBOOK*, (Syngress Publishing Inc, US, 2002).

[40] M. RINGWELSKI, M., *Effects of Cyber Crime*, 2008.

VI. SUMMARY

This aspect of the research work is designed to present the summary of the findings of the research, conclusions as well as recommendations. This study investigated examined the law and cybercrime management in Nigeria with special reference to some selected tertiary institutions in Delta State, Nigeria. In order to address the problem of this study, seven research questions were raised and seven research hypotheses were formulated and tested at .05 level of significance. A correlation approach of survey research design was adopted in this study. The target population in this research will comprise of all the 208 staff of all the forty (40) online businesses canters and cyber cafes in all the 28 tertiary institutions in Delta State, Nigeria. The sample for the study consist of two hundred (200) staff of 20 online businesses centers and cyber cafes out of Two Hundred and eight (208) online business staff drawn from a total of forty the (40) online businesses centers and cyber cafes in tertiary institutions in Delta State, Nigeria. Two hundred (200) online business staff out of Two Hundred and five (208) of them will be selected from 20 online business centers / cyber cafes in tertiary institutions in Delta State, Nigeria using simple random sampling technique. This represents 76% of the population of online business staff in tertiary institutions in Delta State, Nigeria. The instrument that will be used for this study is titled: "The Law and the Cyber Crime Management in Nigeria Survey Scale" (TLCCMINNSS). The Questionnaire will be adopted from Bethran (2017) and part of it will be adapted. The instrument will be made up made of 35 items split into seven sections A, B, C, D, E and F; each section is made up of 5 items. Hypotheses were tested using Pearson Product Moment Correlation Statistics and Fisher-Z Statistics. All hypotheses were tested at a 0.05 alpha level of significance.

CONCLUSION

In view of the outcome of this study, the researcher concluded that the law can provide solution to Cyber Crime management in Nigeria. Poverty is a factor responsible for cyber crime in Nigeria. The law can promote intellectual property and ensure privacy rights. Lack of national framework and infrastructure for such, the obvious lack of cyber law and cyber

policing in protection and management of electronic payment fraud Nigeria will continue to promote the activities of Nigerian and other cybercrimes. Therefore, no single law enforces- cybercriminals. More so, it was concluded that thus, absence of laws (legislation) to crime will take place. In relation to Nigeria, the theory is address online criminality makes it impossible to pro- relevant because cybercrime activities have more to do secure offenders with the ineffectiveness of indirect guardianship; as such, the absence of a national Internet gateway for Nigeria a motivation for such crime to take place. The remarkable development in human history through computer technology has no doubt brought about transformation in all aspects of life, especially in communication and information technology. Nevertheless, the embracement of the internet has come with a lot of mixed feelings despite its numerous advantages to the people. Cyber-crime is the use of computer/internet as an instrument to further illegal ends such as committing hacking, credit card fraud, phishing, pornography, software piracy and theft of intellectual property, stealing identities, unauthorized access, cloning of website amongst others. It can be inferred from the findings that in Nigeria, people are valued in terms of what they possess and command economically. Conversely, those without economic success are undervalued and the pressure to achieve success is intensified despite the harsh economic condition such as unemployment amongst others. This necessitated the ability of individuals to devise survival strategies and attain economic success by indulging in cyber-crime. However, the increasing rates of cybercrime in the society has become a strong threat to Nigeria's e-commerce growth and has led to ill-reputation internationally and consequently denied some innocent Nigerians certain opportunities abroad. The perpetrators of cyber-crime are not far-fetched; they are our brothers, friends, colleague, distant relatives and neighbours who can be tamed under appropriate circumstances with the right and positive communication, orientation, education and empowerment.

RECOMMENDATIONS

The recommendations for this research are proffered based on the major findings on the study. This study recommend that youths should be empowered through the creation of jobs. The study has identified youths

within the ages of 20-30 years to be the most frequent perpetrators of cyber-crime and in addition, the study has also discovered that these youths are either misguided or misdirected by peers, celebration of unknown wealth amongst others. The study therefore recommends that the young ones should be enlightenment on the consequences of cyber-crime. Government should continue to cooperate with IT industries to develop adequate strategy to fight cyber-crime. There should be zero tolerance to corruption at all levels. Cyber-criminals arrested should be prosecuted immediately to deter a would-be-offender. The findings showed that cyber-criminals live in the society, as such; prevention of cyber-crime requires the co-operation of all the citizens and not just the law enforcement agencies. It is therefore, recommended that everyone should watch and report to law enforcement agencies anyone who indulges in cyber-crime. Ethical values should be redefined in Nigeria. The study shows that youths involved in cyber-crime are either in tertiary institutions or have graduated from tertiary institutions; the study therefore, recommends that curriculum which will include courses on cyber-crime, cyber-management and its prevention should be introduced at both tertiary and secondary schools to take care of the present social changes.

REFERENCES

Abdulhamid, S.M, Haruna, C. and Abubakar, A. (2011) Cybercrimes and the Nigeria Academic Institution Networks. *The IUP Journal of Information Technology*, 7(1), 1-36.

Ahmed, A.A. (2010). *Hack No More, Internet Security: Attacks and Defence.* Nigeria: Ahmadu Bello University Press Limited.

Aghatise, E.J. (2006). *Cyber-crime Definition*, Computer Crime Research Centre. Retrieved September 20, 2011 from www.crime-research.org

Akande, F.F. (2007). *Issue in Humanities and Technology.* Ilorin: Integrity Publication.

Akpabio, I.I. & Ebong, F.S. (2009). *Research Methodology and Statistics in Health and Behavioural Sciences.* Calabar Nigeria: UNICAL Printing Press.

Ajewole, A. (2010). *Curbing Cybercrime in Nigeria. Fighting the Masked Enemy and Promoting Productive Alternative for the Youth.* Retrieved October 8, 2011 from http/www.primopdf.com.

Arase, S., & Obaedo, A. (2009), *Policing Nigeria in the 21st Century*. Ibadan, Nigeria: Spectrum Book.

Awe, J. (2009). *Fighting Cybercrime in Nigeria.* Retrieved September 10, 2011 from http://www.jidaw.com/itsolutions/security3.html.

Ayantokun, O. (2006). *Fighting Cyber-Crime in Nigeria, Information-System*, Retrieved September 10, 2011 from www.tribune.com.

Broadhurst, R. G., & Grabosky, P. N. (2005). *Cyber-Crime: The Challenge in Asia*. Hong Kong: Hong Kong University Press.

Dambazau, A. B, Jumare, M. M., & Yakubu, A. M. (1996). *Issues in Crime Prevention and Control in Nigeria.* Kaduna, Nigeria: Baraka Press and Publishers Ltd.

Ehimen, O. R., & Bola, A. (2010). Cybercrime in Nigeria, *Business Intelligence Journal*, 3(1), 85-124.

Erinosho, L, Obasi, I. N., & Maduekwe, A. (2002). *Interdisciplinary Methodologies in the Social Sciences.* Abuja, Nigeria: Auscon Fireseed and Co Ltd.

Fischer, J.R, Halibozek, E., & Green, G (2008). *Introduction to Security*, Oxford: Linacre House, Jordan Hill.

Gyong, J.E (2011). Basic Component of a Research Project in Sociology, *A Paper Presentation at the In-House Training, Department of Sociology, ABU, Nigeria.*

Haralanbos, M, Holborn, M. & Heald, R. (2008). *Sociology: Theme and Perspectives.* London, UK: Harper Collins Publishers.

Hidayatullah, K (2000). *Cyber Crime and Its Consequences*, National Law University Raipur (Chhattisgarh) village Upperwara, Tehsil Abhanpur, New Raipur (C.G).

Imhof, R. (2010). *Cybercrime and Telecommunication Law*, Rochester Institute of Technology USA. Information and Communication Technology.

Internet Crime Complaint Center, (2010). *Internet crime report*, retrieved from http://www.ic3.report.nw3c.org/docs/2010_ic3_report_02_10_11_low_res_pdf.2011

Kumar, K. (2003). *Cyber Laws, International Property and E-commerce Security.* New Delhi: Dominant Publishers and Distributors.

Longe O. S., & Chiemeke S. C. (2008). Cyber Crime and Criminality in Nigeria. What Roles are Internet Access Points in Playing? *European Journal Social Sciences*, 6(4), 132-139.

Matsueda, R. L. (2000). *Differential Association Theory.* Seattle, WA: University of Washington.

McConnell, (2000). Cybercrime and Punishment, *Archaic Laws Threaten Global Information*, www.mcconnellinformation.com.mcconnellinternational L.L.C.

McQuade, S. (2009). *The Encyclopedia of Cybercrime.* Westpoint Connecticut, London: Green Wood Press,

Morley, D., & Parker, C.S. (2007). *Understanding Computers, Today and Tomorrow.* USA: Thomson Course Technology.

National Population Commission (2006), *2006 Population and Housing Census of the Federal Republic of Nigeria*, national population Commission.

Ogbunwezeh, E.F. (2006). *EFCC and Cybercrime The True Lesson*, Retrieved from www.nigeriavillagesquare.com.

Olaide, M. and Adewole, R. (2004). *Cyber Crime Embarrassing for Victims.* Retrieved September 2011 from http//www.heraldsun.com.au

Olayiwola, A.O. (2007). *Procedures in Educational Research.* Kaduna, Nigeria: Hanijam Publications, Ahmadu Bello Way.

Olugbodi, K. (2010). *Fighting Cyber Crime in Nigeria*, Retrieved September 10, 2011 from http://www.guide2nigeria.com/news_articles_about_Nigeria.

Osuala, E.C. (1992). *Introduction to Methodology.* Nigeria: African Fep Publishers Limited.

Oyesanya, F. (2004). *Nigerian Internet 419 On The Loose*. Retrieved October 8, 2011 from http://www.nigeriavillagesquare.com.

Oyewole, A.S. and Obeta, A. (2002). *An Introduction to Cyber Crime.* Retrieved September 2011 from http//www.crime-research.org/articules/cyber-crime.

Pati, P. (2003), *Cybercrime*. Retrieved from wwwnivi.org.

Planetindia, (2001). *Introduction to Cyber Crime.* Retrieved October 9, 2011 http://cybercrime.planetindia.net/intro.htm.

Ribadu, N. (2007). Cybercrime and Commercial Fraud: A Nigerian Perspective, *A paper presentation at the Modern Law for Global Commerce*, Vienna 9-12 July 2007.

Ringwelski, M. (2008). *Effects of Cyber Crime.* Retrieved from http://www.ehow.com/about_5052659_effects-cyber-crime.html#ixzz1gaX6daue.

Roger, E. (1995). *Diffusion of Innovation*, Retrieved September 12, 2011 from http://enwikibooks.org/wiki/communication_Theory/Diffusion_of_Innovations.

Rogers M.K. (2001). *A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behaviour. An Exploratory Study.* Winnipeg, Manitoba: University of Manitoba.

Salihu, T. (2006). Impact of Computer Appreciation in Military Technology, *A Commandant's Paper submitted to Nigerian Army School of Military Police, Nigeria.* School of Postgraduate Studies.

ABU (2010), *Regulations Governing Higher Degree Studies, Nigeria*. Nigeria: ABU Press Limited.

Schell, B.H. and Martin, C. (2004). *Cybercrime: A Reference Handbook.* Santa Barbara, California: ABC-CLIO Inc.

Sesan, G. (2010). *The New Security War*, retrieved from http://www.pcworld.com/article/122492/the_new_security_war.htm #tk.mod-rel.

Shinder, D.L. (2002). *Scene of the Cybercrime: Computer Forensics Handbook.* USA: Syngress Publishing Inc.

Tade, O., & Aliyu, I. (2011), Social Organization of Internet fraud among University Undergraduates in Nigeria. *International Journal of Cyber Criminology*, 5(2), 860-875.

Thomas, D. (2011). *Cybercrime in Nigeria*, Retrieved September, 2011 from http://www.idgnews,net/

Umar-Ajijola, J, (2010a). *Microsoft Combats Cybercrime in Nigeria*, retrieved from http://www.pcworld.com/businesscenter/article/205051/cybercrime.

Umar-Ajijola, J. (2010b). *Fighting Cybercrime in Nigeria*, retrieved from http://blogs.technet.com/b/microsoft_on_theissues_africa/archive/2010/12/9/fighting-cybercrime-in-nigeria-aspx.

Vladimir, G. (2005). *International Cooperation in Fighting Cyber Crime*, retrieved from www.crimeresearch.org.

Wall, D.S (2001), *Crime and The Internet.* London: Routledge Publisher.

Wall, D.S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge, UK: Polity Press.

Yar, M. (2006). *Cybercrime and Society*. London: Sage Publication Ltd.

Young Media Association (2007). *The Internet: Benefits, Danger, and Strategies*. Australia: Australia Young Association.

Zero Tolerance (2006), The Portrait of a Yahoo Boy. *Economic and Financial Crime Commission*, 1(3), 38-39.

QUOTE

Ransomware is unique among cybercrime because in order for the attack to be successful, it requires the victim to become a willing accomplice after the fact

James Scott, Sr. Fellow, Institute for Critical Infrastructure Technology

ABOUT AUTHORS

Ngboawaji Daniel Nte is Professor and Head of Department of Intelligence and Security Studies, Novena University, Delta State. He also a professional researcher at Security Studies.

Urowayinor Kelita Esq is a full professor of intelligence and Security studies at Novena University, Nigeria. He has written extensively on different areas of public safety and national security. He has over seventy journal articles to his credit. He also now serving as a professional lecturer and researcher at the Department of Intelligence and Security Studies, Novena University, Delta State, Nigeria.

Bribena Kelvin Enokie is a Lecturer at the Faculty of Law Niger Delta University, Wilberforce Island, Amasoma, Bayelsa State, Nigeria.

Onyeka Bienose, is Director, Business Development, African Regional Office, Global Intelligence, Peace and Security Institute, Nigeria.