AN APPRAISAL OF THE LEGAL FRAMEWORK FOR COMBATING CYBERCRIME IN INTERNATIONAL LAW

BY

Sekav Stephen, DZEVER
LLM/LAW/06950/2010-2011

BEING A THESIS SUBMITTED TO THE POSTGRADUATE SCHOOL, AHMADU BELLO UNIVERSITY, ZARIA IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTERS OF LAW-LLM

MAY, 2016

DECLARATION

I declare that the work in this dissertation entitled"AN APPRAISAL OF THE LEGAL FRAMEWORK FOR COMBATING CYBERCRIME IN INTERNATIONAL LAW" has been carried out by me in the Department of Public Law, Faculty of Law, Ahmadu Bello University, Zaria. The information derived from the literature has been duly acknowledged in the text and the list of references provided. No part of this dissertation was previously presented for another degree or diploma in this or any other institution.

Sekav Stephen, DZEVER _____ _____
LLM/LAW/06950/2010-2011 **Signature** **Date**

CERTIFICATION

This dissertation entitled "AN APPRAISAL OF THE LEGAL FRAMEWORK FOR COMBATING CYBERCRIME IN INTERNATIONAL LAW" by Sekav Stephen, DZEVER" meets the regulations governing the award of the degree of Master of Laws - LL.M of the Ahmadu Bello University, Zaria, and is approved for its contribution to knowledge and literary presentation.

Professor M.T. Ladan Chairman, Supervisory Committee	_____ Signature	_____ Date
Dr. I.F. Akande Member, Supervisory Committee	_____ Signature	_____ Date
Dr. K.M. Danladi Head, Department ofPublic Law	_____ Signature	_____ Date
Prof. Kabir Bala Dean, School of Postgraduate Studies	_____ Signature	_____ Date

ACKNOWLEDGEMENTS

I strongly acknowledge the contributions of my first supervisor, Professor M.T. Ladan of the Public Law Department for his immense literary and academic scholarship towards the success of this thesis. My thanks also go to my second supervisor and the assistant Dean, Post Graduate, Dr. I.F. Akande of the Faculty of Law for processing the basic requirements of this thesis and for her patience and good guidance during the period of this work, even as my thesis topic was modified on three different occasions, first by my Professor M.T. Ladan, secondly by the Board, Faculty of Law and lastly by the Postgraduate School, after I had finished writing the thesis.All through, Dr. Akande ensure that all that concerns my LL.M degree was put in order. Ma, only God can pay you for all the good deeds you are doing for your students.

I wish to acknowledge the support of all members of my family, particularly Denen Orkar Esquire who always urged me to speed up my master's degree thesis against time. My profound appreciation goes to all academic and non academic staff members of Faculty of Law, Ahmadu Bello University, Zaria as well as all my colleagues and friends at the Postgraduate school in the Faculty of Law (especially His Worship, Paul Aliyu Adama and Tanko Ishaya) for their moral and academic support. I also acknowledge the administrative ingenuity of the Dean of Law, Professor Y. Y. Bambale.

DEDICATION

This thesis is dedicated to my dear mother, Elizabeth Ityavmough Zever and my wife, Gloria Isuwa Dzever for their love and support.

TABLE OF CASES

LOCAL CASES **pg**

FRN vs. Chima L. Larry Ikonji and Blessing Onochie -- -- -- --

-- 74,75,78

Elelu Habeeb vs. A.G. Federation -- -- -- -- -- -- 26, 32

Esso West Africa Inc. vs. T. Oyebgola -- -- -- -- -- 86, 87

FRN vs. Nvene -- -- -- -- -- -- -- -- 98, 99

FRN vs. Odiawa -- -- -- -- -- -- -- -- 73,75,77

Mike Amadi vs. Federal Republic of Nigeria -- -- -- -- -- 98, 104

Yesufu vs. A.C.B. -- -- -- -- -- -- -- -- 86, 87

Registered Trustees of the Nigerian Bar Association vs. The Attorney General of the Federation & the Central Bank of Nigeria -- -- -- 63

FOREIGN CASES

International Shoe Co. vs. Washington, Office of Unemployment Compensation andPlacement et al. -- -- -- -- -- -- -- -- 36

Worldwide Volkswagen Corporation vs. Woodson -- -- -- -- 37

Burger King Corp. vs. Rudzewicz -- -- -- -- -- -- 38

Dow Jones & Co. Inc. vs. Gutnick, -- -- -- -- -- -- 38

CompuServe, Inc. vs. Patterson -- -- -- -- -- -- 39

Mckinnon vs. Government of the USA & 1 Or. -- -- -- -- 42

R vs. Bow Street Magistrates Court and Allison, ex parte Government of the United States of America -- -- -- 42

Federation of Law Societies of Canada vs. The Attorney General of Canada & Canada Bar Association -- -- -- -- -- -- 63

TABLE OF STATUTES

pg

Advance Fee Fraud and other related offences Act No.14 2006…. …. 7,9,10, 24, 53, 55, 56, 74, 92.

Anti terrorism Act (as amended) 2013……. 7,10, 9.

Criminal Code Act, 2004 9,24,78

Economic and Financial Crimes Commission (Establishment) Act 2004… 9,53,54,55,56, 73,74,75,76,77

The Evidence Act No.18 2011 ……. 53, 84, 85, 87

Money Laundering (Prohibition) Act No. 1, 2011 and Money Laundering (Prohibition) (Amendment) Act 2012 …… 7,9,92,

National Identity Management Commission Act, 2007 …….. 9, 91

Penal Code Act Cap 110, Laws of Kaduna State, 1991…….. 9,56,78

FOREIGN STATUTES

Computer misuse Act, 1990 ……. 9, 130

Criminal Justice Act 1978 …… 130

Police and Justice Act, 2006 …… 9,130

Protection of Children Act, 1978 …… 130

Canadian Charter of Rights and Freedoms ……. 84

Proceeds of Crime (Money Laundering) and Terrorist Financing Act, S.C.

2000, c. 17 (as amended) of Canada …….. 63

ABBREVIATIONS

AU	-	African Union
CBN	-	Central Bank of Nigeria
ECOWAS	-	Economic Community of West African States
EFCC	-	Economic and Financial Crimes Commission
EU	-	European Union
GSM	-	Global System of Mobile Communication
ICT	-	Information and Communication Technology
IP	-	Internet Protocol
ISPs	-	Internet Service Providers
ITU	-	International Telecommunications Union
MDAs	-	Ministries, Departments and Agencies
NBC	-	Nigerian Broadcasting Commission
NCC	-	Nigerian Communications Commission
NITDA	-	National Information Technology Development Agency
OECD	-	Organization for Economic Cooperation and Development
UNCTAD	-	United Nations Conference on Trade and Development
UNODC	-	United Nations Office on Drugs and Crime

TABLE OF CONTENTS

		pg
Title page	- - - - - - - - -	i
Declaration	- - - - - - - - -	ii
Certification	- - - - - - - - -	iii
Acknowledgement	- - - - - - - - -	iv
Dedication	- - - - - - - - -	v
List of abbreviations	- - - - - - - -	vi
Table of statutes	- - - - - - - - -	vii
Table of cases	- - - - - - - - -	viii
Table of contents	- - - - - - - - -	ix
Abstract	- - - - - - - - -	xv

CHAPTER ONE
GENERAL INTRODUCTION

1.1	Background of the Study - - - - - - -	1
1.2	Statement of the Research Problem - - - -	3
1.3	Objectives of the Research - - - - - - -	6
1.4	Scope of Study - - - - - - - -	7
1.5	Justification - - - - - - - - -	8
1.6	Research Methodology - - - - - -	8
1.7	Literature Review - - - - - - - -	9
1.8	Organizational Layout - - - - - - -	19

CHAPTER TWO
CONCEPTUAL CLARIFICATION OF KEY TERMS

2.1	Introduction - - - - - - - - -	27
2.2	Meaning of CyberLaw - - - - - - -	20

2.3 Meaning of Cybercrime - - - - - - 21

2.4 Meaning of Cyberspace - - - - - - 24

2.5 Meaning of Cyberjurisdiction- - - - - - 26

2.5.2 Cyberspace and Cyber Jurisdiction - - - - - 28

2.5.3 Determinants of Jurisdiction in the United States of America, United Kingdom and Nigeria- - - - - - - 29

2.5.4 Prescriptive Jurisdiction - - - - - - - - 30

2.5.5 Adjudicative Jurisdiction - - - - - - - 34

2.5.6 Enforcement Jurisdiction - - - - - - - 39

2.6 Cybercrimes Committed in Nigeria and Criminalized under the

Budapest Convention - - - - - - - - 42

2.6.1 Acts carried out by Criminal Minded Individuals against Computers- 42

2.6.2 Acts carried out by Criminal Minded Individuals against Individuals- 43

Other Acts or Omissions against Persons not Criminalized under any Law- 49

2.6.3 Cybercrimes Committed against the State- - - - - - 49

CHAPTER THREE
LEGAL AND INSTITUTIONAL FRAMEWORKS RELEVANT FOR INTERNATIONAL COOPERATION AGAINST CYBERCRIME IN NIGERIA

3.1 Introduction - - - - - - - - - 53

3.2 The Role of the Economic and Financial Crimes Commission (establishment) Act 2004 and the Commission in Fighting Cybercrime - - 53

3.2.1 The Nigerian Financial Intelligence Unit (NFIU) - - - 57

3.2.2 Special Control Unit against Money Laundering- - - - 62

3.2.3 Sectoral Regulations against Money Laundering as Provided by

the NFIU- - - - - - - - - 64

Central Bank of Nigeria (Anti-money Laundering and Combating of Financing of Terrorism in Banks and other Financial Institutions in Nigeria) Regulations, 2013 -- - - - - 64

National Insurance Commission (Anti-money Laundering and Countering the Financing of Terrorism) Regulations, 2013- - - - - 68

Securities and Exchange Commission (Capital Market Operators Anti-Money Laundering And Combating The Financing Of Terrorism) regulations, 2013 - - - - - - 70

3.2.4 Shortcomings in some Crimes which Computer was used and were Investigated and Prosecuted by the EFCC - - - 73

3.3 The Criminal Code Act - - - - - - 78

3.4 The Penal Code Act - - - - - - 78

3.5 Terrorism (prevention) act, 2011 (as amended in 2013) and Regulations 2013 - - - - - - 79

3.6 The Evidence Act - - - - - - - 84

3.7 The Federal Ministry of Justice - - - - - 87

3.8 Directorate for Cyber Security - - - - - 88

3.9 National Information Development Agency - - - - 89

3.10 National Identity Management Commission Act, 2007 - - 91

3.11 The Advance Fee Fraud Act, No. 14, 2006 - - - - 92

3.12 The Money Laundering (Prohibition) Act, 2011 - - - 92

3.13 Challenges of International Cooperation in the Fight against Cybercrime- 93

3.13.1 Lack of Cybercrime Specific Laws - - - - 94

3.13.2 Lack of Adequate Provisions on Collection and use of Electronic Evidence in Nigeria - - - - - - - 94

3.13.3 Lack of Proper Training of Law Enforcement Agencies on Investigating Acts or Omissions that Constitute Cybercrimes- - - - 95

3.14 An Overview of Nigeria's Cybercrime Act, 2015 and Its Relevance in International Cooperation in Combating Cybercrime- - - 95

CHAPTER FOUR
IMPACT OF THE BUDAPEST CONVENTION ON CYBERCRIME AND OTHER INTERNATIONAL ATTEMPTS ON FIGHTING CYBERCRIME

4.2 International Cooperation in the Fighting Cybercrime - - 109

4.3 Continental Cooperation in the Fight against Cybercrime - - 119

4.4 An Appraisal of the Budapest Convention on Cybercrime - - 121

4.4.1 Benefits of becoming a Party to the Budapest Convention on Cybercrime- 124

4.5 Overview of National Implementation of the Budapest Convention in the United Kingdom - - - - - - - - 128

4.6 General the Issues and Challenges in the Fight against Cybercrime - 131

4.6.1 Some Nations are Safe havens for those who Abuse Information Technologies - - - - - - - 131

4.6.2 Investigation and Prosecution of International Cybercrimes are not Coordinated among all Concerned States, Regardless of where Harm has Occurred - - - - - - - - 132

4.6.3 Law Enforcement Personnel are not Trained and Equipped to Address Cyber Crimes - - - - - - - - 133

4.6.4 Legal Systems do not Protect the Confidentiality, Integrity, and Availability of Data and Systems from Unauthorized Impairment and Ensure that serious Abuse is Penalized - - - - - - - 134

4.6.5 Legal Systems do not Permit the Preservation of and quick access to Electronic Data, which are often Critical to the Successful Investigation of Crime - - - - - - - - - 135

4.4.6 Mutual Assistance Regimes do not Ensure the Timely Gathering and Exchange of Evidence in Cases Involving International Cyber Crime- 135

4.6.7 Forensic Standards for Retrieving and Authenticating Electronic Data for use in Criminal Investigations and Prosecutions are not Developed- 136

4.6.8 Information and Telecommunications Systems are not Designed to help Prevent and Detect Network Abuse, and do not Facilitate the Tracing of Criminals and the Collection of Evidence - - - - 136

4.6.9 Duplication of Efforts in International Fora in the Fight Against Cybercrime - - - - - - - - 136

4.7 Comparism between the Budapest Convention on Cybercrime and the Cybercrime bill 2013 - - - - - - - 136

CHAPTER FIVE

SUMMARY, FINDINGS AND RECOMMENDATIONS

5.1 Summary - - - - - - - - 138

5.2 Conclusion - - - - - - - - 139

5.3 Findings - - - - - - - - 139

5.3 Recommendations - - - - - - - 142

ABSTRACT

The current wave of globalization and technological revolution has tremendous effect on the way people interact, carry out business transactions and store information. The internet has a vital role to play in all these. Though there are numerous advantages associated with the internet today as it has made interaction, business transactions and transfer of data easy, cybercrimes which are criminal acts carried out through the internet or through computer devices are serious threats to use of the internet or computer devices. To make matters worse, there are no comprehensive laws which address cybercrimes in most nations today and law enforcement agencies and the judiciary are not properly "equipped" to handle cybercrimes. For instance, in the course of investigating and prosecuting cybercrimes jurisdiction is always very hard to determine in cyberspace, i.e. the internet. What makes the issue of jurisdiction paramount in investigation and prosecution of cybercrimes is the fact that cybercrimes are borderless crimes as they can be committed from anywhere at any where once the cybercriminal has internet connection or has access to a computer device. The current laws regulating criminal conduct in most nations of the world today are ill-equipped to cope with these emerging cybercrimes. The old standard of classification and investigation of traditional crimes cannot meet up with the fast-changing technological advancements especially in the internet. This consequently creates an avenue for criminal minded individuals to hide behind a computer screen and deceive unsuspecting individuals who are the victims of the cybercriminal. The cybercriminal is usually faceless and his location unknown, making it easier for him to enter and exit the cyber space of the cyber victim with little or no detection. There is therefore the need to encourage the adoption of international law in combating cybercrime all over the world. The Budapest Convention on cybercrime which is the only treaty on cybercrime has numerous advantages which parties to the said convention stand to benefit from. Using Nigeria, the United States of America and the United Kingdom as contact-points of this study, this thesis has also attempted to highlight grey areas in criminal law which affects security of most people in the world today and the internet. Some of the laws considered are: Economic and Financial Crimes Commission (Establishment) Act 2004, Criminal Code Act, Cap C 38, LFN 2004, Penal Code law, Cap. 110 law of Kaduna State 1991,*the Terrorism (Prevention) Act, 2013, Money Laundering (Prohibition) Act No. 1, 2011 and Money Laundering (Prohibition) (Amendment) Act 2012, the Evidence Act No.18 2011, Advance Fee Fraud and other related Offences Act No. 14, 2006, the Nigeria Cybercrime Act, 2015 and from the United Kingdom, the Computer misuse Act, 1990 the Criminal Justice Act 1978, the Police and Justice Act, 2006 and the Protection of Children Act, 1978. Jurisdiction is discussed, highlighting principles of jurisdiction from Nigeria, the United States of America and the United Kingdom.The effort in this study is not to lay claim, with certainty, to the fact that the Budapest Convention on cybercrime is the ultimate treaty on cybercrime, but to encourage the participation of the comity of nations in the only treaty on cybercrime and enacting cybercrime specific laws in all nations of the world as encouraged by the said treaty. This would encourage international cooperation in the fight against cybercrime.*

CHAPTER ONE

GENERAL INTRODUCTION

1.1 Background to the Study

Undeterred by the prospect of arrest or prosecution, cyber criminals around the world lurk on the internet as an aim present menace to the financial health of business, to the trust of their customers, and as an emerging threat to nation's security.[1]

The Internet is one of the truly revolutionary phenomena of our times. It has changed the way we live and work and we have come to rely on it in every sphere of our endeavours. From a population of 20million connected to the Internet in 1998 we now have more than two billion and rising.[2]It is estimated that this connectivity will now double in the coming years as a result of a number of factors including the introduction of non-Latin script top level domains for Internet addresses, expansion of the Internet's generic domain name space and the increasing prevalence of smart phones and tablets with Internet access. While the benefits of this borderless ecosystem have grown exponentially the Internet has also become an irresistible magnet for criminal behaviour. Cyber criminals have become increasingly inventive and gravitate to jurisdictions which offer them most protection because of outdated and or non- harmonized legal regimes and law enforcement agencies which do not have the skills and resources to monitor Internet traffic, to investigate complaints, to prosecute or invoke any intervention that may be warranted. The global and borderless nature of the Internet enables criminals to co-operate and co-ordinate their activities and distribute their assets over several jurisdictions with impunity.

---

[1] Shanon, C.S. (2000) *"Global Internet Regulation: the Residual Effect of the "I LOVE YOU' Computer Virus and the Draft Convention on Cybercrime"* www.suffolkedu/../accessed on 12/1/2013 by 9:00pm.

[2] See http://www.internetworldstats.com/emarketing.html accessed on 22/1/2014 by 9:10 pm.

With the ever-evolving computer technology, computer-related crime and cybercrime have become a significant global challenge. The ability to automate attacks against computer systems can lead, for example, to hundreds of thousands of registered attempts to interfere with, or illegally access computer systems each day. Hundreds of new computer viruses are detected every month[3] and virus toolkits enable computer users with even limited skills to create malicious software. Through networks of literally millions of compromised computer systems controlled by individual criminal groups, even the most powerful Internet services can be attacked.[4] Such threats are expansive, not only in terms of quantity, but also in terms of quality. In recent years, the number of reports concerning targeted attacks against critical infrastructure have increased. The Internet is based on single technical standards that allow global communication. This has the advantage of allowing the globalization of Internet services (such as Facebook, Google, Yahoo and others) that are operated in one country but can be accessed by users from all over the world. From a crime prevention perspective, however, it has the disadvantage that acts of cybercrime do not require that the offender be located in the same country as the victim. This explains why the vast majority of cybercrime offences have a transnational dimension. Successful prevention and combating of cybercrime therefore requires effective international cooperation through an adequate treaty and well trained government and law enforcement personnel.

Today there are more Internet users located in developing countries than in developed ones.[5] In addition; the Internet offers small and medium enterprises, particularly, in small developing countries unique opportunities to connect with a global

[3] Websites of governments and corporations are the most attacked by cybercriminals using computer viruses.

[4] Mcafee Inc. (2013) "*A Good Decade for Cybercrime,*" www.mcafee.com,p.5 accessed on 22/1/2013 by 8:00pm.

[5]The United Nations Office on Drugs and Crime Study (2013) " Comprehensive Study on Cybercrime" (Draft, February 2013), Vienna International Centre,Vienna, Austria. See www.unodc.org. p.17.

marketplace.[6]In order to create both an enabling environment for enterprises and to protect users of Internet services in developing countries, it is necessary that treaties for the protection of internet users are put in place and the international community has a clear legal framework and sufficient law enforcement and technological capacities in place to effectively fight cybercrime[7] within all nations. There is also the need for the provision of effective support to foreign law enforcement agencies requesting international cooperation in cross-national cybercrime cases.

The Budapest Convention is the first and only treaty so far on cybercrime.[8]

The objectives of this chapter are to introduce the subject matter of the research work. This is achieved by discussing the statement of the problem, scope of the research, methodology of the research, literature review, organizational layout etce tera.

1.2 Statement of the Research Problem

Unlike traditional crime, cybercrime is a global crime. Nations around the world are very concerned about cybercrime, a concern shared by international organizations, including the United Nations, the G-8, the African Union, ECOWAS, the European Union and the Council of Europe, to mention a few. One important reason to be concerned about cybercrime is the problems faced by law enforcement officials and prosecutors in trying to apply existing laws on cyberspace/crime. Many legal challenges faced by law enforcement officials and prosecutors in pursuit of cyber criminals can be

[6] Ibid, p.6.
[7] Brenner, S.W. (2000)*" Cybercrime Investigation and Prosecution: the Role of Penal and Procedural Law"*26. University of Dayton Law School, Dayton,unpan1.un.org/../unpan003073.pdf. accessed on 13/4/13, 8:00pm.
[8]Michael A. V. (2010) "*The Council of Europe Convention on Cybercrime"* at http://www.nap.edu/catalog/12997.html, pp. 1-17. andhttp://hub.coe.int/what-we-do/rule-of-law/cybercrimeaccessed on 13/4/13, 8:00pm.

illustrated by the brief yet destructive career of the 'Love Bug' virus.[9]Law enforcement officials cannot take action against cyber criminals unless countries first enact laws which criminalize the activities in which these offenders engage and also cooperate in fighting cybercrime. As the "love bug" investigators learned, the existence of such laws and international cooperation is a fundamental prerequisite for investigation as well as prosecution. It would therefore seem obvious that all nations would have or at least desire to have cybercrime laws in the books. The difficulty lies in properly defining the laws needed to allow for cybercriminals' apprehension and prosecution. While seemingly a straight forward task, difficult issues are raised. One is whether the definitional scope of cybercrimes should include only laws that prohibit activities targeting computers or should outlaw crimes against individuals affected through the computer as well, such as cyber-stalking and cyber-terrorism. Another is whether these laws should be cybercrime specific, targeting only crimes committed by exploiting computer technology. Is it, for example, necessary for a country to add a "computer fraud" offence if it has already outlawed fraud? Both these issues are national in scope and only go to the nature of legislation a nation should adopt. Other issues are international in scope, pertaining to the impact a country's cybercrime laws, or lack of thereof have on other countries. For example, the Philippines' failure to have cybercrime legislation meant that a Philippine national could not be tried in any of the 20 countries to which he inflicted damage and thus suffered no consequences for his acts; the failure to have legislation against cybercrime was inadvertent, but its impact was felt around the globe.[10] The "love bug" episode illustrates how fragile our modern networked world is as anyone with a computer

[9] The virus which originated from the Philippines destroyed files and stole passwords', it appeared in Hong Kong on May 1, 2000 and spread rapidly throughout the world. The virus affected Newspaper companies in Germany, Banks in Belgium, internet connectivity in the Netherlands and Sweden, Microsoft, the parliament in London, the Senate in the US, Defense Apartment around the world, NASA and the CIA, to mention a few.

[10] Op cit, p. 1

and an internet connection, no matter where, can use software easily available on the internet to cause havoc somewhere else. Use of computers and internet has become a necessity for everyone.[11] Modern man, both rich and poor may certainly not function properly without computers and Internet. Many financial, Health, Administrative, Educational, Commercial and security process to mention a few depend on computers and internet. As computers have developed so has criminal offences associated with their use. Mankind will always have to live with criminal activity and "someday, every crime is going to be a cybercrime."[12] While some offences of cybercrime are prohibited in other countries, they are not prohibited in others. In essence, even though cybercrimes are not hindered by borders of nations, most countries are not equipped to fight them.

The following are some of the issues considered in this research:

1. Cyber jurisdiction is hard to determine. Even when a country stipulates punishment for cybercrimes within its Jurisdiction, the issue is how to determine cyber jurisdiction. Reaction to the challenges of jurisdiction posed by cybercrime is slow compared with the rate of development of cyber-criminal activity.
2. Existing laws on cybercrime in most nations are archaic or inadequate. Though the Nigerian Evidence Act, 2011 in section 84 prescribes how electronic evidence can be admissible, it does not cater for the admissibility of evidence obtained by forensic analysis of computer. This is in spite of the fact that computer generated evidence can easily vanish.[13]In the United States of America, the U.S. Department of Justice (DOJ) Officials have pointed out that Federal laws to prosecute computer related crimes are not ample or broad as

[11] See 'Philippines'' laws complicate Virus case, in USA Today(June 2000) http://www.usatoday.com/life/cyber/tech accessed on 13/4/13, 9:00pm.
[12] Brenner S.W. (2010) *"Cybercrime: Criminal Threats from Cyberspace,"* Praeger, an imprint of ABC-CLIO,LLC, Santa Babara, page 37 (Quoting the thoughts of Police Officer Colleagues)
[13] Brenner S.W., (2010) *"Cybercrime: Criminal Threats from Cyberspace",* Ibid p.1

those to confront their traditional counterparts, real world crimes.[14]This challenge also exists in Nigeria and other nations of the world.[15]

3. All over the world today, the development of the internet and proliferation of computer technology has created new opportunities for those who would engage in illegal activity.[16]The rise of technology and online communication has not only produced a dramatic increase in the incidence of criminal activity. It has also resulted in the emergence of what appears to be some new varieties of criminal activity. Both the increase in the incidence of criminal activity and the possible law enforcement, especially as cybercrimes are mainly transnational in nature.

Also, stemming from the above, there is the difficulty to determine how many offences have been committed, against whom and the damage resulting from those offences[17] and this has made cybercrime one of the top 4 economic crimes committed in the world today.[18]

The extent to which efforts are being made internationally to combat cybercrime will form the fulcrum of this study, having in mind the provisions of the Budapest convention on cybercrime (the Budapest Convention.)

[14] Kristine, M.F. et al. (2013) *"Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement"* Congressional Research Service, January, www.crs.gov page 4 accessed on 18/1/2013 by 8:00pm.
[15] Op cit., page 37.
[16]Mcafee Inc. (2013) *"A Good Decade for Cybercrime,"* ibid, p.1.
[17]Brenner S.W. (2010) ibid, p. 1.
[18]Global Economic Crime Survey United Kingdom, November, 2011, www.pwc.com/crimesurvey accessed on 19/4/14 by 8:00pm.

1.3 Objectives of the Research

This research intends to proffer solutions to the challenges posed by cybercrime through the template of the Budapest Convention. The Budapest Convention states as follows:[19]

> Effective law enforcement is complicated by the transnational nature of cyberspace. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cybercriminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cybercrimes.

This research highlights the relevance of international law in the fight against cybercrime, need for nations to cooperate and modernize their procedural law as well as their substantive law of crimes to include cybercrimes. Investigating computer-related crime is not an easy task, as most of the evidence is intangible and transient. Cybercrime investigators seek out digital traces, which are often volatile and short-lived. Legal challenges also arise owing to problems of borders and jurisdictions. The investigation and prosecution of computer-related crime highlights the importance of international cooperation.[20] Nations must therefore, also evaluate their procedural law governing evidence collection and analysis, amend existing legislation as necessary so as not to suffer many limitations and enhance international cooperation in combating cybercrime.[21]

This research aims at realizing the following one or more objectives:

1. To examine the factors responsible for the growing phenomenon of cybercrime.

[19] See the introductory pages of the Budapest convention.
[20] The Explanatory Report, council of Europe, convention on cybercrime, Europe, November 8, 2001, p. 171.
[21] United Nations Office of Drugs & Crime (2013) *"Computer-Related Crime"* www.unodc.org, www.11uncongress.org. p.2.accessed on 12th August, 2013 by 8:00pm.

2. To analyse the existing international legal response to the growing incidences of cybercrime and its impact on global and national economies and security.

3. To discuss the situation in some nations, i.e. Nigeria, the United Kingdom and the United States of America in the fight against cybercrime.

1.4 Scope of the Research

All over the world today cybercrime is a great challenge. In fact, cybercrime tops the agenda of most regional organizations[22] and they are making efforts to combat cybercrime.[23]The scope of this research covers various criminal laws in Nigeria, the United Kingdom, the United States of America, Canada and the Budapest Convention on cyber-crime,and how nations of the world can benefit from the Budapest Convention in the fight against cybercrime.

The Budapest Convention is in the fore front in combating cybercrime and as the time of this research, over 45 nations had subscribed to it.

1.5 Justification

When completed, it is the writer's expectation that this study will be of tremendous benefit to among others the following:

(a) Members of the Judiciary who will become informed and equipped to deal with issues of cyber offences, cyber jurisdiction and evidence relating to cybercrime.

(b) Legal practitioners, Academic writers and students who will become better equipped and informed to advise and represent clients, learn and carry out more research over issues of cybercrime.

---

[22] The African Union Division of Communication and Information is also making efforts to combat cybercrime. Seewww.africa-union.org

[23] The first West African Cyber Crime Summit was convened on 30th November, 2011 to 2nd December, 2011 in the Nigeria capital, Abuja. See Eccuni U., "West Africa to Fight Cybercrime - Online Computer Training Can Create IT Security Awareness", www.EzineArticles.com.2011. Accessed on 15th June, 2013 by 10:00pm.

(c) Members of the organized private sector, local and international business men and women who will become better informed as to their duties and responsibilities and how to handle issues involving cybercrime.

(d) Members of the general public who will become better acquainted with international laws regarding the use of computer, the internet and cybercrime.

(e) Encourage international cooperation in the fight against cybercrime.

1.6 Research Methodology

This research is based on the doctrinal and empirical methods of research. This study was carried out purposely to analyze the concept of cybercrime, cyber security and their challenges and provide adequate and sufficient ways of getting out of these challenges particularly by enhancing international cooperation in combating cybercrime, using the Budapest Convention on cybercrime as a template. The writer consulted the works of international and local authors on cybercrime, cyber security, its challenges and international efforts in combating cybercrime. The success achieved so far by the Budapest Convention in enhancing international cooperation against cybercrime was also studied.

This research work will rely on primary and secondary sources. Primary sources to be consulted are statutes and case laws. Statutes such as the Penal Code law Cap. 110 laws of Kaduna State 1991, the Criminal Code Cap. Act C38 LFN 2004, the Economic and Financial Crimes Commission (EFCC) Act 2004, the Anti Terrorism Act 2013 (as amended), the Advance Fee Fraud Act, 2006, Money Laundering Act, 2012,the Evidence Act, 2011, the National Identity Management Commission (NIMC) Act, 2007, the Cybercrime Act, 2015and draft African Union Convention on the establishment of a Credible Legal Framework for Cyber security in Africa and from the United Kingdom, the Computer misuse Act, 1990 the Criminal Justice Act 1978, the Police and Justice Act,

2006 and the Protection of Children Act, 1978. Secondary sources to be consulted include materials from the internet, seminar papers, books, articles and newspapers materials, etc.

1.7 Literature Review

Many authors and scholars have written on cybercrime and international cooperation in combating cybercrime under the Budapest Convention or generally. These authors differ in their approach to international cooperation in combating cybercrime but in most cases, share similar views on cybercrime.

The works of these authors and scholars shall be reviewed in the course of this work. In this work, Sekav Stephen Dzever will be referred to as "the writer".

Ladan, M.T. an erudite professor of Law at Ahmadu Bello University, Zaria in his book published in 2015 and titled "*Cyberlaw and Policy on Information and Communications Technology in Nigeria and ECOWAS*"[24] gives highlights of cyberlaw in West Africa. Decisions of the United Nations and other world regional bodies on cybercrime are discussed. The writer observes that the erudite professor of law does not show how the Budapest convention which is the first treaty on cybercrime can be of benefit in international cooperation against cybercrime. On the other hand, this work shows the benefits of the Budapest Convention in combating cybercrime in the ECOWAS region.

Ani, L., a Research Fellow, Nigerian Institute of Advanced Legal Studies in her article titled "*Cyber Crime and National Security: the Role of the Penal and Procedural Law*"[25] argues that law enforcement officials cannot effectively pursue cybercriminals unless they have the legal tools necessary to do so. The author also carries out a

[24]Ladan M.T. (2015) *"Cyberlaw and Policy on Information and Communications Technology in Nigeria and ECOWAS*" ABU Press Ltd., Zaria.
[25]Ani, L. (2011) in "*Law and Security in Nigeria*", Professor Azinge, E., SAN, et al (eds.) Nigerian Institute of Advanced Legal Studies Press, Lagos, 2011,pp. 197-234.

comparative analysis and critical review of Jurisdictions such as the USA, UK, India and Nigeria, if the existing Laws are adequate to combat cybercrime and consequently, if amendments need to be put in place. The Author states that lack of cybercrime specific laws and inadequate equipment of law enforcement agencies militate against the fight against cybercrime. The author also seeks to lay a roadmap for Nigeria's accession to the Budapest Convention. In considering relevant laws in fighting cybercrime in Nigeria, the author does not consider the relevant provisions of the Anti Terrorism Act 2013 (as amended), the Advance Fee Fraud Act, 2006, Money Laundering Act, the National Identity Management Commission (NIMC) Act, 2007 and the cyber crime Act, 2015which is Nigeria's effort to key into the international fight against cybercrime.

Asma A.I. V. in his paper title "*Facebook Advertisements: Of Relational Materiality, Rituals of Consent, And Data Commodification*"[26]only discusses issues of privacy and consent to agreement page on social networking sites like Facebook and Youtube. The author highlights the need to make agreement pages of these social networks to conform laws of nations and individual needs of the parties signing up to these networks.

Guillaume, L., et al. in their article titled "*Fighting Cybercrime: Technical, Juridical and Ethical Challenges*,"[27] an article reviewed by parties with technical, legal, or law-enforcement backgrounds sheds light on those aspects, and attempt to proffer solutions to issues raised by cybercrime. Some of the issues raised include if we need more international cooperation processes? Would an 'Inter(net) pol' be the solution, or is everything we need already there at a juridical level, as we are only lacking will, knowledge, and concrete collaboration between deciders and experts? Could we end up endangering liberties in the process of addressing cybercrime? The authors state that

[26] 26. Electronic copy available at: http://ssrn.com/abstract=2731159 accessed on 9/3/2016 by 10:00am.
[27] Virus Bulletin Conference, September, 2009

increasing the level of international cooperation and equipment of law enforcement agencies would enhance the fight against cybercrime. They posit that the Budapest Convention is likely to be the 'way to go' in the struggle against transnational cybercrime.[28]The writer observes that though this article is apt on the issues concerning the Budapest Convention and cooperation against cybercrime it does not deal with issues of international cooperation, solutions for challenges of law enforcement agencies and judicial systems in combating cybercrime.

Stefan, F. in his report titled "*UK Cybercrime report*",[29]a report from criminologists from specialist consultancy firm 1871 Ltd. focuses on an estimated quantification of cybercrime in the United Kingdom. It discusses the cost and effect of cybercrime on the Citizens of the United Kingdom. It also discusses relevant laws in the United Kingdom for combating cybercrime. The writer observes that this report however, does not consider the possibility of cybercrimes like cyber terrorism or cyber warfare in spite of increase in use of the internet by terrorists to facilitate terrorism.

Okonigene, R. E., et al. in their article titled" *Cybercrime in Nigeria*"[30] discuss cybercrime vis-à-vis the Economic and Financial Commission Act, 2004 and the Criminal code as laws available to combat cybercrime in Nigeria. The authors state that the internet as an instrument to aid crime ranging from business espionage, to banking fraud, obtaining un-authorized and sabotaging data in computer networks of some key organizations. The writer observes that even though the authors claim to have examined the inadequacies of the existing laws in combating cybercrime in Nigeria and proffer solution, they only consider two laws of Nigeria, i.e. the EFCC Act and the Criminal code

[28] Ibid, pp. 68-70.
[29] See www.garlik.com/file/cybercrime_report accessed on 12/1/14 by 11:00pm.
[30] See www.saycocorporativo.com/saycoUK/BIJ/journal/Vol3No1/Article_7 accessed on 12/1/14 by 10:00pm.

in considering the relevant laws to fight cybercrime in Nigeria and their research is limited to Nigeria.

PricewaterhouseCoopers LLP in the article titled "*Cybercrime: protecting against the growing threat*"[31] study the impact of cybercrime on organizations, their awareness of the crime and what they are doing to combat the risks. It also studies fraud, the fraudsters and the defrauded-the types of economic crimes committed, how they are detected, who is committing them and what the repercussions are. The writer observes that though this article gives a great insight on the effect of cybercrime on businesses its scope limited to the United Kingdom.

Andy, B. et al. in their article titled "*What Role and Responsibility Does the Government Have in Protecting Consumer's Rights to Privacy/Security on the Internet*?,"[32]analyze the role of government in protecting its citizens from internet fraud. Though the authors advocate that governments should give adequate enlightment to the members of the public, they do not show how the governments can unite to fight cybercrime globally. The writer observes that there may be a need to caution internet users to serve as a way to enlighten them on the risks of using the internet but does not show how nations of the world can unite against cybercrime.

Micheal, A. V. in his article titled "*The Council of Europe on Cybercrime'. Proceedings of a workshop on Deterring Cyber attacks: Informing Strategies and Developing Options for U.S. policy"*[33]analyses the Budapest convention on Cybercrime and its role and effects on cooperation among nations in the fight against Cybercrime. The writer states that this article serves as one of the highlights on how the U.S.

[31] Global Economic Crime Survey United Kingdom, November, 2011, www.pwc.com/crimesurvey accessed on 23/1/14 by 8:00pm.
[32]Toby F. et al (eds.) (2010) *"The Future Challenges of Cybercrime"* Vol.5 Proceedings of the Futures Working Group. Quantico, Virginia.
[33] Seehttp://www.nap.edu/catalog/12997html accessed on 12/1/14by 8:00pm.

government is keying into the Budapest Convention in the bid to rid the country of cybercrime. The article however does not show how nations of the world can be signatories to the convention.

Brenner, S.W. in her book titled "*Cybercrime investigation and Prosecution: the role of Penal and Procedural Law*,"[34]argues that law enforcement officials cannot effectively pursue cybercriminals unless they have the legal tools necessary to do so. These legal tools include an arsenal of well-defined cybercrime offenses for use in prosecuting cybercriminals and procedural rules governing evidence-gathering and investigation. Because cybercrime is often transnational in character, offenders can take advantage of gaps in existing law to avoid apprehension and/or prosecution. It is, therefore, important that every legal system take measures to ensure that its penal and procedural law is adequate to meet the challenges posed by cybercrimes. The writer observes that the focus of this author is only on law enforcement agents and how they can be trained to fight cybercrime. International cooperation in fighting cybercrime like nations assisting each other in the fight against cybercrime is not discussed by the author.

Data Protection and Cybercrime Division of the Council of Europe in a document titled "*Global Project on Cybercrime: Cooperation against Cybercrime in 2012, Activities of the Council of Europe*."[35] gives us an insight on the efforts of the Council of Europe in 2012 and how far the Budapest Convention on Cybercrime has assisted in the global fight against cybercrime.

It is the observation of the writer that though this document is pivotal in showing the relevance of the Budapest convention in the fight against cybercrime, it does not show how the Council of Europe intends to ensure that other nations of the world become party to the only treaty on cybercrime.

[34] University of Dayton Law School, Dayton,unpan1.un.org/../unpan003073.pdf accessed on 12/3/2-13 by 8:00pm.
[35] See ijlit.oxfordjournals.org/content/10 accessed on 24/5/13 by 9:00pm.

Marc D. G. and Brenner S. in their book titled *"The Emerging Consensus on Criminal Conduct in Cyberspace"*[36]analyse the challenges of archaic procedural and substantive law in fighting cybercrime. These issues are the focus of this article; it examines how they are being addressed at the national and international levels and assesses the measures that are being taken in an effort to resolve them. The writer observes that the authors also do not discuss the Budapest convention as a tool of international cooperation against cybercrime.

Alexander, S. in the article titled "*Budapest Convention on Cybercrime* "[37]gives guidelines for harmonized international legislation on cybercrime, framework for international cooperation and vector for capacity building. The writer states that this article which is on the Budapest Convention highlights its relevance in the fightagainst cybercrime but does not discuss how enforcement agents can be equipped in the fight against cybercrime.

"*A Good Decade for Cybercrime*"[38] by McAfee Incorporation looks back at ten years of cybercrime. This article explains that despite a global recession, improved security and international crackdown efforts, cybercrime has thrived over the last decade, growing by double digits year after year. In this article, the author analyses types of cybercrime and circumstances promoting its growth for the past ten years. The writer observes that this article shows how cybercrimes increased over the last decade. It also emphasizes the need for knowledge of these crimes by individuals to enable them protect themselves from these crimes but does not emphasize making of treaties in the fight against the menace of cybercrime.

[36] See www.coe.int/cybercrime, Strasbourg,7 December,2012 accessed on 24/5/13 by 9:00pm.
[37] See www.cto.int/.../Alexander Sager-... accessed on 24/5/13 by 9:00pm.
[38] Mcafee Inc.(2010) '*A Good Decade for Cybercrime,*' www.mcafee.com,p.5

Kristine M.F. et al in the book titled *"Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement"*[39]discuss the efforts made by the U,S congress for over three decades in combating cybercrime and its related threats. This book also discusses the concept of cybercrime and related cyber threats such as cyber espionage and cyber warfare. While it touches on these related threats, this book only does so in the context of framing the discussion of cybercrime. The book also outlines how current federal strategies may address cybercrime. It raises issues surrounding the measurement and tracking of cybercrime. The writer observes that though this book gives an insight on how the United States of America (U.S.A) grapple with the challenges of cybercrime, the scope of the work is only the U.S.A.

Adejoke O. O. in the work titled "*The ICT Revolution and Commercial Sectors in Nigeria: Impacts and Legal Interventions*"[40]examines the impacts and challenges of information and communication technology in diverse aspects of commerce, banking and business activities in Nigeria. Against the background of international standards, the paper discusses emerging legal responses aimed at safeguarding the security and integrity of online transactions, and promoting certainty in the outcomes of dealings carried out through the medium. The paper concludes that while ongoing legislative interventions are desirable, the highly fragmented nature of emerging ICT laws and multi-layer regulatory institutions will unnecessarily complicate the legal and institutional landscape, and defeat the purpose of certainty and simplicity. The writer observes that though the author discusses some bills on cybercrime and electronic fraud which were pending before the Nigerian National Assembly, the author does not discuss the Budapest Convention and how it can be useful in Nigeria's efforts at international cooperation in the fight against cybercrime.

[39] Congressional Research Service, January, 2013, www.crs.gov accessed on 23/5/13 by 8:00pm.
[40]British Journal of Arts and Social Sciences, Vol.5 No.2, British Journal Publishing, Inc. 2012. http://www.bjournal.co.uk/BJASS.aspx accessed on 4/4/13 9:00pm.

The United Nations Office on Drugs and Crime Study title *"Comprehensive Study on Cybercrime" (Draft, February 2013)*"[41] is a study prepared with a view to examine options to strengthen existing laws on cybercrime and to propose new national and international legal or other responses to cybercrime. In this respect, the focus of the Study is limited to the *crime prevention* and *criminal justice* aspects of preventing and combating cybercrime. The Study represents a 'snapshot' in time of crime prevention and criminal justice efforts to prevent and combat cybercrime. It paints a global picture, highlighting lessons learned from current and past efforts, and presenting possible options for future responses. While the Study is, by title, a study on 'cybercrime', it has unique relevance for *all* crimes. The writer observes that though this detailed study discusses national legislation, best practices, technical assistance and international cooperation in combating cybercrime and crime generally it does not show how to address the challenge of cyber jurisdiction.

Gbenga S. et al in the article title *"Economic Cost of Cybercrime*"[42] discuss the effect of cybercrime on the Nigerian economy, efforts of the Nigerian National Assembly to provide laws to fight cybercrime and the need to fight cybercrime to encourage e-trade and salvage the nation's battered image.[43]Though the writer discusses the cost of cybercrime to Nigerian consumers, he does not postulate how to nip it in the bud as propose in this work.

Yusuf I. A. in "*The New Phenomenon of Phishing, Credit Card Fraud, Identity Theft, Internet Piracy and Nigeria Criminal Law"*[44]discusses the cybercrime of phishing and how the EFCC and other law enforcement agencies are tackling the cybercrime in

[41]See www.unodc.org accessed on 12/1/14 by 7:00pm.
[42]A report for the Cyber Stewards Network project of The Citizen Lab, Munk School of Global Affairs, University of Toronto.
[43]Ibid, p.11.
[44]See unilorin.edu.ng/… accessed on 15/3/2013 by 8:00am.

Nigeria. Though this article shows attempts by the EFCC to prosecute cybercrime, it does not address the issue of inadequate cybercrime legislation in most nations of the world.

Jonathan C. in his book titled *"Principles of Cybercrime"*[45]gives a deeper understanding of the legal principles which are applied to 'cybercrimes', whether they be academics, legal practitioners, law enforcement officers or students. The unique feature of this book is that the various offences are analyzed across four major common law jurisdictions: Australia, Canada, the United Kingdom and the United States. The writer observes that aside from jurisdictional issues, the author does not address the law of criminal investigation, procedure or evidence and it is restricted to issues of cybercrime in Canada, United States and the United Kingdom only.

Scott J. S. and Scott R. in "*Operationalizing Cybersecurity Due Diligence: A transatlantic comparative case study"*[46] compares how the United States of America and the European Union are handling issues of due diligence in issues of cybersecurity. In this paper with the scope of the United States of America and the European Union, the authors do not discuss the role of the Budapest convention is cybersecurity due diligence or how the convention can be relevant in cybersecurity due diligence.

Ric S. in the paper title "*The Failure of the Computer Fraud and Abuse Act: Time to Take a New Approach to Regulating Computer Crime*"[47]using the Computer Fraud Abuse Act of the United States as a case study discusses how to tackle inadequacy of laws in fighting cybercrime. The author proposes that instead of enacting new laws every time a new cybercrime is discovered, an agency of the government saddle with responsibility to make regulations to curtail cybercrime should be created. The author

[45]See www.cambridge.org/.../principles accessed on 15/3/2013 by 8:20am.
[46]University of South Carolina Law Review, 2016 available at http://ssrn.com/abstract=2714529, accessed on 16/2/16 by 10:00pm.
[47]George Washington Law Review, forthcoming Public Law and Legal Theory Working Paper Series No. 329, accessed at http://ssrn.com/abstract=2726662 on 16/3/2016 by 8:00pm.

however does not discuss a holistic approach to fighting cybercrime in international community.

Garon, J.M. in *"2015 Cyber law Year in Review – Seeking Security Over Privacy, Finding Neither"*[48] discusses highlights of cybercrimes and challenges of cybercrime for the United States in the year 2015. This work shows the dimension cybercrimes are taking but the scope of the work is the United States, Asia and Europe.

From all the literature review discussed above, the writer observes that all the authors see cyber jurisdiction as a great challenge in combating cybercrime. The writer through this research proposes a solution to the challenge posed by cyber jurisdiction by enhancing international cooperation and also show how the source of the challenge, i.e. the internet can be a solution to the challenge.

1.8 Organizational Layout

There are five chapters in this research work with subheadings discussed there under.

Chapter one deals with the general introduction under which the background of the study, statement of the problem, objectives, scope, and methodology are stated. It also discusses a vivid literature review of some existing literatures on the subject matter.

In chapter two, the relevant key terms involving cybercrime and international cooperation in its fight are to be clarified.

Chapter three takes a critical analysis of the legal and institutional frameworks relevant for international cooperation in combating cybercrime. This chapter uses Nigeria as a case study.

[48]Electronic copy available at: http://ssrn.com/abstract=2707756 accessed on 15/3/2016 by 8:00pm.

Chapter four discusses the Budapest Convention and its nature, significance, scope, impact and prospects for nations in combating cybercrime through necessary cooperation and collaboration with both regional and global partners.

Chapter five deals with findings, conclusions and recommendations.

CHAPTER TWO

CONCEPTUAL CLARIFICATION OF KEY TERMS

2.1 Introduction

The objective of this chapter is to clarify key terms used in law by defining the concepts of cyber law, cybercrime, cyberspace and cyber jurisdiction and their meanings as conceived by some authors and the writer. The work will further discuss the perspective of the Nigerian Judiciary on these concepts. This chapter will also highlight cybercrimes committed in Nigeria and classified as cybercrimes under the Budapest Convention. These acts are discussed because the individuals whom carry them out through the internet, cause injury to other individuals or the society at large. In discussing these acts or omissions, the writer will consider the provisions of the Cybercrime Act, 2015. The Act is meant to criminalize these acts or omissions in Nigeria. Some terms clarified in this chapter have their origin in science.

2.2 Meaning of Cyber-law

The word cyber is a combining form meaning "computer," "computer network," or "virtual reality," used in the formation of compound word (cybertalk; cyberart; cyberspace, etc) and by extension meaning "very modern."[1]

Law is a term which does not have a universally accepted definition,[2] but one definition is that law is a system of rules and guidelines which are enforced through social institutions to govern behavior.[3] Laws can be made by legislatures through legislation, the executive through decrees and regulations, or judges through binding precedents

[1]See http://dictionary.reference.com/browse/Cyberaccessed on 23/9/13 by 5:00pm.
[2]Chukkol, K.S. (1988) "The Law of Crimes in Nigeria"(1st Edition) Ahmadu Bello University, Zaria, 1988, p.1.
[3]See definitions.uslegal.com/c/cyber-law/-Cyber Law & Legal Definition accessed on 23/1/13 by 10:00pm.

(normally in common law jurisdictions). The formation of laws themselves may be influenced by a constitution (written or unwritten) and the rights encoded therein.

Cyber-law is a rapidly evolving area of civil and criminal law as applicable to the use of computers, and activities performed and transactions conducted over internet and other networks. This area of law also deals with the exchange of communications and information thereon, including related issues concerning such communications and information as the protection of intellectual property rights, freedom of speech, and public access to information.[4] In the writer's opinion, cyber-law is basically rules and regulations established by the Federal or State Legislatures, courts, and international conventions to govern conduct in cyberspace or prevent and resolve disputes and crimes that arise from the use of computers and the Internet.

2.3 Meaning of Cyber-crime

Section 2 of the Criminal Code of Nigeria defines crimes as acts or omissions which render the person doing the act or making the omission liable to punishment under the Code or under any other Act or law.

Various writers have also made attempts to define what crimes are.

Glanville Williams defines crimes as follows:[5] "a legal wrong that can be followed by criminal proceedings which result in punishment"

Okonkwo et al, define crimes by way of procedure used in hearing criminal matters and civil matters. They conclude that crimes or civil actions can only be defined by way of procedures involved in the hearing of the matter.[6]

[4]See http://definitions.uslegal.com/c/cyber-law/-Cyber Law & Legal Definition**,** 2013 accessed on 23/1/13 by 10:00pm.
[5] Glanville W. (1983) "*The Text Book of Criminal Law*", 2nd ed. Stevens & Sons London, p.27.
[6] Okonkwo, N. et al (1994) "*Criminal Law in Nigeria*," 2nd ed. Spectrum Law Publications, Ibadan.

The writer defines crimes as act(s) or omissions prohibited by written law which also specify punishment(s) for them.[7]

The word cyber-crime is a hybrid word. It is made of "cyber" and "crime". According to Sackson, M. [8] cyber-crime is a crime that is committed with the help of a computer through a communication device or a transmission media called the cyberspace and global network called the Internet.

The Commonwealth Organisation,[9]states that cyber-crime includes not only crimes against computer systems (such as hacking, denial of service attacks and the set up of botnets) but also traditional crimes committed on electronic networks (e.g. fraud via phishing and spam; illegal Internet-based trade in drugs, protected species and arms) and illegal content published electronically, (such as child sexual abuse material). The author states that cybercrime is any offence carried out involving the use of computers and the internet.

In International Actions Against Cybercrime: Networking Legal Systems in the Networked Crime Scene,[10]cyber-crime is defined as criminal activity involving an information technology infrastructure: including illegal access; illegal interception that involves technical means of non-public transmissions of computers data to, from or within a computer system; data interference that include unauthorized damaging, deleting, deterioration, alteration or suppression of computer data; system interference that is interfering with the functioning of a computer system by inputting, transmitting,

[7] This definition is premised on the provision of Section 36(8) of the 1999 Constitution of Nigeria (as amended).

[8] Sackson, M. (1996) " *Computer Ethics: Are Students Concerned*" First Annual Ethics Conferenceavailable online athttp://www.maths.luc.edu/ethics96/papers/sackson.doc**.** accessed on 12/2/13 by 8:00pm.

[9] Commonwealth Internet Governance Forum *"Commonwealth Cybercrime Initiative"* http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. accessed on 12/2/13 by 8:00pm.

[10] International Actions Against Cybercrime: Networking Legal Systems in the Networked Crime Scene, in Xingan Li,(Ed.) Webology, Vol. 4, No. 3, 2007. pp.2-6.

damaging deleting, deteriorating, altering or suppressing computer data; misuse of devices, forgery (identity theft), and electronic fraud.

In Botnets, Cybercrime, and Cyber terrorism: Vulnerabilities and Policy Issues for Congress, cyber-crime is defined as crime that is enabled by, or that targets computers.[11]

According to Chik, W.B.[12]cybercrimes are to be distinguished from computer-enabled crimes. They relate to crimes against computer hardware as well as the digital contents contained within it such as software and personal data. Computer enabled crimes have an adverse effect on the integrity and trust in information technology infrastructure such as computer or telecommunications networks and in the security of transactions conducted through them.

"Computer crimes" is often used to define any criminal activities that are committed against a computer or similar device, and data or program therein. According to Chik W.B.[13]and Longe, O.[14], et al, in computer crimes, the computer is the *target* of criminal activities.

The writer's comprehension of cyber-crime is that it is a crime carried out by criminal minded individuals or computers enabled by criminals who use computers and internet enabled devices like smart phones, ipads, etc. to commit crimes through the internet from any location at any location.[15]

[11]Clay, W. (2008) "*Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress,"* CRS Report for Congress, p.7.
[12]Chik, W.B. (2007) *"Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore*", Icfai law books, http://works.bepress.com/warren_ p.4.
[13]Ibid. p.7
[14] Longe, O. et al (2005) "*Implications of the Nigeria Copyright Law for Software Protection"* in the Nigerian Academic Forum Multidisciplinary Journal. Vol. 5, No. 1, pp. 7-10.
[15]The writer's opinion is premised on the fact that cybercrimes are carried out by individuals or by computers programmed by individuals for the purpose of carrying out cybercrimes. This definition also reflects the fact that cybercrimes are borderless crimes.

The writer opines that the categorization of cybercrime into computer crimes and computer enabled crime by some writers[16]overlooks the fact that it is a human being with criminal intent (*mens rea*) that programs a computer to perpetuate a computer enabled crime. Thus, the categorization of cybercrimes as crimes enabled by computers is misleading. The writer subscribes to the position of the Commonwealth Organization on cyber-crimes.[17]

Criminal-minded individuals carry out acts or omissions which harm individuals every day in cyberspace. Criminal-minded individuals that indulge in the advance fee fraud schemes are now popularly called "Yahoo Boys" in Nigeria.[18]Nigeria has therefore carved a niche for herself as the source of what is now popularly called 419-mails, named after Section 419 of the Nigerian Criminal Code Act Cap. C 38, LFN 2004 which forbids advance fee fraud. In fact, Nigeria is ranked first in Africa as the target and origin of malicious cyber activities; and this is spreading from the West African sub-region with Ghana also gaining prominence in cybercrime which is popularly referred to as "*Sakawa*" in Ghana.[19]

2.4 Meaning of Cyberspace

This is an attempt to find the meaning of a virtual eco system and it would involve delving into fields of study which are not law related.

According to Chip M. and Randall F. F., cyberspace is defined more by the social interactions involved rather than its technical implementation.[20]

---

[16] See Chick W. B., ibid, p.4 and Longe, O. et al, ibid, pp.7-10.
[17] See Commonwealth Internet Governance Forum "Commonwealth Cybercrime Initiative" Ibid.
[18] Longe O. et al, Ibid , pp. 7-10.
[19] Ribadu, N. (2007) "*Cybercrime and Commercial Fraud: A Nigerian Perspective*" a presentation at Modern Law for Global Commerce Congress to celebrate the fortieth annual session of UNCITRAL Vienna.
[20]Wadrip, F. and Nick, M. (eds.), (2003) *"The Lessons of Lucasfilms Habitat: The New Media Reader,"* the MIT Press, pp. 664-667.

Cyberspace is a word that began in science fiction literature in the 1980s, was quickly and widely adopted by computer professionals as well as hobbyists, and became a household term in the 1990s. During this period, the uses of the internet, networking, and digital communication were all growing dramatically and the term "cyberspace" was able to represent the many new ideas and phenomena that were emerging.[21]

The parent term of cyberspace is "cybernetics", derived from a Greek word which means steersman, governor, pilot, or rudder.[22]

As a social experience, individuals can interact, exchange ideas, share information, provide social support, conduct business, direct actions, create artistic media, play games, engage in political discussion, and so on, using this global network. The term 'cyberspace' has become a conventional means to describe anything associated with the Internet and the diverse Internet culture.[23]

As an internet metaphor, cyberspace should not be confused with the Internet, the term is often used to refer to objects and identities that exist largely within the communication network, so that a Website, for example, might be metaphorically said to "exist in cyberspace." According to this interpretation, events taking place on the internet are not happening in the locations where participants or servers are physically located, but "in cyberspace.[24]

Firstly, cyberspace describes the flow of digital data through the network of interconnected computers: it is at once not "real", since one could not specifically locate it as a tangible object, and clearly "real" in its effects. Secondly, cyberspace is the site of computer-mediated communication (CMC), in which online relationships and alternative forms of online identity were enacted, raising important questions about the social

[21]Ibid, p.1
[22]This word was coined by Norbert Weiner, an American and renowned Mathematician and Cybernetic
[23] This has become the norm hence the internet is a virtual ecosystem.
[24]Graham, M. (2014) *"Geography/Internet: Ethereal Alternate Dimensions of Cyberspace or Grounded Realities?"* in the Geography Journal, vol. 179, no. 2, pp. 177-188.

psychology of internet use, the relationship between “online and “offline” forms of life and interaction, and the relationship between the "real" and the virtual.[25] Cyberspace draws attention to remediation of culture through new media technologies: it is not just a communication tool but a social destination, and is culturally significant in its own right. Finally, cyberspace can be seen as providing new opportunities to reshape society and culture through "hidden" identities, or it can be seen as borderless communication and culture.[26]

Computers and electronic devices communicate through cyberspace. Cyberspace also brings together every service and facility imaginable to expedite all cyber-crimes. For example, in money laundering, one can purchase anonymous credit cards, bank accounts, encrypted global mobile telephones, and false passports. From there, one can pay professional advisors to set up IBCs (International Business Corporations, or corporations with anonymous ownership) or similar structures in OFCs (Offshore Financial Centers). Such advisors are loath to ask any penetrating questions about the wealth and activities of their clients, since the average fees criminals pay them to launder their money can be as much as 20 percent.[27]

The writer sees cyberspace is a creation of science and a medium through which all electronic devices and computers interact and transmit data. This is as the medium through which computers get internet network, television operates, GSM service providers transmit data, etc is electronically.[28]

[25] Ibid, 177-188.
[26] Ibid, 177-188.
[27] Ibid, 177-188.
[28] *Elelu-Habeeb vs. A.-G., Fed.* 2012 13 NWLR (part 1318), 423 at 440, paragraphs D- E.

2.5 Meaning of Cyber jurisdiction - What is Jurisdiction?

According to The Encyclopedia America[29]jurisdiction is defined as follows:

> power or authority. It is usually applied to courts and quasi-judicial bodies describing the scope of their right to act. Jurisdiction in the sense of judicial power, often describes the general authority of a court to hear and determine controversies and to carry its judgment in to effect. In this abstract sense it does not relate to particular case, but instead refers to the scope of courts, capacity to act within certain geographical boundaries and in connection with various kinds of legal controversies. In a more limited sense, jurisdiction means the power of a court to make valid and binding determination in particular controversy. This kind of jurisdiction relates solely to the court's authority in terms of the specific subject matter and property which are involved in the case under consideration.

Encyclopedia Britannica[30]defines jurisdiction as follows:

> Jurisdiction in general, the exercise of lawful authority, especially by a court or a judge and so that extent or limits with which such authority is exercisable. It has primarily a territorial signification, but where its power are otherwise limited, it is rather a matter of competence and in system of law based on codes this distinction is more clearly evident than it is in English and U.S. law.

Nigerian perspective of jurisdiction is similar to that of the British.[31]

In the writer's opinion, jurisdiction is the territorial and or inherent power of a court or a judge to adjudicate over an issue brought before them.

Any matter decided by a court without jurisdiction is a nullity no matter how well decided. The Nigeria Supreme Court has observed that "Any defect in competence is fatal, for the proceedings are a nullity however well conducted and decided; the defect is extrinsic to the jurisdiction.[32]

---

[29]Golak P. S. (2009) "*Jurisdictional Jurisprudence and Cyberspace"* in: Assam University Journal of Science &Technology: Physical Sciences and Technology Vol. 4 Number II, p. 58.
[30] Ibid., p. 58.
[31] Nigeria was a British Colony and as such, derived most of its jurisprudence from Britain.
[32] For example, Section 251 (1) (q) and (r) of the Nigerian 1999 Constitution vests Jurisdiction over matters involving the Nigeria Federal Government exclusively in the Federal High Court.

In a wider sense, the expression 'jurisdiction' does not mean the power to do or order the act impugned but generally the authority of the judicial official to act in the terms of subject matter, the prescriptive matter, the pecuniary and the territorial aspects.

A court may be given exclusive jurisdiction in respect of a particular subject matter by the Sovereign, or the constitution or statute, and it may prescribe restrictions/constraints in respect of the pecuniary or the territorial aspects.[33]In exercising the jurisdiction conferred on a court, a Judge has no power to expand its jurisdiction, but he can only expound the jurisdiction conferred on him.[34]Therefore, the court need not always have an unfettered and uncircumcised authority to deal with even a particular subject matter. However, jurisdiction to entertain the suit is different from the point of maintainability of the suit. The court may have jurisdiction to entertain a suit in relation to the grievances made by the plaintiff yet the suit as filed may not be maintainable for various reasons. Similarly a suit may be otherwise maintainable, yet the court in which the suit is instituted may not have jurisdiction to entertain the same.[35]

2.5.2 Cyberspace and Jurisdiction

Generally, the question of jurisdiction when a cybercrime offender has been detected is complex.[36] Electronic impulses may cross many jurisdictional boundaries before hitting their targets or bringing about the responses they seek. A cybercriminal can sit in one country, route electronic communications through several others, commit a crime in another and park the proceeds in yet another. Offences may be committed in several countries along the way. Decisions may have to be made about where the perpetrator may be amenable to justice and what offences should be prosecuted, under

[33]*Elelu-Habeeb vs. A.G., Fed*., (ibid)p. 443 paragraphs B-E.
[34] In Nigeria, if any ingredient of jurisdiction is lacking at any point of the matter, the court immediately, automatically lacks jurisdiction to entertain the matter.
[35] This is because this is because the cybercriminal might have committed the crime via a website hosted in another country in another country.
[36]

what law (and where) in the general public interest. Practical considerations such as the effective obtaining of evidence may impact on those decisions.

General issues of jurisdiction also apply – is it sufficient that an act occurs in the jurisdiction; is a national subject amenable to the jurisdiction of his or her citizenship, wherever the offence occurs; and so on.

It is believed that the law courts are the last hope of the common man, hence the saying that, *'Ubi jus ebi remedium'*- there is a right and there is a remedy. Criminal acts carried out in cyberspace through the internet affect people daily. In the last two decades, the pervading impact of information technology being a transnational character poses a serious threat to the administration of justice. Hence, the question is: 'which courts would have jurisdiction to adjudicate over a crime committed by a cybercriminal against an individual on the internet, via cyberspace, a vast distance between them and connected by two computers at both ends?[37]A widely recognized view which is gaining ground is that the existing law of jurisdiction is redundant for cyberspace and an entirely different set of rules are required to govern the jurisdiction over the internet which is free from the shackles of geographical borders.

To analyze the issue of cyber jurisdiction, the writer discusses jurisdiction generally and cyber jurisdiction specifically. Three countries, namely, the Unites States of America,[38]United Kingdom and Nigeria would be the focus of this discussion. The analysis may in some cases, cover scenarios involving complex civil matters involving the internet in which cyber jurisdiction had to be determined.

2.5.3 Determinants of jurisdiction in the United States, United Kingdom and Nigeria

[37] Ground-breaking technological inventions are created every day. Also, Internet connectivity is becoming easily available in Nigeria.

[38] Brenner, S.W.(2000) "*Cybercrime investigation and Prosecution: the role of Penal and Procedural Law",* University of Dayton Law School, Dayton,unpan1.un.org/../unpan003073.pdf .

This discussion is based on factors responsible when considering if a court has jurisdiction to hear a matter involving cybercrime. For the United States and England (which are bound by the Budapest Convention), instances of cyber jurisdiction are discussed, while for Nigeria (which is not a signatory to the Budapest Convention and just passed its cybercrime specific laws in 2015) references would be made to case law on general jurisdiction of courts in Nigeria. Some of the case laws referred to in this discussion are *locus classicus* cases on jurisdiction generally or cyber jurisdiction in the countries where they were determined. In this context, the term "jurisdiction' in fact conceals three distinct concepts which require separate discussion as follows:[39]

i. Prescriptive Jurisdiction

ii. Adjudicative Jurisdiction

iii. Enforcement Jurisdiction

2.5.4 Prescriptive Jurisdiction

Prescriptive jurisdiction is also known as subject matter or legislative jurisdiction.

According to the U.S. Constitution, the lawsuits can be brought either in a state or a federal court, provided that the state in which the court is located must have a long-arm statute which allows the court to assert jurisdiction over a non-resident defendant. Although these statutes will differ from state to state, Fifth and Fourteen Amendments of the U.S. Constitution lay down the outer limits for the courts while asserting jurisdiction.[40] Courts in the U.S., England and Nigeria have evolved various principles to measure the legitimate exercise of judicial power over the parties to the litigation.[41]

---

[39]Golak P. S. (2010)*"Jurisdictional Jurisprudence and Cyberspace"* (ibid), pp.59-65. The America perspective of cyber jurisdiction as discussed in this research is as discussed in this reference.

[40] This is a statute that enables local courts in the U.S. to exercise jurisdiction over foreign defendants, whether on a statutory basis or through a court's inherent jurisdiction. This jurisdiction permits a court to hear a case against a defendant and enter a binding judgment against a defendant residing outside the jurisdiction concerned.

[41] This means that before asserting jurisdiction over the non-resident defendant, the court has to comply with the provisions laid down in Fifth and Fourteen Amendments Due process Clause.

In England, the offences of unauthorized access or modification of computer material under Sections 1 and 3 of the Computer Misuse Act, 1990 may be prosecuted in the 'home country',[42] even if no element of the offence occurred in that country and or the defendant was not present in that country, so long as there is at least one 'significant link' with the jurisdiction.[43] In essence, a 'significant link' arises where either the defendant was in the home country when he or she did the relevant act, or the unauthorized access or modification occurred in the home country.[44]British citizenship is immaterial to the question of guilt.[45]

Generally, in the last 40 years, however, revolutions have occurred in international travel, trade, finance, and telecommunications, principal among which is the role of internet in facilitating them. These, together with the changing patterns of criminal conduct associated with them, have spawned numerous exceptions to the basic principle of territoriality, many of which have been required in order to comply with the United Kingdom's treaty obligations under international law.[46]

In Nigeria, it is the statute creating a Court that vests it with its jurisdiction.[47]Lower Courts of Law in Nigeria are created by the various States in Nigeria for the purpose of Administration of Justice.[48]

The writer observes that these courts, whether superior courts or inferior courts of law have the jurisdiction to entertain cases involving crime.

[42] This is basically due to judicial activism of the law courts.
[43] Defined as England and Wales, in so far as the Act applies to England and Wales, and similarly for Scotland and Northern Ireland: Computer Misuse Act, s. 4(6).
[44]Ibid., s. 4(1)–(2).
[45]Ibid., s. 5. The provision for extraterritorial jurisdiction in respect of a s. 2 offence is found in ss. 4(3) and 8(1). For a more detailed discussion of these provisions.
[46] Section 9(1) Computer Misuse Act of the United Kingdom, 1990.
[47] See Section 230-269 of the 1999 Constitution of Nigeria (as amended).
[48] For instance, the Kaduna State Laws, 1991 creates the District and Magistrate Courts.

Even though issues of cyber jurisdiction rarely arise in Nigeria courts,[49]in considering whether they have jurisdiction over a matter, Nigeria Courts of law may likely consider the following ingredients of jurisdiction:

> (a) it is properly constituted as regard number and qualifications of the members of the bench, and no member is disqualified for one reason or the other; and
> (b) The subject matter of the case is within its jurisdiction; and there is no feature in the case which prevents the court from exercising its jurisdiction; and
> (c) The case comes before the court of law initiated by due process of law and upon fulfillment of any condition precedent to the exercise of jurisdiction….

In issues involving conflicts of laws and jurisdiction generally, the courts in Nigeria consider whether they have jurisdiction on the basis ofthe subject[50]matter i.e. *in rem*[51]or in *personam*.[52]

For civil and criminal matters, Nigerian courts have jurisdiction overforeign companies. A foreign company can sue and be sued in its corporate or registered name in Nigeria even though it is not locally registered and without the requirement of its suing through an agent.[53]

The writer observes that in considering whether they have jurisdiction over criminal cases, courts in Nigeria would consider their inherent[54] and the territorial[55]jurisdiction. In Nigeria today, Jurisdiction to try cybercrimes is vested in the Federal High Courts.[56]

The writer observes that as complex offences are tried in Nigerian Courts and various issues involving cyber jurisdiction arise, Judges and legal practitioners in Nigeria

[49] This is because there are no cybercrime specific laws in Nigeria.
[50] See *Elelu-Habeeb vs. A.G. Fed*., (ibid) p. 441 paragraphs F-B.
[51] Ibid, pp. 423-442.
[52] i.e. an action brought to assert a right over a property.
[53] i.e. an action brought against an individual.
[54]*O.U. Ins. Ltd. vs. Marine & Gen. Ass. Co.* (2001) 9NWLR (Pt. 717) 92 at p. 95 paragraphs B-C.
[55] See *Elelu-Habeeb vs. A.G., Fed*., (ibid)p. 441 paragraphs F-B.
[56] Section 22 of the Cybercrime Act, 2015.

would through judicial activism, be opportune to make *locus classicus* cases on cyber jurisdiction in Nigeria, just as American and English Courts are doing.

In the Budapest Convention, Prescriptive jurisdiction is addressed in Article 22. This sets out a number of basis on which parties are to establish jurisdiction.[57]The first is where the offence is committed within its territory, reflecting the principle of territoriality.[58] This is the most common basis for the exercise of criminal jurisdiction,[59] there being a general presumption that criminal laws are local in operation.[60] Although allowing a country to exercise jurisdiction over conduct which occurs within its sovereign territory, there are a number of ways in which the territorial principle operates to encompass extraterritorial conduct.[61]First, a country may assert territorial jurisdiction over conduct which occurs on a flagged ship or registered aircraft of that country. This is specifically recognized in the Convention, and expands the scope of territorial jurisdiction to those situations where the ship or aircraft is outside the terrestrial jurisdiction of the relevant country.[62] Such an extension of territorial jurisdiction is important in closing potential gaps in jurisdictional reach. For example, if the ship or aircraft is in international waters or airspace, no other country may be able to assert jurisdiction in respect of that conduct.[63]Alternatively, even where a ship or aircraft is within the territorial jurisdiction

[57] McConnell International (ibid), page 3 states that Nigeria is yet to criminalize cybercrimes. This is no longer the position by virtue of the cybercrime Act, 2015. See www.mcconnellinternational.com December 2000. Even though the report was published in the year 2000, the position stated therein still remains the same.

[58] These do not exclude other forms of jurisdiction exercised by a country under its domestic law: Cybercrime Convention, Art. 22(4).

[59]*Ibid*., Art. 22(1)(a) and Cybercrime Convention, Explanatory Report, [233].

[60] Council of Europe: European Committee on Crime Problems, 'Extraterritorial criminal jurisdiction' (1992) 3 *Criminal Law Forum* 441, 446; Restatement (Third) of Foreign Relations Law of the United States § 402, comment c; and D. Lanham, *Cross-BorderCriminal Law* (Sydney: FT Law & Tax, 1997), p. 30.

[61]*Treacy* vs. *DPP* [1971] AC 537 at 561 per Lord Diplock; *Equal Employment Opportunity Commission* v. *Arabian American Oil Co*., 499 US 244 (1991); and *R* vs. *Finta* [1994] 1 SCR701 at 805–6 per Cory J.

[62] Council of Europe, 'Extraterritorial criminal jurisdiction', 447; 462.

[63]Ibid.

of another country, its presence may be so transient as to the make the assertion of jurisdiction impractical.[64]

2.5.5 Adjudicative Jurisdiction

Once prescriptive jurisdiction has been established, the question remains whether the particular court has adjudicative jurisdiction over the specific case. In considering its adjudicative jurisdiction, courts use the following yardsticks:

(a) The general jurisdiction of the court
(b) The specific jurisdiction of the court

In the United States, general jurisdiction of a court equates to 'continuous and systematic contacts' with individuals or subject matter within the jurisdiction of the court by the plaintiff, whether or not the contacts are related to the suit. For example, in the United States, if a Plaintiff in the course of carrying out a transaction went to 5 different states in the bid to execute the transaction, the courts in any of these states would have jurisdiction to entertain an action filed by the Plaintiff with respect to the contract. It would allow the forum to assert jurisdiction for any cause of action pertaining to the contract.

On the other hand, specific jurisdiction arises from contact with the court related to the suit. It would permit the court to assert jurisdiction only to adjudicating a dispute which took place within the court's jurisdiction.

In absence of clear rules and regulations, the courts in the United States have devised new jurisprudence in order to resolve rivalry grievances of the parties in cyber jungle. Prior to the mid-nineties, there were very few decisions by U.S. Courts on competence over the Internet disputes. Since 1995, there has been a true explosion of cyberspace litigation and the United States blazes the trail on issues of internet law.

[64]Ibid.

American courts have used various tests to determine whether they have jurisdiction over Internet disputes arising within their jurisdiction or affecting their citizens. Some courts have simply applied traditional rules while others have tried to devise new tests to accommodate the peculiarities of the medium.

The principles considered by courts in the United States, England and Nigeria when considering issues of extraterritorial jurisdiction are discussed below.

(a) The territorial principle (Pennoyer Theory)[65]

The traditional law of personal jurisdiction in the United State is reflected in the landmark decision of the US Supreme Court. In the Year 1877, Pennoyer laid down the fundamental principles that "every state possesses exclusive jurisdiction and Sovereignty over persons and the property within its territory and no state can exercise direct jurisdiction and authority over person and property within its boarder. Due to these laws one state could not infringe the laws of another state because that other state is also a sovereign power". However during 18th and early 19th. Centuries, the federalist model of jurisdiction upon which Pennoyer theory was founded no longer reflected political and commercial reality. After the Second World War, there was an exponential growth of industrialization, urbanization, modernization and 'computerization in all walks of life. The expansion of the United States, international Commerce after the world wars and the increasing ease of travel across the state lines created problems when a state could not assert jurisdiction over entities that established connections with the state. The interstate movement of goods and persons compelled the states to provide a way for their citizens to sue non-residents in local court.

Unfortunately, Pennoyer test could not stand the test of time, as it has the effect of prohibiting the states from exercising personal jurisdiction over persons and things

[65] This is specifically envisaged in the Convention and is intended to apply where the victim is within the jurisdiction. See Cybercrime Convention, Explanatory Report, [233].

physically located outside of its territorial limits. Due to this, and to keep a pace with the changing needs of the society, the state started to enact long arm statutes, which permitted the local courts to exercise personal jurisdiction over non residents-defendants. Provided the exercise of jurisdiction did not violate the 14th Amendment of the US Constitution.

(b) Minimum contact Principle

States in the United States wanted to give its citizens an option to sue non-residents in local courts. The impact if these changes could be seen in a landmark judgment in which the United States Supreme Court upheld a Massachusetts Statute[66] deeming that non-residents using the roads of Massachusetts consented to be sued in that state. After analyzing the perspective of natural person, the court held that a state may sue a non-resident foreign corporation provided the corporation has "minimum contact" with the forum state and provided that exercise of jurisdiction does not violate the "principle of fair play and justice". This principle permits the exercise of jurisdiction in the light of "virtual" presence of the defendant within a state. Furthermore, the minimum contact principle developed by the United States Supreme Court in *International Shoe Co. vs. Washington, Office of Unemployment Compensation and Placement et al.*[67]accordingly it analyzed the distinction between specific and general jurisdiction. Historically, personal jurisdiction could satisfy due process if the foreign defendant was present within jurisdiction or consented to the jurisdiction of a court to hear a matter. However, the U.S. Supreme Court by this case cleared the mist that was gathered around 'jurisdiction in *rem* and jurisdiction in *personam* by making it clear that there must be certain relationship between non-residents property and law suit. On the other hand, in the case of *World-*

[66] In the case of *United States vs. Roberts,* 1 F. Supp 2d 601 (E.D. La. 1998 a crime was committed on international waters against a minor, who was a U.S. Citizen by a Citizen of the Caribbean Islands, aboard a ship registered in Liberia and belonging to a company registered in Panama. The defendant was indicted by a Federal grand jury in Louisiana after his motion to dismiss the action for lack of jurisdiction was refused.
[67] 41. 444. U.S. 286 (1980).

Wide Volkswagen Corp. vs. Woodson[68]a New York Volkswagen dealer sold a car to New York Residents. The New York couple relocated to Oklahoma where they met with an automobile accident that injured the wife and child. The purchaser filed a suit in Oklahoma under its long-arm statute claiming "defective automobile design." The Supreme Court held that the defendant corporation did not have minimum contacts with state of Oklahoma because they limited their sales, advertisements and business within New York only. The sole fact that the product sold was readily movable in commerce did not subject the defendants to jurisdiction of courts outside the area of where they conducted business. The court held that forseeability has never been a sufficient benchmark for personal jurisdiction under Due Process Clause.[69]

(c) Effects Principle[70]

When a defendant targets a particular forum, he may be called to answer his or her actions in that forum. The court asserted its jurisdiction on the principle that when the defendant knew that her action would be injurious to the plaintiff, and then she must reasonably anticipate being sued into the court where the injury occurred. The "Effects Principle" is of particular importance in cyber space because conduct in cyber space often has effects in various jurisdictions.[71]

(d) Purposeful Availment principle

The concept of this theory is that a person by conducting activities within a state enjoys certain benefits and privileges of that state and with these privileges certain obligations also arise which bears nexus with the activities within the state which require the person to answer litigations in the state. Also, the theory states that for a court to have

[68] 42. 326 U.S. 310 (1945).

[69] Under the Oklahoma State of the U.S, due process requirements are satisfied when personal jurisdiction is asserted over a non resident corporate defendant that has "certain minimum contacts. " See the case of *Burger King Corp. vs. Rudzewicz,* 471 U.S. 462, 474.

[70]

[71] See the case of *Dow Jones & Co. Inc. vs. Gutnick,* (2002) HCA 56, where the High Court of Australia held that the Wall Street Journal who defamed Gutnick as subject to jurisdiction in Gutnick's country of Australia, as the journal availed themselves to Australian law by defaming a resident there.

jurisdiction over any cause of action and the defendant, the legal action must have arisen from defendant's activities there. Furthermore, the acts of the defendant or consequences of his actions must have a sufficiently substantial connection to the state.[72]

(e) The nationality principle[73]

The other basis of jurisdiction recognized under the Convention is the 'Nationality Principle'. This requires parties to establish jurisdiction where the offence is committed by one of its nationals, irrespective of where it occurs in the world.[74] For this principle to apply, the conduct must have also been punishable under the laws of the country where the offence was committed, or where the offence was committed outside the territorial jurisdiction of any state.[75] Although parties may opt out of asserting jurisdiction on the basis of nationality or in respect of its ships or aircraft, they must apply territorial jurisdiction of the relevant country.[76]

(f) The Universality Principle (principle of universal jurisdiction)

This principle is closely aligned with the international law doctrine of peremptory norms (*jus cogens*). The principle holds that all states have jurisdiction over crimes that are universally recognized to be a crime against humanity. These have historically included piracy, slave trading, torture, genocide, and perhaps, terrorism. It is the writer's belief that soon, cybercrimes would also be tried under this principle, considering its effects on nations today.

---

[72] See the case of *CompuServe, Inc. vs. Patterson* 89 F.3d 1257. In this case, the defendant who lived in Texas entered into a contract with the Claimant through the Internet. The Plaintiff later filed an action against him and he brought an application to dismiss the case for lack of jurisdiction, that he had never in his life visited Ohio, where the Claimant was based. Based on the purposeful availment theory, the court held that it had jurisdiction to entertain the matter even though the transaction was through the internet.

[73] The principle of universal jurisdiction, which recognizes the right of any country to exercise jurisdiction over a defendant in respect of 'universal crimes' such as piracy, genocide, and war crimes, is of limited significance in the cybercrime context.

[74] *CompuServe, Inc. vs. Patterson,* ibid.

[75] *CompuServe, Inc. vs. Patterson,* ibid.

[76] Cybercrime Convention, Art. 22(1)(b)–(c) and Cybercrime Convention, Explanatory Report, [235].

The writer observes that from the above principles of jurisdiction, the judiciaries are striving to handle challenges of cyber jurisdiction when they arise. The judiciaries over the years have shown a propensity to readily make laws or solve legal issues by judicial activism and sound reasoning. This is probably the reason why cases involving the internet and cyber jurisdiction are properly dealt with when they are instituted in Americanor English Courts of law.

For cyber-crimes which of course are criminal offences, it is the writer's opinion that American or English courts would likely consider its inherent and prescriptive jurisdiction in hearing and determining them.

2.5.6 Enforcement Jurisdiction

Even if there is both prescriptive and adjudicative jurisdiction, the ability to enforce presents the most significant limitation on criminal jurisdiction. Unlike civil actions, where principles of *forum non conveniens* may apply, in criminal law the issue is effectively reduced to the question of who has the defendant in custody? This has the practical effect of limiting the number of cases in which states assert jurisdiction.[77] It is a general principle that individuals will not be tried *in absentia* for serious offences. This is based in part on fairness to defendants but also the pragmatic fact that a foreign state will not enforce another state's public law judgments.[78] Criminal courts also invariably apply local law.[79] The effect of this is that 'on those fairly rare occasions when in possession of enforcement power, [states] have not been too concerned about the limits of their legislative/adjudicative jurisdiction under public international law'.[80] Hence, it is the jurisdiction which has the defendant in custody which has the practical ability to exercise

[77] Kohl, U. (2007)" *Jurisdiction and the Internet"*, www.worldcat.org accessed on 25/12/ 2013, p. 105.
[78]Ibid., p. 105.
[79] Most cases are resolved in accordance with the laws of nations.
[80] Cybercrime Convention, Explanatory Report p. 1

jurisdiction. In this respect, the Convention recognises the principle of *aut dedere aut judicare*: the obligation to extradite or prosecute.[81] That is, a country must assert jurisdiction where one of its nationals has committed an offence within its jurisdiction, and a request for extradition has been refused solely on the basis of nationality.[82]

Extradition is the process whereby one state will formally surrender a person for prosecution in another state. This is a matter of international comity rather than an obligation under international law, and is typically supported by bilateral treaties and domestic legislation in each country.[83]Extradition typically requires there to be 'dual criminality' between the requesting party and the country where the person is located. That is, the offence must be an offence under the laws of both jurisdictions, usually subject to a minimum level of penalty, commonly a maximum penalty of at least twelve months' imprisonment.[84] The difficulties presented by this requirement are well illustrated by the case of the 'love bug' virus.[85]Where dual criminality exists, however, it allows one jurisdiction to seek the surrender of a person alleged to have caused damage in the requesting jurisdiction. In a recent example, English-man Gary McKinnon lost his appeal against extradition to the United States in respect of his unauthorized access to United States federal computers.[86] When the number of extraditable offences were relatively few, it was typical for extradition treaties to enumerate those offences which were extraditable. This tradition continued, even as the number of extraditable offences

[81] Ibid, p.1.
[82] Cybercrime Convention, Art. 24.
[83] Extradition Act 1988 (Cth); Extradition Act 1999 (Can); Extradition Act 2003 (UK); and 18 USC ch. 209. Some Jurisdictions also make provision in relation to the transfer of criminal proceedings in order to resolve such disputes: United Nations General Assembly, Model Treaty on the Transfer of Proceedings in Criminal Matters, A/RES/45/118,14 December 1990.
[84] Cybercrime Convention, Art. 24.
[85] Cybercrime Convention, Art. 24. See Goodman M.D. et al. "*The Emerging Consensus on Criminal Conduct in Cyberspace*" UCLA Journal of Law and Technology (ibid), p.16.
[86]*McKinnon* vs. *Government of the USA; Secretary of State for the Home Department* [2007] EWHC 762.It is alleged that between 2001 and 2002 he accessed ninety-seven federal computers including the Department of Defense, the US Army and Navy and NASA, causing an estimated $US700, 000 worth of damage.

grew, so that the 1976 Treaty between Australia and the United States specified twenty-nine types of extraditable offence. This approach presents particular difficulties where novel offences arise, with very few applicable to computer-facilitated crimes, and none encompassing conduct where a computer was the target of the offence.[87] Because of such difficulties, treaties have moved away from an enumerative to an eliminative approach.[88] For example, the Australia–U.S. treaty was subsequently amended so that an extraditable offence was defined as an offence 'punishable under the laws in both Contracting Parties by deprivation of liberty of more than one year, or by a more severe penalty'.[89]Although preferable, such an approach requires whether or not the contracting parties place the offence within the same category of still requires consideration of whether an equivalent law can be found in each jurisdiction, just two instances of conduct that is commonly unlawful in one jurisdiction but not others. In addition, even if technically extraditable, the complexity and cost of the and can still present an obstacle.[90] For example, online gambling and hate speech are extradition process ensures that it is typically reserved for serious offences.[91]

2.6 Cybercrimes committed in Nigeria and Criminalized under the Budapest Convention

Fighting cybercrime, like any other crime requires three important elements namely: identification, classification and the actual deployment of effective counter-measures. The classification of cybercrimes, which is an important step to fighting it, has been grossly limited to whether these crimes are "computer-crimes" or "computer-

[87] Soma, J.T et al (1997)"*Transnational extradition for computer crimes: Are new treaties and laws needed?"* 34 *Harvard Journal on Legislation* 317,324–6.
[88] Treaty on Extradition between Australia and the United States of America, opened for signature 14May 1974, Australian Treaty Series 1976 no. 10, Art. II(1) (entered into force8 May 1976).
[89] Protocol Amending the Treaty on Extradition between Australia and the United States of America of 14 May 1974, Australian Treaty Series 1992 no. 43, Art. 1(1) (entered into force 21 December 1992).
[90] See, e.g., *R* vs. *Bow Street Magistrates Court and Allison, ex parte Government of the United States of America* [2000] 2 AC 216.
[91] Paust, J. (2007) *"Panel: Cybercrimes and the domestication of international criminal law",*5 *Santa Clara Journal of International Law pp.* 432, 442.

assisted crimes."[92] To further identify acts carried out by criminal-minded individuals today in Nigeria, the writer would attempt to make them easier to identify by linking them to traditional crimes committed today in Nigeria. Under the Cybercrime Act, 2015cybercrimes are categorized as follows:

i. Acts carried out by criminal-minded individuals against computers.

ii. Acts carried out by criminal-minded individuals against people.

iii. Acts carried out by criminal-minded individuals against the State.

2.6.1 Acts carried out by Criminal Minded Individuals Against Computers[93]

Acts carried out against computers with criminal intent in Nigeria constitute cybercrimes. The cybercrime Act, 2015 in Section 2 states that unlawful access to a computer constitutes a cybercrime. See particularly, Section 2(3).

Section 3 makes it unlawful to intercept communications by technical means, transmissions of non-public computer data, content data or traffic data, including electromagnetic emissions or signals from a computer, computer system or network carrying or emitting such, to or from a computer, computer system or connected system or network an offence. This provision covers mobile phones as the definition of a computer in the cybercrime Act, 2015 include mobile phones.[94]

Section 4 of the Act prohibits unauthorized modification of computer program or data and sections 5 and 6 prohibit System interference and Misuse of devices respectively.

2.6.2 Acts carried out by Criminal Minded Individuals against Individuals

Acts carried out by criminal-minded individuals against people are done with the intention to cause harm to them. These acts are as follows:

[92] See Chick W. B. (ibid) and Longe, O. et al, (ibid).
[93] See Sections 2, 3, 4, 5 and 6 of the Act.
[94] See Section 37 of the Act.

A. Computer-related Fraud[95]

Computer-related fraud is one of the most popular crimes on the Internet in Nigeria[96]as it enables the offender to use automation and software tools to mask criminals' identities. This act is referred to as a crime because in most cases, the computer is only a medium to establish a link with gullible victims whom they may later meet physically or convince to deposit huge sums of money in their accounts.

Automation enables offenders to make large profits from a number of small acts.[97]

One strategy used by offenders is to ensure that each victim's financial loss is below a certain limit. With a 'small' loss, victims are less likely to invest time and energy in reporting and investigating such crimes.[98]The main distinction between computer-related and traditional fraud is the target of the fraud. If offenders try to influence a person, the offence is generally recognized as fraud. The writer observes that where offenders target computer or data-processing systems, offences are often categorized as computer-related fraud. Those criminal law systems that cover fraud, but do not yet include the manipulation of computer systems for fraudulent purposes, can often still prosecute the computer related fraud.[99]

B. Online Auction Fraud

Online auctions are now one of the most popular e-commerce services. In 2006, goods worth more than USD 20 billion were sold on eBay, the world's largest online auction marketplace.[100]In Nigeria, many indigenous online auctions websites are existing

[95]Section 8 of the cybercrime Act, 2015.
[96]Computer related fraud is popularly referred to as "yahoo yahoo" in Nigeria. See Azeez N. A. et al (2009) *"Towards Ameliorating Cybercrime And Cybersecurity"* in (IJCSIS) International Journal of Computer Science and Information Security, Vol. 3, No. 1, pp.1-11.
[97]International Telecommunication Union Cybercrime Legislation Resources (2009) *"Understanding cybercrime: A guide for developing countries"*Draft, April, www.itu.int/ITU.D/cyb/**,** p. 45.accessed on 19/3/13 by 9:00pm.
[98]Ibid, p.45.
[99]Under section 419 of the Nigerian Criminal Code.
[100] See http://www.ebay.com**.**

today[101]Nigerians can access varied or specialist niche goods from around the world. Sellers enjoy a worldwide audience, stimulating demand and boosting prices. Offenders committing crimes over auction platforms can exploit the absence of face-to-face contact between sellers and buyers.[102]The difficulty of distinguishing between genuine users and offenders has resulted in auction fraud being among the most popular of cybercrimes.[103]

The two most common scams include:[104]

i. Offering non-existent goods for sale and requesting buyers to pay prior to Delivery.[105]

ii. Buying goods and asking for delivery, without intention to pay.

In response, auction providers have developed protection systems such as the feedback/comments system. After each transaction, buyer and sellers leave feedback for use by other users[106]as neutral information about the reliability of sellers/buyers. In this case, reputation is everything and without an adequate number of positive comments, it is harder for offenders to persuade targets to either pay for non-existent goods or, conversely, to send out goods without receiving payment first. However, criminals have responded and circumvented this protection through using accounts from third parties.[107]

C. Computer Related Forgery[108]

[101] See konga.com, cheki.com nairaland.com, jumia.com.ng, inspiredmotors.com, etc.
[102]This however poses some challenges as computer fraud is a hybrid fraud. Most times, some laws are archaic when it comes to computer related offences.
[103] See Goodman et al. Ibid
[104] The United States Internet Crime Complaint Centre (IC3) (a partnership between the FBI and the National White Collar Crime Centre) reported that around 45% of complaints refer to Auction Fraud. See: "IC3 Internet Crime Report 2006", available at: http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf accessed on 13/12/13by 8:pm.
[105] "Law Enforcement Efforts to combat Internet Auction Fraud", Federal Trade Commission, 2000, page 1, available at**:** http://www.ftc.gov/bcp/reports/int-auction.pdf.accessed on 13/12/13 by 8:45pm.
[106] For more information, see for example: http://pages.ebay.com/help/feedback/feedback.html**.**
[107] In this scam called "account takeover", offenders try to get hold of user names and passwords of legitimate users to buy or sell goods fraudulently, making identification of offenders more difficult. For example, many Facebook users in Nigeria have discovered that their accounts are been hijacked or fraudsters are cloning their accounts and sending friend requests to their friends on Facebook. These fraudsters often use these account to carry out transactions on the internet.
[108]Section 8 of the cybercrime Act, 2015.

Computer-related forgery describes the manipulation of digital documents by cyber-criminals in Nigeria- for example, by:

i. Creating a document that appears to originate from a reliable institution;

ii. Manipulating electronic images (photo shopping, for example, pictures used as evidence in court,); or

iii. Altering text documents.

The falsification of e-mails includes the scam of "phishing" which is a serious challenge for law enforcement agencies worldwide.[109] "Phishing" seeks to make targets disclose personal/secret information by e-mail or text messages. The e-mails or text messages are designed in a way that it is difficult for targets to identify them as fake e-mails. The e-mail asks a recipient to disclose and/or verify certain sensitive information. Many victims follow the advice and disclose information enabling offenders to make online transfers or hack their ATM's, etc. In Nigeria prosecutions involving computer-related forgery are rare, because most legal documents are tangible documents. Digital documents play an ever more important role and are used more often. The substitution of classic documents by digital documents is supported by legal means for their use e.g., by legislation recognizing digital signatures. Criminals have always tried to manipulate documents. With digital forgeries, digital documents can now be copied without loss of quality and are easily manipulated. Even though Section 84 of the Nigerian Evidence Act, 2011 provides for admissibility of electronically generated evidence, Judges have to be very careful when admitting electronically generated evidence as it is subject to manipulation. For forensic experts in Nigeria, it is difficult to prove digital manipulations, unless technical protection is used to protect a document from being a falsified.[110]

[109]International Telecommunication Union Cybercrime Legislation Resources. 'Understanding cybercrime: A guide for developing countries' (ibid), p. 46.
[110] One technical solution to ensure the integrity of data is the use of digital signatures.

D. Identity Theft[111]

The term identity theft – that is neither consistently defined nor consistently used describes the criminal act of fraudulently obtaining and using another person's identity.[112] The National Identity Management Commission Act, 2007[113]and the Cybercrime Act, 2015[114] rather state actions that constitute identity theft, rather than define what it means. These acts can be carried out without technical means[115]as well as online by using Internet technology.[116]

In general the offence described as identity theft contains three different phases:[117]

i. In the first phase the offender obtains identity-related information. This part of the offence can for example be carried out by using malicious software or phishing attacks

ii. The second phase is characterized by interaction with identity-related information prior to the use of the information for criminal offences. An example is the sale of identity-related information.

iii. The third phase is the use of the identity-related information in relation with a criminal offence. In most cases the access to identity-related data enables the perpetrator to commit further crimes. The perpetrators are therefore not focusing on the set of data itself but the ability to use them in criminal

[111]Ladan, M.T. (2015) "Cyberlaw and Policy on Information and Communications Technology in Nigeria and ECOWAS" ABU Press Ltd. , Zaria. p. 68.
[112]Azeez N. A. et al (2009)"Towards Ameliorating Cybercrime And Cybersecurity" in (IJCSIS) International Journal of Computer Science and Information Security, Vol. 3, No. 1, pp.1-11.
[113]See Section 37 of the National Identity Management Commission Act, 2007.
[114]See Section 13 of the Cybercrime Act, 2015.
[115]For example, when individuals dump documents containing confidential information in dust bins.
[116]Peeters, (2007) "*Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection,Multimedia"* und Recht, page 415; ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 39, available at:http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html; Regarding the different definitions of Identity Theft See: Gercke, Internet-related Identity Theft, 2007, available at:http://www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-didentity%20theft%20paper%2022%20nov%2007.pdf.
[117]International Telecommunication Union Cybercrime Legislation Resources (2009) *"Understanding cybercrime: A guide for developing countries"* (ibid), p. 48.

activities. Examples for such offence can be the falsification of identification documents or credit card fraud. The methods used to obtain data in phase one cover a wide range of acts. The offender can use physical methods and for example steal computer storage devices with identity-related data, searching trash or mail theft. In addition they can use search engines[118]to find information on individuals.

File sharing by individuals from their computer or computer networks also makes it easy for cybercriminals to get valuable information on individuals.

Finally the perpetrators can use social engineering techniques to persuade the victim to disclose personal information. In recent years perpetrators developed effective scams to obtain secret information (e.g. bank account information and credit card data).By manipulating users through social engineering techniques. The type of data cybercriminals target varies. The most targeted data however are:

i. Date of birth, address and phone numbers.

ii. Drivers' license or Passport Number.

iii. Password for non-financial accounts.

iv. Password for financial accounts.

E. Gambling, Pornography and Other Offenses against Morality

Online casinos have proliferated widely[119]enabling individuals all over the world to gamble from the comfort of their homes despite the fact that gaming is illegal in most countries like Nigeria.[120]The Internet is used to showcase pedophilic and gay[121]activities

[118]Search engines like google are used by cybercriminals to gather information on Nigerians. "Googlehacking" or "Googledorks" are terms that describe the use of complex search engine queries to filter through large amounts of search results for information related to computer security issues as well as person.

[119] According to one estimate, there are "approximately 200+ casinos, sports books, and full service venues operating on the internet." A Personal Message, ONLINE CASINO GAMBLING, at http://www.adult-fun.net**.** Accessed on 29/1/14 by 8:00pm.

[120]Gaming Machines (Prohibition) Act CAP G1 L.F.N. 2004.

in Nigeria - viewing images, discussing activities, arranging tourism, enticing a child to a meeting - are carried out over the Internet. As one report explained: Child sexual abusers are rapidly turning the Internet and commercial online services into red-light districts, where they can distribute vast quantities of pornography often depicting bondage and other forms of violence, including murder and organize with like-minded individuals. The Internet gives child molesters and pornographers unprecedented opportunities to target and recruit new victims. It allows sexual predators to stalk juvenile victims anonymously from the comfort of their homes.[122]

The Internet gives the pedophile the advantages of a wider scope of communications and the likelihood of eluding the law, given the jurisdictional problems which arise in prosecuting cases that transcend borders, as is the nature of the Internet.[123]

F. Stalking and Criminal Defamation

With the advent of social networking sites like Facebook and Twitter, Cybercriminals perpetuate crimes like stalking and defamation against individuals. In some cases stalking leads to kidnapping which is prohibited under section 366 of the Criminal Code Act of Nigeria.[124]

With internet stalking can be easily carried out in Nigeria with no punishment against the cybercriminal.

G. Other Acts or Omissions against Persons not criminalized under any law

Cyber homicide[125]using computer technology to kill someone is neither considered under the cybercrime Act, 2015 nor in the Budapest Convention. Also, it has

[121]The Nigerian National Assembly in 2013 passed a bill prohibiting same sex marriage and gay activities in Nigeria. However it is noted that perpetrators of these acts can still carry them out with the aid of the internet as they may not be caught.
[122] See Goodman M.D. et al. (2002) "*The Emerging Consensus on Criminal Conduct in Cyberspace"* UCLA Journal of Law and Technology (ibid), p.16.
[123]Ibid, p. 1
[124] Criminal Code Act, Cap. C38 Laws of the Federation of Nigeria, 2004.
[125]Op cit, p. 17.

not been reported anywhere in the world but the writer believes it will some day. An example of this cybercrime is as follows – an aspiring mass murderer could hack into a hospital's computer system, learn about the medication prescribed for patients and alter the dosages, causing them to die.

2.6.3 Cybercrimes Committed against the State

A. Cyber terrorism

Terrorism is a growing menace all over the world today and Nigeria is also affected by terrorist activities.[126] Though terrorists do not use the internet to carry out terror activities, the internet plays a role in aiding terrorists' activities.[127]Today it is known that terrorists use ICTs and the Internet for:[128]

i. Propaganda;

ii. Information gathering;

iii. Preparation of real-world attacks;

iv. Publication of training material;

v. Communication;

vi. Terrorist financing;

vii. Attacks against critical infrastructures.

This shift in the activities of terrorists via Internet had a positive effect on research related to cyber terrorism as it highlighted areas of terrorist activities that were rather unknown before. Due to the digitalization of government organizations in Nigeria,

[126]International Telecommunication Union Cybercrime Legislation Resources (2009) *"Understanding cybercrime: A guide for developing countries"* (ibid), p. 48.
[127] See Section 1 of the Terrorism Act, No. 10, 2011 (as amended) and Sections 1 & 2 of the Terrorism Act (Prohibition Order Notice), May, 2013.
[128] Op cit, pp. 51-52.

terrorists can launch attacks against government websites crippling governance for several hours.[129]

B. Cyber-Warfare[130]

Cyber-warfare describes the use of ICT in conducting warfare using the Internet. It shares a number of features in common with cyberterrorism.[131]Discussions originally focused on the substitution of classic warfare by computer-mediated or computer-based attacks.[132]Network-based attacks are generally cheaper than traditional military operations and can be carried out even by small states. Protection against cyber attack is difficult. Until now, there have been limited reports on the substitution of armed conflicts by Internet-based attacks.[133]Current discussions focus on attacks against critical infrastructure and control of information during a conflict. In considering both civil and military communications, information infrastructure is a key target in armed conflicts. However, it is uncertain if these attacks will be carried out via the Internet. Attacks against computer systems in Estonia[134]and the United States has been linked with cyber-warfare. Since attacks cannot be traced back to official state organizations with any certainty, it is difficult to categorize them as cyber-warfare. In Nigeria, no known attack has been carried out against Nigeria cyberspace by another nation. Attacks against infrastructure that are carried out physically – e.g. by arms and explosives – are also difficult to categorize as cyber war fare. Nevertheless, in a bid to secure Nigeria's

[129] During the January 2012 fuel subsidy protests a group of cybercriminals referring to themselves as "hacktivists" hacked into several government websites in show of solidarity with the protesters. See *"EFCC & NCC websites hacked"* atwww.dailytimes.com.ng/article/efcc-ncc-websites-hacked accessed on 20/12/14 by 8:00pm.

[130]Marc D.G. et al (2002) *"The Emerging Consensus On Criminal Conduct In Cyberspace"* ibid, p. 18.and International Telecommunication Union Cybercrime Legislation Resources (2009) *"Understanding cybercrime: A guide for developing countries"* ibid, p. 52.

[131]This is because the aim is to destroy property and terrorize. See above Unit 2.5.2 A.

[132]Op cit, p. 57.

[133]Ibid, p. 57.

[134]Ibid, p. 57.

Cyberspace, the Nigerian government in April 2013 awarded a $40 million contract for monitoring Nigerian's internet communication for national security reasons.[135]

C. Cyber-laundering

Cyber laundering is a new phenomenon in Nigeria.[136]The Internet is transforming money laundering in Nigeria. With larger amounts, traditional money-laundering techniques still offer a number of advantages, but the Internet offers several advantages. Online financial services provided by banks in Nigeria offer the option of enacting multiple, worldwide financial transactions very quickly. The Internet has helped overcome the dependence on physical monetary transactions. Wire transfers replaced the transport of hard cash as the original first step in suppressing physical dependence on money, but stricter regulations to detect suspicious wire transfers have forced offenders to develop new techniques. The detection of suspicious transactions in the fight against money-laundering is based on obligations of the financial institutions involved in the transfer.[137]

The writer observes that cybercriminals are always perfecting ways of carrying out cybercrimes and with sophistication in technology;[138] they seem to be limitless in their endeavour. On the other hand, law enforcement agencies in Nigeria and the world over daily grapple to comprehend cybercrimes committed and how the cybercriminal operates.

This chapter has discussed key terms associated with cyber-crimes under the Nigeria legal system. The chapter also discussed the issue of cyber jurisdiction in the

[135]See http://ireporterstv.co/president-goodluck-jonathan-awards-40-million-contract-t0-israeli-company-for-internet-communication-monitoring -in-nigeria/ accessed on 21/1/2014 by 7:00pm
[136]This is mainly because it is the traditional crime of Money Laundering that is common in Nigeria.
[137]By section 2 Of the Anti-money laundering Act, 2011, Banks in Nigeria are required to report suspicious financial transactions to the EFCC. Cyber-laundering makes this law difficult to enforce.
[138]With Internet Banking, Nigerians can log into their accounts on-line and carry out banking transactions without physically visiting the bank. A Cybercriminal can hack a customer's on line account if he has the motivation.

United States and Nigeria, with some case law and statutes. The chapter also discussed types of cybercrimes committed in Nigeria and how they are similar with their traditional counterparts. Before cybercrimes were prohibited in Nigeria, Nigerian law enforcement agencies prosecute offences committed in Nigeria through the computer and the internet under existing criminal laws in Nigeria.[139]

The writer observes that cybercrimes increase every day as cybercriminals are always coming up with new methods of committing these crimes. Consequently, only when proper classification of the fraudulent acts or omissions carried out by criminal minded individuals in Nigeria are made that the Nigerian judiciary and law enforcement will tackle them head on.

The writer observes that the international community battles with the challenge of jurisdiction in issues of cybercrime. Recommendations to this issue are proffered in Chapter 5 of this research.

[139] For example, even though there is no cybercrime specific law in Nigeria yet, identity theft and impersonation is prosecuted by the EFCC under section 419 of the Criminal code of Nigeria (ibid).

CHAPTER THREE

LEGAL AND INSTITUTIONAL FRAMEWORKS RELEVANT FOR INTERNATIONAL COOPERATION AGAINST CYBERCRIME IN NIGERIA

3.1 Introduction

The aim of this chapter is to analyze the current legal and institutional regime on acts or omissions that constitute cybercrime in Nigeria with a view to also identify provisions relevant to fighting these acts or omissions and the lapses of the institutional and legal regime, whether or not they are effective in fighting cybercrime in Nigeria and relevant in international cooperation against cybercrime. This will be achieved by examining the provisions of the Economic and Financial Crimes Commission (the EFCC) Act;[1] the Criminal Code Act[2], the Penal Code Act,[3] the Anti-terrorism Act,[4] the Money Laundering Act,[5] the Evidence Act[6] the Advance Fee Fraud Act,[7]the National Identity Management Commission Act, 2007 and the Cybercrime Act, 2015.

Institutional regimes discussed are; the EFCC, the Federal Ministry of Justice, the Directorate of Cyber security, National Information Technology Development Agency, the National Identity Management Commission. This chapter also shows how Nigeria is poised among the comity of Nations in International cooperation against cybercrime.

[1] Economic and Financial Crimes Commission (Establishment) Act 2004
[2] Criminal Code Act, Laws of Nigeria, 2004.
[3] Penal Code law of Kaduna State, 1991.
[4] The Terrorism (Prevention) Act, 2013.
[5] Money Laundering (Prohibition) Act No. 1, 2011 and Money Laundering (Prohibition) (Amendment) Act 2012.
[6] The Evidence Act No.18 2011.
[7] Advance Fee Fraud and other related Offences Act No. 14, 2006.

3.2 The Role of Economic and Financial Crimes Commission (Establishment) Act 2004 and the Commission in fighting cybercrime[8]

The preponderance of cybercrimes involving advance fee fraud(419), money laundering, phishing to mention a few has had severe negative consequences on Nigeria, including decreased Foreign Direct Investments in the country and tainting, Nigeria's image.[9]The menace of cybercrime and the magnitude and gravity of the situation led to the passing into law of the EFCC Act 2004. The EFCC Act also establishes the Economic and Financial Crimes Commission (the EFCC) to implement and execute the provisions of the act.

Specifically, the EFCC Act mandates the Commission to collaborate with government bodies within and outside Nigeria concerning the following:

a) The identification, determination of the whereabouts and activities of persons suspected of being involved in economic and financial crimes,

b) The movement of proceeds or properties derived from the commission of economic and financial and other related crimes;

c) The exchange of personnel or other experts;

d) The establishment and maintenance of a system for monitoring International Economic and Financial crimes in order to identify suspicious transactions and persons involved;

e) Undertaking research and similar works with a view to determining the manifestation, extent, magnitude and effects of economic and financial crimes, advising government on appropriate intervention measures for combating same.

[8]See Ladan M.T.,(2013) *"Appraisal of Legal, Regulatory And Institutional Frameworks In Combating Money Laundering And Terrorism Financing In Nigeria"* being an independent study on the recent legal, regulatory and institutional regimes (2011-2013) in combating money laundering and terrorism financing in Nigeria Zaria, Kaduna state, Nigeria. Pp. 12-16. Blogsite: - http://mtladan.blogspot.com/accessed on 7/5/14 by 8:00pm.

[9] See Fight Against Cybercrime, Legislation As Rescue at http://callcenterinfo.tmcnet.com/news/2006/04/14/1573060.html

Since its establishment, the Commission has investigated and prosecuted several offences relating to cybercrimes.[10]The writer however observes that this is not adequate considering the rate acts and omissions that constitute cybercrimes under the Budapest Convention are committed in Nigeria today and the EFCC Act is not cybercrime specific.

The power of the Commission to investigate all financial crimes including advance fee fraud, money laundering, counterfeiting, illegal charge transfers, future market of negotiable instruments, computer credit card fraud, contract scam etc has been subjected to serious judicial contest and some pronouncements, the end result is that the trials particularly that of politically exposed persons are unnecessarily delayed and thus no appreciable progress has been achieved over the years. In plethora of these cases, the trial hardly go beyond the initial stage of arraignment before being stalled owing to multiple preliminary applications ranging from challenges of territorial jurisdiction of the trial courts, the propriety of the indictments/charges and to a large extent, the authority of the prosecuting authorities to try the accused persons, often citing the federal system envisaged in the Nigerian Constitution as an excuse.[11]These challenges are discussed below.

Though Inchoate offences similar to cybercrime are mostly prosecuted by the EFCC under section 7 of the EFCC Act and relevant sections of the Criminal Code Act,[12]the Penal Code law[13]and Advance Fee Fraud Act, 2006[14] and generally other laws of Nigeria, they are not adequate enough to fight cybercrime.

---

[10] See section 1 of the EFCC Act, 2004 and http://www.efccnigeria.org/index.php?option=com_contact&catid=4&Itemid=3. Accessed on the 20th April, 2014 by 8:00pm.

[11] See Over 288 persons jailed for internet fraud, EFCC says at www.cybercrimejournal.com

[12] See Sections 382 to 390 of the Criminal Code on stealing, Sections 418 to 426 on cheating and obtaining property by false pretences, Sections 434 to 439 on fraud and false accounting 463 to 483 of the criminal Code on the offence of forgery generally, and Section 484 to 489 on personating. Telecommunication offences are regulated by Sections 161 to 189.

Generally, in a bid to fight crime in Nigeria, the EFCC Act 2004 has vested the following powers in the commission as follows:

1. The Commission is only charged with the responsibility of enforcing the provisions of the following Acts:
   (a) The Money Laundering Act 2004; 2003 No.7 1995 No. 13.
   (b) The Advance Fee Fraud and Other Fraud Related Offences Act 1995;
   (c) The Failed Banks (Recovery of Debts) and Financial Malpractices in Banks Act 1994, as amended;
   (d) The Banks and other Financial Institutions Act 1991, as amended; and
   (e) Miscellaneous Offences Act
   (f) Any other law or regulations relating to economic and financial crimes, including the Criminal code or Penal code.

The writer opines that section 7(f) of the EFCC Act, particularly the phrase that "any other law or regulations relating to economic and financial crimes…" is an omnibus clause which gives the EFCC unlimited powers to fight crime. This omnibus clause causes friction between the EFCC and other law enforcement agencies.[15]

Though the Advance Fee Fraud and Other Fraud Related Offences Act 1995 and other laws referred to in the EFCC Act, 2004and to be enforced by the EFCC are archaic

---

[13] See Sections 362 to 380 on forgery, Section 179 on false personating and Sections 320 to 325 on cheating.14See Sections 1, 2, 3, 4, 5, 6, 7, 8 and 9 of the AFF Act 2006 on telecommunication offences.
[14] See Sections 1, 2,3,4,5,6,7,8 and 9 of the AFF Act, 2006.
[15]There has been several clashes between the EFCC ICPC in the course of executing their mandates. While by virtue of its enabling Act the ICPC targets corruption in the public sector, especially bribery, gratification, graft and abuse or misuse of office, the EFCC by the wide powers vested in it by its enabling act investigates people in all sectors who appear to be living above their means and is empowered to investigate and prosecute money laundering and other financial crimes. The EFCC tracts illicit wealth accruing from abuse of office, especially attempts to integrate such wealth in to the financial system. There has been tension between the two commissions. Due to the tension, the ICPC Chairman complained about the duplication of functions of ICPC, particularly the overlap between the ICPC anti- corruption and transparency committees. A solution to this problem almost came when there was a proposal in the Nigerian Senate to merge the EFCC and the ICPC, but this proposal never became a reality.

laws which are not in use any more, yet that the EFCC Act states that the EFCC has the mandate to implement them. According to Professor Ben Nwabueze (SAN) the EFCC Act is illegal.[16] His argument is on the basis that Section 174 of the 1999 Constitution of Nigeria (as amended) vests the powers to prosecute criminal matters in the Attorney General of the Federation and not in the EFCC. His argument is primarily on the prosecution of the crimes and not on the investigation of crimes which the EFCC also carries out.

The EFCC carries out its mandate with other units like the Nigerian Financial Intelligent Unit, Special Control Unit against Money Laundering, National Insurance Commission, Securities and Exchange Commission and the Central Bank of Nigeria. The roles played by the above listed units and establishments in fighting Money Laundering is discussed in a bid to see how effective they are in the fight against cybercrime.

3.2.1 The Nigerian Financial Intelligence Unit[17]

The rationale behind the establishment of the Nigerian Financial intelligence Unit (NFIU) is to safeguard the Nigerian Financial system and contribute to the global fight against money laundering, terrorism financing and related crimes through the provision of credible financial intelligence. Considering that there are different FIU models, Recommendation of the Financial Action Task Force (FATF) do not prejudge a country's choice for a particular model and applies equally to all of them. The Recommendation however emphasizes that countries should establish an FIU with responsibility for acting

[16]See www.nigeriavillagesquare.com/forum/.... accessed on 20th April, 2014 by 8:00am.

[17]Ladan M.T. (2013) "*Overview of Financial Laws in Nigeria*" being a paper presented at a training workshop on drafting financial legislation for legal officers and staff of committee on appropriation of the national and state houses of assembly organized by: The National Institute For Legislative Studies (NILS) in collaboration with West Minister Foundation for Democracy, 18th March, 2014 and Recent Trends in Regulating Money Laundering & Terrorism Financing in the Banking, Insurance and Capital Market Sectors Of The Financial Economy of Nigeria: - Role of the Financial Regulators (A 3-Day National Conference On Money Laundering In Nigeria Organized By: The United States Embassy, Abuja In Collaboration With The Economic And Financial Crimes Commission, Abuja, pp. 29-33 Blogsite: - http://mtladan.blogspot.com/. And accessed on 4th April, 2014 by 9:00am. See *www.nfiu.gov.ng/* access on 20th January, 2014, 4:00pm.

as a national centre for receipt and analysis of suspicious transaction reports and other information relevant to money laundering, associated predicate offences and terrorist financing; and for the dissemination of the results of that analysis. Further, the FIU should be operationally independent and autonomous in carrying out its core and distinct functions and be free from any undue political, government or industry influence or interference, which might compromise its operational independence. Accordingly, the NFIU is the Nigerian arm of the global financial intelligence Units (FIUs) domiciled within the EFCC as an autonomous unit and operating in the African Region. The NFIU seeks to comply with international standards on combating Money Laundering and Financing of Terrorism and proliferation. The establishment of the NFIU is based on the requirements of Recommendation of the Financial Action Task Force (FATF) Standards and Article 14 of United Nations Convention Against Corruption (UNCAC). The NFIU was admitted into the Egmont Group of FIUs in 2007. The Egmont Group is the global body responsible for setting standards on best practices for FIUs and is made up of more than 131 FIUs from 131 jurisdictions. It was founded in 1995 to foster international collaboration in the exchange of intelligence by member states. It also supports and influences the work of FATF as it relates to the mandate of FIUs under FATF Recommendations 29 and 40. The NFIU, as a member of Egmont Group has reached out to other African FIUs by sponsoring and mentoring them to join the Egmont Group. The Unit has since then sought to develop standards and procedures for the receipt, analysis and dissemination of financial intelligence to law enforcement agencies, perform onsite and off-site examination of financial institutions, enhance compliance with the legal and regulatory regimes on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) in Nigeria as well as respond to the global trends by collaborating with other FIUs worldwide.

Powers/Mandate: - The NFIU largely draws its powers from the Money Laundering (Prohibition) Act 2011 as amended in 2012 and the Economic & Financial Crimes Commission (EFCC) establishment Act, 2002. The core mandate of every FIU as required by international standard is to serve as the national center for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of the analysis to law enforcement and anti-corruption agencies. Other Functions of the NFIU include the responsibility to receive currency transactions reports, suspicious transactions reports; currency declaration reports and other information relating to money laundering and terrorist financing activities from financial institutions and designated non-financial institutions (DNFIs); receive reports on cross-border movement of currency and monetary instruments; maintain a comprehensive financial intelligence database for information collection, analysis and exchange with counterpart FIUs in the jurisdiction and law enforcement agencies in Nigeria; advise the government and regulatory authorities on prevention and combating of economic and financial crimes; provide information relating to the commission of an offence by entities and subjects linked to another jurisdiction to foreign financial intelligence unit based on the membership of Egmont Group or on the basis of bilateral cooperation; promote public awareness and understanding of matters relating to economic and financial crimes, money laundering & financing of terrorist activities; liaise with compliance officers and ensure strong compliance culture by reporting entities. The NFIU has a reporting requirement which requires that it works closely with all the core regulators of financial, other-financial institutions and designated non- financial businesses and professions, namely Central Bank of Nigeria (CBN), National Insurance Commission (NAICOM), Securities

& Exchange Commission (SEC), Special Control Unit against Money Laundering (SCUML), particularly in the receipt of the following reports:

i. Report of international transfer of funds and securities exceeding US$10,000.00 or naira equivalent as required by Section 2 (1) of the MLP.

ii. Suspicious Transaction Reports (STRs) related to potential money laundering activities from reporting entities.

iii. The STRs mentioned under Section 6 (2) of the MLPA 2011 shall be reported exclusively to the NFIU to aid intelligence gathering and in line with Financial Action Task Force (FATF) 2012 Recommendations 20 and 29.

iv. Declaration reports of more than USD$10,000 or its equivalent made to the Nigerian Customs pursuant to the Foreign Exchange Act, 1995 and Section 2 (3) of the MLP Act, 2011 as amended.

v. Currency Transaction Reports (CTRs) that should be submitted directly to the NFIU from the reporting entities as provided in Section 10 of the MLP Act 2011 as amended.

vi. Application of freezing measures under Section 6 (5) (b) of the MLP Act 2011 as amended.

vii. Mandatory Disclosures by financial institutions and any other individual (voluntarily) – related to single transaction, lodgment or transfer of funds in excess of ₦5, 000,000 or ₦1, 000,000 by an individual and ₦10, 000,000 or ₦5, 000,000 by a corporate entity as provided Section 10 (1) and (2), MLP Act.

viii. To determine the flow of transactions and the beneficiaries for individual and corporate accounts as provided by Section 14 MLP Act, 2011 as amended.

ix. Receive STRs on transactions that may relate to Terrorism or terrorist financing from reporting entities as provided under Section 14 of the Prevention of Terrorism Act 2011 as amended in 2013; The financial institutions shall also have regard to the Regulation on the freezing of terrorist assets issued in 2012 by the Attorney General of the Federation and United Nations Security Council Resolutions as issued from time to time.

x. Other statutory reports mandated by the regulators in their AML/CFT Regulations must also be complied with and the reports filed with the NFIU and the regulators.

Section 25 of the MLP Act 2011 as amended in 2012 defines the reporting institutions to include but not limited to:

Financial Institutions: - Commercial Banks; Primary Mortgage Institutions; Micro Finance Banks; Finance Companies; Discount Houses; Bureau de change (BDCs); Development financial institutions (NEXIM, Agric, Rural and Urban development banks, FMBN etc); Money Service Businesses and Transmitters.

Capital and Stock Market Operators: - Stock brokers; Issuing houses; Registrars; Trust Fund and Assets Managers; Investment and Portfolio Managers.

Insurance Sector: - Insurance companies; Reinsurance Companies; Insurance Brokers.

Designated Non-Financial Businesses and Professions (DNFBPs) 33: - Non-Governmental Organizations (NGOs); Estate surveyors and Valuers; Dealers in Precious Stones and Metals; Trust and Company Service Providers; Casinos, Pool Betting and Lottery; Dealers in jewelry, cars and luxury goods; Chartered/professional accountants and Audit firms; Tax Consultants; Legal practitioners; supermarkets; Hotels and Hospitality Industries; and Casinos.

The writer observes that the NFIU the creation of the Nigerian Financial Intelligence Unit (NFIU) was geared towards ensuring that all financial transactions meet with international best practices on monitoring and fighting financial crimes. Indeed, this body ought to be independent enough to be able to also monitor, collate and circulate intelligence to all the agencies of law enforcement charged with the constitutional duty of keeping Nigeria free from money launderers and international kingpins who engage in illegal capital flight that contribute to the economic downfall of the country. Inclusion of legal practitioners as designated non financial institutions is not appropriate as lawyers are not traders and the Legal Practitioners Act is the only law regulating practice of law in Nigeria.

There are regulations on financial transactions for the different sectors of the Nigerian economy. A unique regulation is the Special Control Unit against Money Laundering (SCUML). This is because it affects every Nigerian Citizen, as every citizen of the country use money.

In a bid to educate the general public on how to identify money laundering activities, the Nigerian Financial Intelligence Unit has provided money laundering indicators.

3.2.2 Special Control Unit against Money Laundering[18]

The Special Control Unit against Money Laundering (SCUML) domiciled in the Federal Ministry of Commerce and Industry (FMC&I) has the responsibility under the provisions of the Money Laundering (Prohibition) Act No. 1, 2011 (as amended)[19] to monitor, supervise and regulate the activities of Designated Non-Financial Businesses and Professions in Nigeria. By section 5(4) of the Money Laundering (Prohibition) Act

[18] Section 5(4) of the Money Laundering (Prohibition) Act No. 1, 2011 is not amended by the Money Laundering (Prohibition) (Amendment) Act 2012.

[19] See http://www.scuml.org/userfiles/SCUML%20FINAL%20REGULATORY%20DOCUMENT%5B1%5D.pdf retrieve o**n** 5/4/14 by 5:00am.

No. 1, 2011 (as amended) the Honourable Minister of Commerce and Industry can make regulations for the Designated Non-Financial Businesses and Professions (DNFBP) to protect the designated sectors against money laundering and combating the financing of terrorism. In line with the statutory mandate, the Minister may designate and include businesses and professions to be so regulated. Inclusion of the legal profession as "trading" to be so regulated was challenged and set aside by Justice Gabriel Kolawole of the Federal High Court in the suit between *Registered Trustees of the Nigerian Bar Association vs. the Attorney General of the Federation & the Central Bank of Nigeria*.[20]

This suit is similar with the case of *Federation of Law Societies of Canada vs. the Attorney General of Canada & Canada Bar Association.* Delivering its judgment, the Honourable Madam Justice Gerow noted that the section that has to do with legal practitioners infringes on their rights.[21]The Regulation is guided by the Money laundering Prohibition Act 2011(as amended), Terrorism Prevention Act 2011 (as

[20]In an originating summons dated March 15, 2013 the plaintiffs, the NBA had asked the court to declare that the provisions of Section (5) MLA, insofar as they purport to apply to legal practitioners, are invalid, null and void. The plaintiffs also sought an order of the court deleting legal practitioners from the definition of Designated Non-Financial Institutions (DNFIs) as contained in Section 25 of the MLA, an order of perpetual injunction restraining the CBN from seeking to implement its circular reference FPR/CIR/GEN/VOL.1/028 dated 2nd August 2012 in relation to legal practitioners, and an order of perpetual injunction restraining the Federal Government, acting through SCUML, the National Financial Intelligence Unit (NFIU), EFCC or otherwise howsoever from seeking to enforce the provisions of Section 5 of the MLA in relation to legal practitioners. The respondents had argued that the objective of the MLA and the SCUML was not to monitor the legal practitioner but to monitor their clients who may have the potential to commit heinous crimes, adding that the MLA is a valid and deliberate exercise of legislative power to enact a law in derogation of the rights conferred by Section 37 of the Constitution for the purposes of preventing the financing of terrorism and other criminal activities inimical to public health and safety. In its judgment, the court granted the reliefs sought by the plaintiffs and held that the provisions of the MLA as it applies to legal practitioners are null and void. It also adjudged the inclusion of legal practitioners in the definition of designated non-financial institutions as inapplicable. Justice Kolawole gave an order of perpetual injunction restraining the Federal Government, the CBN and the SCUML from seeking to enforce Section 5 of the MLA against legal practitioners.

[21]She said: "In summary, I have concluded that the Regime infringes s. 7 of the Charter insofar as it applies to lawyers and law firms because it puts both lawyers and their clients' liberty interests in jeopardybyrequiring lawyers to collect and retain information about clients, and make the information available to the government to aid in combating money laundering and terrorist financing. As well, I haveconcluded that the infringement is not justified under s. 1 of the Charter. In my opinion the appropriate remedy is to read down some of the impugned provisions, and sever and strike down other portions. Accordingly, I am making the following declarations: Sections 5(i) and (j) of the Act are inconsistent with the Constitution of Canada and are of no force and effect to the extent that "persons and entities" includes legal counsel and legal firms".

amended),Financial Action Task Force 40 recommendations(February 2012) as well as international best practice documents. Pursuant to the above, the Special Control Unit against Money Laundering (SCUML) issues AML/CFT regulation to guide DNFBP's in the implementation of the Know Your Customer (KYC) and Customer Due Diligence (CDD) requirements for the DNFBP sector. The Regulation not only minimizes the risk faced by DNFBP's on laundering the proceeds of crime but also provide protection against fraud, reputational and institutional market risks.

As part of the effort to ensure that financial crime in cyberspace is curtail, this regulation requires that all DNFBP's businesses shall be conducted in compliance with the requirements of the Money Laundering (Prohibition) Act, 2011 and Terrorism (Prevention) Act, 2011.

3.2.3 Sectoral Regulations against Money Laundering as provided by the NFIU

i. Central Bank of Nigeria (Anti-Money Laundering and Combating of financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013[22]

The CBN Governor made the following Regulations on 29th August 2013 in the exercise of the powers conferred upon him by the provisions of Section 51(1) of the Banks and other Financial Institutions, Act, 2004 and all other powers enabling him in that behalf. In terms of structure and contents, the 133 Regulations are divided into thirteen parts and three schedules. Part 1 deals with the objectives, scope and applications of these regulations. Part 2 covers Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Directives:- AML/CFT institutional policy framework; risk assessment; risk mitigation; designation and duties of AML/CFT Compliance Officers; and cooperation with competent authorities. Part 3 deals with Offences, Measures and Sanctions: - scope of offences includes only terrorism financing offences; targeted

[22]Ladan M.T. (2013) "*Overview of Financial Laws in Nigeria*" Ibid, pp. 1-34.

financial sanctions related to terrorism financing and proliferation; limitation of secrecy and confidentiality laws. Part 4 covers customer due diligence, higher risk customers and activities of politically exposed persons: - customer due diligence ('CDD') measures; identification and verification of customers; verification of beneficial ownership; application of enhanced due diligence to higher risk customers and activities; attention to high risk countries; politically exposed person (PEP); cross-border and correspondent banking; new technologies and non face-to-face transactions; money or value transfer (MVT) services; foreign branches and subsidiaries; wire transfers; simplified due diligence applicable to lower risk customers, transactions or products; timing of verification; existing customers; failure to complete CDD; and reliance on intermediaries and third parties on CDD function. Part 4 covers maintenance of records: - maintenance of records on transactions; attention on complex and unusual large transactions; suspicious transaction monitoring; and procedure for the monitoring and reporting of suspicious transactions. Part 6 deals with monitoring, internal controls, prohibitions and sanctions: - internal controls, compliance and audit; sanctions and penalties for non-compliance; prohibition of numbered or anonymous accounts, accounts in fictitious names and shell banks; other forms of reporting; AML/CFT employee-education and training programme; monitoring of employee conduct; protection of staff who report violations; additional areas of AML/CFT risks; additional procedures and mitigates; testing for the adequacy of the AML/CFT compliance; formal board approval of the AML/CFT compliance; and culture of compliance. Part 7 covers guidance on know your customer (KYC): -three tiered KYC requirements; duty to obtain identification evidence; nature and level of the business; application of commercial judgment; identification; factors to consider in identification; time for verification of identity; exceptions; additional verification requirements; identification of directors and other signatories; joint

account holders; verification of identity for high risk business; duty to keep watch of significant changes in nature of business; verification of identity of person providing funds of trust; savings schemes and investments in third parties' names; personal pension schemes; timing of identification requirements; consequence of failure to provide satisfactory identification evidence; identification procedures; new business for existing customers; certification of identification evidence; concession in respect of payment made by post; term deposit account ('TDA'); and investment funds. Part 8 deals with general information: - establishing identity; private individuals – general information; private individuals resident in Nigeria; and electronic checks. Part 9 covers financial exclusion for the socially or financially disadvantaged applicants: - "Financial Exclusion" for the socially or financially disadvantaged applicants resident in Nigeria; private individuals not resident in Nigeria; non face-to-face identification; refugees or asylum seekers; students and minors; and quasi corporate customers. Part 10 deals with trust, policy, receipt and payment of funds: - trust, nominees and fiduciaries; off-shore trusts; conventional family and absolute Nigerian trusts; receipt and payment of funds; identification of new trustees; life policies placed in trust; and powers of Attorney and third party mandates. Part 11 covers executorship, client accounts, un-incorporated and corporate organizations: - executorship accounts; "Client Accounts" opened by professional intermediaries; un-incorporated business or partnership; limited liability partnership; pure corporate customers; the identity of a corporate company; non face-to-face business; public registered companies; private companies; higher risk business relating to private companies; foreign financial institutions; bureau de change; designated non-financial businesses and professions (DNFZBPs); occupational pension schemes; registered charity organizations; religious Organizations (ROs); three-tier of government and parastatals; and foreign consulates; and intermediaries or other third parties to verify

identity or to introduce business. Part 12 deals with introductions, applications and foreign intermediaries: - introductions from authorized financial intermediaries; written applicants; non-written application; foreign intermediaries; corporate group introductions; business conducted by agents; syndicated lending; correspondent relationship; acquisition of one financial institution and business by another; vulnerability of receiving bankers and agents; categories of persons to be identified; applications received through brokers; applications received from foreign brokers; and multiple family applications. Part 13 covers linked transactions, foreign accounts and investment: - linked transactions; foreign domiciliary account (FDA); safe custody and safety deposit boxes; customer's identity not properly obtained; exemption from identification procedures; one-off cash transaction, remittances and wire transfers; re-investment of income; amendment or revocation of these regulations; interpretation; and citation.

Finally, schedules 1-3 of these Regulations relate to the following matters respectively: -sanctions and penalties; information to establish identity; and money laundering and terrorist finance red flags.

a) Rationale, scope and applications[23]

The rationale behind the AML/CFT 2013 Regulations made by the Governor of Central Bank of Nigeria, is to ensure that the banking industry and other financial institutions of the Nigerian economy comply with the subsisting Anti-Money Laundering and Combating the Financing of Terrorism Legislations (namely, the Money Laundering (Prohibition) (Amendment) Act, No.1, 2012, the Terrorism (Prevention) (Amendment) Act 2013 and the Terrorism Prevention (freezing of international terrorists funds and other related measures) Regulations, 2013). Accordingly, the objectives of these Regulations are to: (a) provide Anti-Money Laundering and Combating the Financing of

[23]Ibid, p.1

Terrorism ("AML/CFT") compliance guidelines for financing institutions under the regulatory purview of the Central Bank of Nigeria ("CBN") as required by relevant provisions of the Money Laundering (prohibition) Act, 2011 (as amended), the Terrorism Prevention Act, 2011 (as amended) and other relevant laws and Regulations; (b) enable the CBN to diligently enforce AML/CFT measures and ensure effective compliance by financial institutions; and (c) provide guidance on Know Your Customer ("KYC") measures to assist financial institutions in the implementation of these Regulations. In terms of scope, these Regulations cover the relevant provisions of the Money Laundering (Prohibition), the Terrorism Prevention Act, 2011 (as amended) and any other relevant laws or Regulations. These Regulations cover the following:

(a) the key areas of Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Policy;

(b) development of Compliance Unit and function; (c) Compliance Officer designation and duties (d) the requirement to co-operate with the competent or supervisory authorities;

(f) monitoring and filing of suspicious transactions to the Nigerian Financial Intelligence Unit ("NFIU") and other reporting requirements;

(g) reporting requirements;

(h) record keeping; and (AML/CFT employee training.

These Regulations shall apply to banks and other financial institutions in Nigeria within the regulatory purview of the Central Bank of Nigeria.

ii. National Insurance Commission (Anti-Money Laundering and Countering the Financing of Terrorism) Regulations, 2013.[24]

In the exercise of the powers conferred on it by Section 101 of the Insurance Act, 2004 and all other powers enabling it in that behalf, the national Insurance Commission, with the approval of the Honourable Minister of Finance, made the following Regulations on 29th August 2013. The 34 Regulations are structured into ten parts. Part 1 deals with the objectives and general requirements. Part 2 covers AML/CFT institutional policy and programme: - proceeds of crime; anti-money laundering and countering the financing of terrorism institutional policy framework. Part 3 deals with customer due diligence measures; customer due diligence for beneficiaries of life insurance policy; enhanced customer due diligence (ECDD); simplified customer due diligence (SCDD); timing of verification; failure to complete customer due diligence; establishing a business relationship; existing customers; reinsurance; and on-going due diligence. Part 4 covers suspicious transaction (STR) and currency transaction report. Part 5 deals with AML/CFT training: - AML/CFT training programme. Part 6 covers designation of compliance officer and money laundering reporting officer. Part 7 deals with internal control measures and record keeping. Part 8 covers other high risk activities: - new technology and non face-to-face transaction; offshore operations; risk classification of policy holders; complex and unusual large transactions; and payment under life insurance. Part 9 deals with sanctions. Part 10 covers miscellaneous: - interpretation; revocation; and citation.

a) Rationale, application and general requirements[25]

The rationale behind the National Insurance Commission (NAICOM) (Anti-Money Laundering and Countering the Financing of Terrorism) Regulations, 2013 is to regulate and ensure that the insurance industry complies with subsisting Anti-Money

[24]Ibid, pp. 34-35
[25]Ibid, p. 34.

Laundering and Countering the Financing of Terrorism Legislations in Nigeria. In terms of application, Regulation 2 provides that these Regulations shall apply to all insurance institutions in Nigeria including their agents and insurance brokers, and to all insurance transactions. Setting out the general requirements for compliance by all insurance businesses, Regulation 3 provides that all insurance businesses shall comply with the requirements of the Insurance Act, 2003, National Insurance Commission Act, 2004, Money Laundering (Prohibition) Act, 2011 (as amended), Terrorism (Prevention) Act, 2011 (as amended) and Terrorism Prevention (Freezing of International Terrorists Funds and other Related Measures) Regulations 2013, including successor laws and Regulations 2. The obligation to establish AML and CFT (AML/CFT) programme shall apply to all insurance institutions and insurance institutions and an insurance company shall in addition integrate its agents and insurance brokers into its AML/CFT framework in order to ensure and monitor compliance with the programme.

iii. Securities and Exchange Commission (Capital Market Operators Anti-Money Laundering and Combating the Financing of Terrorism) Regulations, 2013.[26]

In the exercise of the powers conferred on it Section 13(n), (aa) and (dd), and section 313 of the investments and Securities Act, 2007 and all other powers enabling it in that behalf, the Securities and Exchange Commission (SEC), made, on 29th August 2013, the following Regulations. In terms of structure and contents, the 96 Regulations are divided into eleven parts. Part 1 deals with the objectives; applications and scope. Part 2 covers AML/CFT institution policy framework: - general guidelines on institutional policy; duties of an AML/CFT compliance officer; co-operation with relevant authorities; identification of proceeds of crime; secrecy and confidentiality laws; and anonymous and numbered accounts. Part 3 deals with customer due diligence measures; correspondent

[26]Ladan M.T.(2013) "Overview of Financial Laws in Nigeria" Ibid, pp. 36-38.

relationships with high risk foreign banks; on-going due diligence; application of enhanced customer due diligence (ECDD) for higher risk clients; lower risk categories of clients; timing of verification; application of CDDto application of CDD to existing clients; determination of a politically exposed person; measures to prevent the misuse of new technologies and non face-to-face transactions; reliance on intermediaries and third parties on CDD measures; keeping and maintenance of records of transactions; and complex and unusual large transactions. Part 4 covers internal controls, compliance and audit. Part 5 deals with monitoring and reporting of suspicious transaction, "red flags"; and business relationships with persons from countries which do not apply the FATF recommendations. Part 6 covers employee education and training programme; monitoring of employee conduct; protection of staff who report violations; additional areas of AML/CFT risk; additional procedures and mitigants; testing for the adequacy of the AML/CFT compliance programme; and board approval of the AML/CFT compliance manual. Part 7 deals with know your customer and identification procedures; guidance on know your customer; duty to obtain identification evidence; identification procedure; verification of identification requirements; cancellation and cooling-off rights, redemptions and surrenders; new business transaction by an existing client; certification of identification documents; recording identification evidence; concession in respect of payment made by post; and investment funds. Part 8 covers establishing of identity under these regulations; general information; private individuals resident in Nigeria; physical checks on private individuals resident in Nigeria; electronic checks; private individuals not resident in Nigeria; information to establish identity; identification guidance for institutions; other types of operators; retirement benefit of operators; retirement benefit programmes; mutual or friendly, cooperative and provident societies; charities, clubs and associations; trusts and foundations; professional intermediaries; false identifies and

impersonations; refugees and asylum seeker; identification procedures for opening accounts for students or young person; establishing the identity of trust, nominees and fiduciaries; offshore trusts; conventional family and absolute Nigerian trusts; receipt and payment of funds on behalf of a trust; power of Attorney and third party mandates; executorships accounts; unincorporated business or partnerships; verification of legal existence of a corporate client; non face-to-face business; low risk corporate business; private and public unquoted companies; high risk business relating to private or public unquoted companies; foreign capital market operator; charities in Nigeria; registered charities; clubs and societies; occupational pension schemes; religious organizations (ROs); three-tiers of government and parastatals; and foreign consulates. Part 9 deals with intermediaries or other third parties to verify identity or to introduce business:- introductions from authorized financial intermediaries; written applications; non-written application; introductions from foreign intermediaries; corporate group introductions; business conducted by agents; correspondent relationship; and acquisition of a capital market business by another. Part10 covers receiving capital market operators and agents: - vulnerability of receiving bankers and agents to money laundering; who to identify; applications received via brokers; multiple family applications; linked transactions; and exemption from identification procedures. Part 11 deals with miscellaneous: - sanctions for non-compliance with the provisions of these regulations; revocation; interpretation; and citation.

a) Rationale, application, general guidelines on institutional policy, duties, cooperation, identification of proceeds of crimes, secrecy and confidentiality laws

The rationale behind these Regulations is first, to provide protection to the capital market against fraud, reputational and other financial market risks faced by the Capital Market; second, to protect the integrity of the security market against all forms of abuse,

fraudulent and unfair trade practices, money laundering, proceeds of crime and financing of terrorism; and third, guide the capital market operators in the implementation of Know Your Customer (KYC) and Customer Due Diligence (CDD) requirements for the capital market.

The 96 Regulations are meant to apply to the activities of money laundering and financing of terrorism in the Nigerian capital market operations and related matters. Regulations 3 provides for the following general guidelines on institutional policy. That a Capital market Operator shall: - (a) adopt polices stating its commitment to comply with Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) obligations under the law and regulatory directives to actively prevent any transaction that facilitates criminal activities; (b) formulate and implement internal controls and other procedures that will deter criminals from using its facilities for money laundering and terrorist financing and to ensure that its obligations under subsisting laws and Regulations are met; (c) designate AML/CFT Chief Compliance Officer at the management level, with the relevant competence, authority and independence to implement the institution's AML/CFT compliance programme; and (d) comply with the requirements of the Money Laundering (Prohibition) Act, 2011 (as amended), Terrorism (Prevention) Act, 2011 (as amended) and Terrorism Prevention (Freezing of International Terrorists Funds and other Related Measures) regulations 2013, including related laws and Regulations.

3.2.4 Short comings in Some Crimes which Computer was used and were investigated and Prosecuted by the EFCC

The EFCC has prosecuted several acts or omissions which are classified as cybercrimes under the Budapest Convention. Examples of these are the case of *Mike*

Amadi vs. Federal Republic of Nigeria,[27] the case of *FRN vs. Nvene*[28]*FRN vs. Odiawa*[29]*FRN vs. Usman*and the case of *FRN vs. Chima L. Larry Ikonjiand Blessing Onochie*.[30]

The case of *Mike Amadi vs. Federal Republic of Nigeria*, which is a case involving the cybercrime of phishing was decided based on the Advance Fee Fraud Act. The fraudster, Amadi, cloned the official website of the Nigerian Economic and Financial Crimes Commission, which he used to transact fraudulent financial business with several persons. Amadi was later arrested over the fraud of the sum of US$125, 000.00. He was charged to court and eventually sentenced to 10 year jail term. His appeals to the Court of Appeal and Supreme Court were all dismissed and the 10 year jail term was reaffirmed. The writer observes that the judgment against the accused was primarily based on the fact that he collected money from the victims of his crime, and not on the basis that he cloned the website of the EFCC. In essence, the decision would probably have been in favour of the accused if he only cloned the EFCC website and not defraud his victims.

The case of *FRN vs. Nvene is* a case involving computer forgery and uttering a false document. The Accused was arraigned on two counts of forging a document, a Lord's Providence Swiss/German/Italian Welfare Association knowing it to be false, offences punishable under Section 1(2) (c) of the Miscellaneous Offences Act, 1990 (now Cap. M17 Law of the Federation of Nigeria, 2004) and a third count of attempt to obtain money by false pretence and with intent to defraud in sending a letter containing false pretence to wit; request for financial assistance to carry out welfare projects for Swiss/German/Italian nationals in Nigeria from Bank Cantonale Neuchate and purporting

[27]Unreported judgement of the Nigerian Federal Court of Appeal (Lagos Judicial Division), Appeal Case No: CA/L/389/2005 delivered on Monday the 11th day of June 2007. Before their Lordships; Dalhatu Adamu, OFR, JCA, M.B. Dongban – Mensem, J.P. J.C.A and Paul Adamu Galinje, J.C.A.
[28]2010 E.C.L.R vol. 1 at page 1,
[29]Ibid, at page 25.
[30]See EFCC ALERT! (2007) A publication of the Economic and Financial Crimes Commission, vol. 2, No .1 January 8, pp. 1 and 5.

the letter to be written by Lord's Providence Swiss/German/Italian Welfare Association contrary to Section 8(b) and punishable under Section 1(3) of the Advance Fee Fraud and Other related Offences Act.

The Prosecution called six witnesses and tendered several computer forged documents, including the Central Processing Unit (CPU) of the Computer used in forging the documents. The Accused was convicted and sentenced accordingly.

The writer observes that this case is one of the few cases where the prosecution was able to tender the computer system use in carrying out the crime. The accused would have been discharged and acquitted if he had only forged the documents on the computer and not print out the hard copies; moreover, the soft copies might have been deleted on the computer system even before the matter was charged to court. In cases of cyber crime involving distant computer systems connected via the internet, the computer systems cannot be recovered and tendered in court as the computer may be outside the jurisdiction of the EFCC, in another country. The fact that Nigeria is not a member to the Budapest Convention on Cybercrime is one of the challenges that will be encountered in an attempt to recover such a computer system outside the jurisdiction of the EFCC.

In the case of *FRN vs. Chima Larry Ikonji and Blessing Onochie*the couple was each sentenced to 45 years imprisonment for impersonating the former executive chairman of EFCC, Mallam Nuhu Ribadu to dupe one Mr. William Ellison, an American, of the sum of US$750, 000. They were tried and convicted for identity fraud and not the cybercrime of phishing. In essence, due to the non existence of a cybercrime specific law, the charge of phishing was not preferred against them.

In the case of *FRN vs. Odiawa*, the accused person was arraigned before the High Court of Lagos State, Ikeja Judicial Division on 10th January, 2005 on information containing 54 Counts to which he pleaded Not Guilty. It is apt to note that none of the

counts contained a cybercrime specific offence; hence there was none in Nigeria as at the time this case was instituted.

The gist of the case is that one Harrison Odiwa (alias Abu Belgore) in 2003 sent an e-mail to one Mr. George Robert Blick, an American Citizen resident in Virginia, U.S.A. he used to be a chief executive officer of a company called Enterprise Integration Incorporated (hereinafter called the Enterprise Integration) which he co-founded with two other gentlemen while he was the sole owner of a company called Quest Incorporation Exploration and Development Incorporated (hereinafter called Quest). In the e-mail, Abu Belgore introduced himself as the Chairman of a Contract Review Panel responsible for the job to transfer $20.5million from Nigeria. Mr. George Robert Blick had agreed to use his company Enterprise Integration for the transaction. In a bid to facilitate the transfer of $20.5million, Mr. George Robert Blick was made to part with various sums of money totaling over $2million. It was when he was bankrupt and was threatened by his business partners in the U.S.A.; investigated by the Federal Bureau of Investigation (F.B.I.), tried and sentenced to jail in the U.S.A. that it dawned on him that he was conned. He later came to Nigeria and reported the matter to the EFCC.

In the Course of the Trial, the said Information was amended on a number of occasions, the final one being the amended information dated 14th July, 2005 containing 58 counts. The writer observes that the amendments were made because the prosecutor was trying to grapple with the nature of crime committed by the accused hence it was committed with the aid of computers and there was no cybercrime specific law in Nigeria. These amendments delayed the matter longer than necessary and the accused was convicted only because there were hardcopies of computer generated documents. The conviction would not have hold if only soft copies of computer generated documents were used by the accused in carrying out the crime.

The 58 Counts of offences alleged against the Accused person fell into 5 broad categories of Conspiracy to obtain by False Pretense, obtaining by false pretence, forgery, Uttering and Possession of documents containing false pretences contrary to the Advanced Fee Fraud and Other related Offences Act, Cap. A6, Laws of the Federation of Nigeria, 2004, the Prosecution called 8 witnesses and tendered 120 forged documents and e-mails, while the defence called three witnesses including the Accused person and tendered 25 Exhibits. The Accused was found guilty and sentenced accordingly.

In the writer's opinion, these cases were successfully tried due to the little complexity involved in their commission and the availability of evidence for proof of the prosecution's case. If the convicts carried out the crimes only virtually, the law enforcement agencies would have found it difficult to prove their case, consequently, the accused persons might have been discharged and acquitted.[31] The writer further opines that the case of *FRN vs. Odiawa* was successfully investigated and prosecuted due to the cooperation between the F.B.I. and the E.F.C.C. Even though the EFCC has a vast mandate to prosecute crimes committed under other criminal laws, the Chairman of the Commission had admitted that they encounter great challenges when they have to prosecute crimes committed through the internet. The writer opines that this is no longer the position in Nigeria as the cybercrime Act, 2015 has being passed into law. The Chairman and the Nigeria Bar Association advocate for the making of a cybercrime specific law by the Nigerian legislature.[32]

3.3 The Criminal Code Act Cap. C38 LFN 2004

[31]Complex cybercrimes like creation and dissemination of computer viruses are difficult to prove and prosecute. See Goodman, M.D. et al the emerging consensus on criminal conduct in cyberspace, ibid,pp.5-7

[32]The House of Representatives sitting on Tuesday 27 November 2012 read for the second time 'A bill for an Act to amend the Criminal Code Act, Cap. C38 Laws of the Federation of Nigeria, 2004 in Order to provide for Offences and Penalties Relating to Computer Misuse and Cybercrimes and for Other Matters Connected Therewith (HB.352)'. http://www.nassnig.org/nass2/news.php?id=191**,** retrieved on 10/9/2013 and EFCC, NBA Back Anti-cyber Crime Bill athttp://www.thisdaylive.com/articles/efcc-nba-back-anti-cyber-crime-bill/139206/ both retrieve on 20th January, 2014.

The Criminal Code Act of Nigeria is an Act wholly administered in southern Nigeria. Most crimes committed in southern Nigeria are tried under this law and other laws. Acts or omissions that constitute cybercrimes are prosecuted under the provisions of the Criminal Code of Nigeria under the traditional crimes of stealing, identity fraud, piracy, etc. Specifically, sections 382 to 390 of the Criminal Code are on stealing, sections 418 to 426 on cheating and obtaining property by false pretences, sections 434 to 439 on fraud and false accounting, 463 to 483 of the Criminal Code on the offence of forgery generally, and sections 484 to 489 on personating. Telecommunication offences are regulated by Sections 161 to 189.

Law enforcement agencies like the EFCC and the Nigeria Police Force have the mandate to prosecute crimes and hence, prosecute these offences. Examples of such offences successfully prosecuted by law enforcement agents are the case *Mike Amadi vs. Federal Republic of Nigeria*(supra) *Chima Larry Ikonji vs. Blessing Onochie* (supra).

However, the writer observes that the provisions of this law are not adequate to fight cybercrimes. This is because it does not contain any cybercrime specific laws.

3.4 The Penal Code Law, Cap. 110 laws of Kaduna State, 1991

The Penal Code is mainly applicable in northern Nigeria. Law enforcement agencies prosecute all criminal offences committed in northern Nigeria under this law. For instance, sections 362 to 380 are on forgery, section 179 is on impersonation, sections 320 to 325 are on cheating and section 334 is on telecommunication offences, to mention a few. All offences including acts or omissions classified as cybercrimes under the Budapest Convention are prosecuted by law enforcement agencies under this law. This is by prosecuting cybercrimes as traditional crimes. An example of an offence classified as cybercrime (identity theft) under the Budapest Convention is the crime of impersonation.

In the case of *FRN vs. Muitala Abbas Ubandawaki,* who is serving a 10year jail term for impersonating the former EFCC boss, Mallam Nuhu Ribadu. Ubandawaki by use of computer generated documents and the internet conned the former Governor of Zamfara State – Nigeria, Alhaji Sani Ahmad Yarima and obtained the sum of ₦1million from him while presenting himself as Ribadu.[33]

3.5 Terrorism (Prevention) Act 2011, as Amended in 2013 and Regulations, 2013[34]

Under the Anti-terrorism Act, acts referred to as terrorist activities are many but there is neither a specific cybercrime offence nor cyber terrorism offence. In other words, acts or omissions carried out by terrorists in cyber space against Nigeria are not specifically referred to as acts of cyber terrorism.[35]

Though there is no discovery of an act of cyber terrorism yet in Nigeria, the internet plays a great role in aiding terrorists' activities.[36] At a three-day conference on cybercrime held in Lagos,[37]Dr. Martins Ikpehai, chief executive officer, Computer Audit and Security Associates Ltd., Lagos heightened tension of the participants when he disclosed that the third world war might be fought on the computer considering how different attacks were being launched through internet. Ikpehai, expressing concerns on how terrorists have been distorting information on internet, said internet facility has recently become an instrument of terrorism. He reiterated that the third world war might

---

[33]See EFCC ALERT! A publication of the Economic and Financial Crimes Commission, (ibid), pp.1and 5.

[34]See Ladan M.T. (2013) , *"Appraisal of Legal, Regulatory and Institutional Frameworks in Combating Money Laundering and Terrorism Financing in Nigeria"* being an independent study on the recent legal, regulatory and institutional regimes (2011-2013) in combating money laundering and terrorism financing in Nigeria Zaria, Kaduna state, Nigeria, pp. 36-40. Blogsite: - http://mtladan.blogspot.com/.

[35]See Goodman M.D. et al. *"The Emerging Consensus on Criminal Conduct in Cyberspace*," UCLA Journal of Law and Technology (ibid),pp. 51-52. Also see en.wikipedia.org/wiki/internet_and_terrorism.

[36]International Telecommunication Union Cybercrime Legislation Resources. 'Understanding cybercrime: A guide for developing countries' Draft, April, 2009,www.itu.int/ITU.D/cyb/**,** p. 55. retrieve on 8th November, 2013 by 4:09pm.

[37]See www.saycocorporativo.com/saycoUK/BIJ/journal/Vol3No1/Article_7**,** p.2. retrieve on 8th November, 2013 by 4:00pm and Nigeria Ranked Third In The World For Cyber-Crime, Says Survey - See more at:http://www.balancingact-africa.com/news/en/issue-no-302/computing/nigeria-ranked-third/en#sthash.TdPUGs7Z.dpuf, retrieve on 27th January, 2014 by 8:00pm.

be fought on computers as terrorist groups like Al Qaeda have been taking advantages of internet facilities to launch attacks and invectives.

Okonigene, R. E., et al. in their article titled" *Cybercrime in Nigeria*"[38]state that Nigerian websites and email system were used by Al Qaeda to disseminate internet information. This has once again brought up the pertinent questions of the safety and security of Nigeria's national cyberspace. Furthermore, in view that Nigeria is not a party to the Budapest convention on cybercrime, international cooperation against terrorist activities in Nigeria and all over the world may be hard to come by.

Today, some international terrorist organizations finance terrorist activities all over the world by internet trade. For instance, a local terrorist may order for goods on-line and they are paid for by their financiers whom may be based abroad or in the country their financiers are based.[39]The goods are delivered to the local terrorist whom sells them and converts the proceeds to finance terrorist activities.

The above scenarios necessitated the passing into law the first anti-terrorism Act in Nigeria in 2011. The first ever Terrorism (Prevention) Act, No. 10, 2011 came into force with the aim of providing for measures for the prevention, prohibition and combating of acts of terrorism, the financing of terrorism in Nigeria and for the effective implementation of the Convention on the Prevention and Combating of Terrorism and Terrorism Financing; as well as prescribe penalties for violating any of its provisions.

The Terrorism (Prevention)(Amendment) Act, 2013 amends the 2011 Act and makes provision for extra-territorial application of the Act and strengthens terrorist financing offences in the following ways:

[38]Through this method, the terrorists are able to sell the goods and use the money for their terrorist acts. See www.saycocorporativo.com, ibid.

[39]Terrorists also finance their activities through business activities. Through buying and selling, they are able to raise cash to procure weapons or items for terrorist activities.

First, Section 13 of the 2013 Amended Act prohibits financing of terrorism and provides for a liability regime with stiffer sanctioning strategy as follows: 13(1) Any person or entity who, in or outside Nigeria –

a) Solicits, acquires, provides, collects, receives, possesses or makes available funds, property or other services by any means to –

   i. terrorists, or

   ii. terrorist groups, directly or indirectly with the intention or knowledge or having reasonable grounds to believe that such funds or property will be used in full or in part in order to commit an offence under this Act or in breach of the provisions of this Act,

b) Possesses funds intending that it be used or knowing that it will be used, directly or indirectly, in whole or in part, for the purpose of committing or facilitating the commission of a terrorist act by terrorist or terrorist groups, commits an offence under this Act and is liable on conviction to imprisonment for life imprisonment,(2) Any person who knowingly enters into, or becomes involved in an arrangement - a) which facilitates the acquisition, retention or control by or on behalf of another person of terrorist fund by concealment, removal out of jurisdiction, transfer to a nominee or in any other way, or(b) as a result of which funds or other property are to be made available for the purposes of terrorism of for the benefit of a specified entity or proscribed organization, commits an offence under this Act and is liable on conviction for life imprisonment.(3) For an act to constitute an offence under this section, it is not necessary that the funds or property were actually used to commit any offence of terrorism. Second, Section 14 of the same Act outlaws dealing in terrorist property by any person or entity, knowingly and provides equally for a liability regime that may attract at least 20

years jail term. According to Section 14(1) A person or entity who, knowingly does the following:

a) deals, directly or indirectly, in any terrorist funds;

b) acquires or posses terrorist fund,

c) enters into, or facilitates, directly or indirectly, any transaction in respect of a terrorist funds,

d) concerts, conceals, or disguises terrorist funds or property, or

e) provides financial or other services in respect of terrorist fund or property at the direction of a terrorist or terrorist group, commits an offence under this Act and liable on conviction to imprisonment for a term of not less than twenty years.

(2) It is a defense for a person charged under subsection (1) of this section to prove that he did not know and had no reasonable cause to suspect or believe that the arrangement is related to a terrorist property.

Section 32 of the amended Act confers the jurisdiction to try all prohibited acts of terrorism and financing of terrorism under the amended Section 1, on the Federal High Court located in any part of Nigeria, regardless of the location where the offence is committed; and to impose any prescribed penalty (ranging from death sentence and life imprisonment to lower prison terms) on any convicted person.

The amended Section 33 empowers the Court to, in addition to any penalty imposed, order the forfeiture of any proceed or fund traceable to a terrorist act and includes proceed or fund irrespective of the person in whose names such proceeds or funds are standing or in whose possession they are found.

In the exercise of the powers conferred on the Attorney-General of the Federation and Minister of Justice by Section 9(6) and 39 of the Terrorism (Prevention) Act 2011, as

amended in 2013, the Regulations on the Freezing of International Terrorists Funds and other Related Measures, 2013 were made in August 2013with the aim of prescribing the procedure for the freezing of funds, financial assets or other economic resources of any suspected terrorist, international terrorist or an international terrorist group, the conditions and procedure for utilization of frozen funds, or economic resources and constituted the Nigeria Sanctions Committee for the purpose of Proposing and designating persons and entities as terrorists within the framework of the Nigerian legal regime. In terms of scope of application, the regulations shall apply to any person or entity listed under Regulation 3(1) as follows:

a) designated persons contained in the Consolidated List of the United Nations 1267 and 1988 Sanctions Committee (‘the UN Consolidated List’);

b) designated persons approved by the Nigeria Sanctions Committee under the Nigeria (‘the Nigeria List’); and

c) all law enforcement agencies to implement measures to prevent the entry into or the transit through the Nigerian borders or the direct or indirect supply, sale and transfer of arms and military equipment by any individual or entity associated with Al Qaeda, or the Taliban, including other international terrorists based on requests from other countries or other third parties.

The above Regulations are structured into ten parts. While Part 1 deals with preamble, purpose and scope; Part 2 covers the constitution of the Nigeria Sanctions Committee and the effective implementation of the relevant UN Security Council Resolutions; Part 3 provides for the freezing of funds procedure and reference to lists by financial, designated non-financial institutions, law enforcement and security agencies;

Part 4 relates to funds held by designated persons; Part 5 prohibits making funds, financial services or economic resources available to designated persons and circumventing prohibitions; Part 6 lays down the conditions and procedure for utilisation of frozen funds; Part 7 places travel restrictions and arms embargo on designated persons; Part 8 provides for information and reporting obligations; Part 9 on penalties and sanctions provides for a maximum of 5 years of imprisonment for any individual or corporate or institutional violator of the regulations; and Part 10 on miscellaneous matters covers revocation of the 2011 Regulations, guidelines for effective implementation, interpretation and citation.

The writer observes that there is no specific reference to cyber terrorism in the Anti-terrorism laws of Nigeria. This makes one to put a poser as follows: how will Nigeria law enforcement agencies likely prosecute acts or omissions which constitute cyber terrorism in Nigeria?

3.6 The Evidence Act

Evidence is the means by which facts are proved, excluding inferences and arguments. It is anything presented in support of an assertion.[40]

The Evidence Act, 2011 is the latest Nigeria law on admissibility of evidence by Courts of Law in Nigeria. It is applicable to all criminal trials in Nigerian Courts of Law.

Generally, all evidence is admissible under the Evidence Act once it is relevant.[41]

Section 84 of the Evidence Act relates to admissibility of electronically generated evidence. In most cases, electronically generated evidence is tendered by third parties and this amounts to hearsay. This section is also an exception to the hearsay rule of evidence, which states that hearsay evidence will otherwise be inadmissible.

[40] See the commencement page of the Evidence Act, 2011.
[41] Ibid, Section 2.

By Section 41 the Evidence Act, where even though the maker of the evidence cannot be called to give primary evidence of the "hearsay evidence", such evidence is established to have been made and kept contemporaneously in an electronic device, in the ordinary cause of business or in the discharge of a professional duty or in acknowledgment, written or signed, of the receipt of money, goods, securities or of property of any kind. Where the statement and the recording of the transaction are not instantly contemporaneous, they must occur such that a Court of Law will consider it most likely that the transaction was at the time of the record, still fresh in the memory of the maker of the recorded statement.

Section 258 (1) (d) of the Act describes a document, for the purpose to include "any device by means of which information is recorded, stored or retrievable including computer output". A computer is in turn described to be "any device for storing and processing information and any reference to information being derived from other information is a reference to its being derived from its calculation, comparison or any other process."

Been that it may be difficult to carry computers around, secondary evidence of computer evidence are tendered in most cases. Primary documentary evidence is the original document itself produced for inspection of the Court. Secondary evidence is a copy of primary evidence produced for inspection by the court.

Section 86(3) of the Evidence Act 2011 provides that where a number of documents have all been produced by one uniform process as in the case of printing, lithography, photography, computer or other electronic or mechanical process, each of such documents shall be the primary evidence of the contents of all the documents so produced by this one uniform process.

As for documents signed electronically, Section 93 (1-3) of the Evidence Act, 2011 provides that an electronic signature will satisfy the legal requirement that a document must be signed where the electronic signature shows that a procedure was followed whereby the person that executed a symbol or followed some other security procedure verifying that an electronic signature was made to an electronic record, actually followed an established procedure.

The earliest and commonly referred to case law on the admissibility of electronic evidence in Nigeria is the Nigerian Supreme Court decision in *Esso West Africa Inc. vs. T. Oyebgola*[42]where the Supreme Court said orbiter that "the law cannot be and is not ignorant of modern business methods and must not shut its eyes to the mysteries of the computer."

The document that called for the decision of the Court is this case was one that was signed in quadruplicate with carbon copies through one single process with the original copy. The Supreme Court ruled on this matter, relying on the old section 93 of the 1945 Evidence Act to hold that where a number of documents have been made by one single paper, each of such document so reproduced is primary evidence of the quadruplicate copies. The *Esso West Africa Inc. vs. T. Oyegbola* case was referred to in the case of *Yesufu vs. A.C.B.*[43]where the document that was tendered with objection by opposing Counsel was a bank statement prepared by a Machinist from the ledger of card of the Respondent Bank; the Machinist obtained the entries from the Respondent Bank's day-to-day vouchers. The bank officer that tendered the statements did not personally prepare the statements or verify that the statements were correct. Objection was raised to the admissibility of the bank statements on the grounds that the existence of the bankers book from which the entries were extracted was not established neither was the custody

[42](1969) 1NMLR 194, 27.
[43](1976) 4 SC (reprint) 1 at pages 9-14.

and control, with the examination of the original entries established before the lower court admitted the bank statements. The Supreme Court held in the case of *Yesufu vs. A.C.B.* (supra) that the admission of the bank statements which entries were derived from day-to-day vouchers of the Respondent Bank did not qualify without supporting oral evidence, as bankers book and therefore offended the provision of the Section 96 (1) (h) of the 1945 Evidence Act. The Supreme Court did however refer to the orbiter in the case *of Esso West Africa Inc. vs. T. Oyegbola* (supra) and said as follows:

> ….it would have been much better, particularly with respect to a statement of account contained in a book produced by a computer, if the position is clarified beyond doubt by legislation as has been done in the English Civil Evidence Act, 1968.

In generating and tendering electronically generated evidence in cases involving cybercrimes, law enforcement agencies and Courts of law in Nigeria follow the procedure laid down by the Nigerian Evidence Act, 2011.

The writer observes that in as much as the Evidence Act provides for means of proof of electronic evidence, it is not sufficient to prove cybercrimes as most acts of cybercrimes are done through computers which may not produce hard copies of the actions involved in the crime as proof of the criminal actions.

3.7 The Federal Ministry of Justice

The Federal Government of Nigeria in the year 2010 approved the establishment of a Computer Crime Prosecution Unit (CCPU) for the prosecution of those involved in cyber crime related offences. This Unit was established under the Federal Ministry of Justice.[44]

[44]See FG Okays Establishment of Computer Crime Prosecution Unit in Nigeria - See more at: http://www.balancingact-africa.com/news/en/issue-no-518/computing/fg-okays establishment#sthash.I0zOlg0r.dpuf. retrieve on 30th December, 2013 by 2:00pm.

The approval for the establishment of the Unit was given by a then Attorney General of the Federation and Minister of Justice, Mohammed Adoke. While giving the approval, he stated that cyber crimes could not be successfully prosecuted without developing the necessary structure and capacity in that area.

The CCPU is under the Public Prosecution Unit of the Federal Ministry of Justice and also harmonise into appropriate policies and legislation the various efforts so far made by some sectors like the Economic and Financial Crimes Commission (EFCC), the telecoms and banking sectors in addressing the cybercrime in Nigeria. Officers to man the unit are trained in basic cyber prosecutors' courses and electronic evidence handling among others.

Recently this unit drafted and submitted the cybercrime bill, 2013 to the Federal Executive Council of Nigeria[45] and same has been passed into law.

3.8 Directorate for Cyber security (DfC)

The Directorate for Cyber security (DfC), was created as a permanent autonomous body within the Office of the National Security Adviser (ONSA) to takeover all assets and liabilities of the NCWG, including all uncompleted projects.[46]

[45] African Independent Television (AIT) News Bulletin, 4:00pm, 5, September, 2013.

[46] In 2004, the former President, Chief Olusegun Obasanjo, formed a cybercrime committee - a 15-member committee consisting of representatives from the government and private sector and tasked them with designing solutions for Nigerian internet-based fraud and cybercrime. The Committee was made up of Economic and Financial Crimes Commission (EFCC), Nigeria Police Force (NPF); the National Security Adviser (NSA), the Nigerian Communications Commission (NCC);Department of State Services (DSS); National Intelligence Agency (NIA); Nigeria Computer Society (NCS);Nigeria Internet Group (NIG); Internet Services Providers'Association of Nigeria (ISPAN); National Information Technology Development Agency (NITDA), and Individual citizen representing public interest.
The committee then formed the Nigerian Cybercrime Working Group (NCWG), and after several months of hard work and determination, presented a 'Draft Nigerian Cybercrime Act' to the President. The Act passed the first reading in the Nigerian National Assembly but the committee later crumbled the Act and it died. See http://www.thisdaylive.com/articles/growing-menace-of-cybercrime/125466/by Udotai B. Directorate for Cybersecurity (DfC) Office of the National Security Adviser Three Arms Zone Aso Rock Villa, Abuja, retrieved 10/9/2013 by 6:00pm.

The mandate of this directorate is as follows:

i. Developing effective framework and interfaces for inter-agency collaboration on cybercrime and cyber security;

ii. Establishing appropriate platforms for public private partnership (PPP) on cyber security;

iii. Coordinating Nigeria's involvement in international cyber security.

iv. Cooperation to ensure the integration of our country into the global frameworks on cyber security;

v. Executing such other functions and responsibilities as it shall consider necessary for the general purpose of promoting cyber security in Nigeria and fostering a framework for critical information infrastructure protection in the country.

Its main mandate is to develop and implement a National Cyber security Policy for Nigeria.

The writer observes that the Directorate is doing its best to reduce the effect of cybercrime on the Nigerian Economy.[47]

3.9 National Information Technology Development Agency

This Agency is created by the National Information Technology Development Agency Act 2007.

The functions of the Agency are as follows:[48]

(a) Create a frame work for the planning, research, development, standardization, application, coordination, monitoring, evaluation and regulation of Information Technology practices, activities and systems in Nigeria and all

[47] See http://www.cipaco.org/spip.php?article1272retrieved on 6/2/14 by 8:00pm.
[48] See Section 6 of the Act.

matters related thereto and for that purpose, and which without detracting from the generality of the foregoing shall include providing universal access for Information Technology and systems penetration including rural, urban and under-served areas.

(b) Provide guidelines to facilitate the establishment and maintenance of appropriate for information technology and systems application and development in Nigeria for public and private sectors, urban-rural development, the economy and the government.

(c) Develop guidelines for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper-based methods in government, commerce, education, the private and public sectors, labour, and other fields, where the use of electronic communication may improve the exchange of data and information.

(d) Develop guidelines for the net working of public and private sector establishment.

(e) Develop guidelines for the standardization and certification of Information Technology Escrow Source Code and Object Code Domiciliation, Application and Delivery Systems in Nigeria.

(f) Render advisory services in all information technology matters to the public and private sectors.

(g) Create incentives to promote the use of information technology in all spheres of life in Nigeria including the setting up of information technology parks.

(h) Create incentives to promote the use of information technology in all spheres of life in Nigeria including the development of guidelines for setting up of information technology systems and knowledge parks.

(i) Introduce appropriate regulatory policies and incentives to encourage private sector investment in the information technology industry.

(j) Collaborate with any local or state Government, company, firm, or person in any activity, which in the opinion of the agency is intended to facilitate the attainment of the objective of this act.

(k) Determine critical areas in Information Technology requiring research intervention and Development in those areas.

(l) Advice the Government on ways of promoting the development of information technology in Nigeria including introducing appropriate information technology legislation, to enhance national security and vibrancy of the industry.

The writer observes that the functions of this Agency are such that they have a very important role to play in the fight against cybercrimes. This is because as a regulatory agency saddled with the responsibility to plan, develop and promote the use of information technology in Nigeria, they are in a position to make regulations useful in combating cybercrimes.

3.10 The National Identity Management Commission Act, 2007

The National Identity Management Commission Act 2007 is an Act repeals the National Civic Registration Act, Cap 240, Laws of the Federation of Nigeria 2004 and establishes a National Database for the Country and the National Identity Management Commission as the Statutory body charged with the responsibility of maintenance of the

National Database, the registration of individuals, issuance of general purpose Identity Cards among other things.[49]

This Act and Commission are important in the fight against cybercrime as it has a very crucial role in checking the act or omission of Identity theft or phishing.[50]

The Act is to be administered by the Commission.[51]The Act provides for the registration of individuals upon which they are given a national identification number.[52]

Section 27 of the Act contains a list of mandatory transactions for which individuals must use their identification number as follows:

i. Opening of personal bank account,

ii. Purchase of insurance,

iii. Payment of taxes

iv. All consumer credit transactions etc.

The writer observes that if this would be implemented, it will reduce the crime of identity theft to a reasonable extent.

3.11 The Advance Fee Fraud Act No. 14, 2006

The advance Fee Fraud Act 2006 is an Act to create offences pertaining to advance fee fraud[53] and other fraud related offences.

Sections 1 and 2 of the Act makes it an offence for any person to obtain property from another person in Nigeria or outside Nigeria or induce a person to deliver property

[49]See the Explanatory Memorandum of the Act.

[50]This is one of the most committed cybercrime in the world today. It is akin to obtaining under false pretences.

[51]The internet services providers rarely obtain the personal information of their customers. Even if they did, internet modem devices sold by GSM service providers have made it very difficult to trace cybercriminals whom are always on the run and can carry out their fraudulent activities from the comfort of their rooms or in Hotels via internet modems registered with false identity.

[52]The limitations are ₦5, 000,000.00 or its equivalent, in the case of an individual and ₦10, 000, 000.00 or its equivalent in the case of a corporate body.

[53]See www.cenbank.org/cashless/ accessed on 28th April, 2014 by 8:00pm.

to someone within or outside Nigeria or to obtain property by false pretence. This may be either through the internet or by physical contact with the victim.

Section 11A (1) of the Act states that any person or entity providing an electronic communication service or remote computing service either by e-mail or any other form shall be required to obtain personal information of their customers.

Section 11A (2) makes it an offence if they fail to obtain their customer's personal data.

Sections 11B (1) (2) and (3) provides that providers of internet services shall be registered with the EFCC and together with GSM service providers provide information on demand to the EFCC. All these are in a bid to trace them or their customers if it is later discovered that they are carrying out fraudulent activities on-line.[54]

3.12 The Money Laundering (Prohibition) Act, 2011

The Money Laundering Act as the name implies, prohibits money laundering. In section 1 of this Act, there are limitations to make or accept cash payments by individuals and corporate bodies. in as much as banking business is mainly carried out through banking institutions in Nigeria, the cashless economy policy and mobile banking services currently propagated by the Central Bank of Nigeria has created loopholes for cybercriminals to exploit and launder money. It is the writer's opinion that by the time these loopholes are discovered, the cybercriminals would have already enriched themselves.[55] Section 3 of the Act stipulates that bankers should identify their

[54]This is as they would have maximized these loopholes to enrich themselves. See Nigeria's Transition to Cashless Economy, Thisday Live, 3rd July, 2013 , http://www.thisdaylive.com/artilcles/nigeria-s- transition -to-cashless-economy/122241 accessed on 30th January, 2014 by 8:00pm.

[55]This is as they would have maximized these loopholes to enrich themselves. See Nigeria's Transition to Cashless Economy, Thisday Live3rd July, 2013, at http://www.thisdaylive.com/articles/nigeria-s-transition-to-cashless-economy/152241 retrieved on 27th December, 2013 by 6:00pm.

customers.[56] The writer observes that 3rd parties whom benefit from electronic or mobile payments through banks are not customers of the bank and consequently, they cannot be identified by the bank. The least the bank can do is to verify that the person initiating the transaction and the transaction itself are not frauds.

The writer observes that in spite of the provisions of this Act and attempts by financial and non-financial institutions to comply with the provisions of the Act, cyberspace and the internet has provided vast opportunities, more than can be imagined and only discovered gradually, for cybercriminals to carry out money laundering activities.

3.13 Challenges of international cooperation in the fight against cybercrime

The writer observes that the following challenges militate against effective fight against cybercrime all around the world today as follows:

3.13.1 Lack of cyber crime specific laws in many nations

Lack of cybercrime specific laws are the motive for cybercriminals to commit cybercrime. Most nations of the world today prohibit punishing of criminals in the absence of specific laws. Lack of cyber crime specific laws has militated against international cooperation in fighting cybercrime.[57]

On this lapse, Marc D. G. et al. in their work titled 'The Emerging Consensus on Criminal Conduct in Cyberspace[58] state as follows:

> Law enforcement officials cannot take action against cyber criminal sunless countries first enact laws which criminalize the activities in which these offenders engage. As the "Love Bug" investigators learned, the existence of such laws is a fundamental prerequisite for investigation as well as for prosecution.

[56]This is also known as the Know you Customer (KYC) policy. The customer provides his personal information and a means of identification. The bank verifies the address of the customer and in some cases, asks individuals within the customer's premises to confirm if they know him.
[57]The EFCC chairman admitted to this fact. See "*EFCC, NBA Back Anti-cybercrime Bill"* at www.thisdaylive.com accessed on 10/3/2015 by 3:42pm.
[58]Ibid, page 7.

It is against this background that the Chairman of the EFCC advocated for the passing into law of the cybercrime bill[59] and it has being passed into law as the Cybercrime Act, 2015.

3.13.2 Lack of adequate provisions on collection and use of electronic evidence

There are no adequate provisions on admissibility of electronically generated evidence in most nations of the world. In spite of the fact that cybercrimes are mainly carried out in cyberspace which is an electronic medium, the laws of Nigeria and most countries are lagging behind by not taking a bold step in making adequate laws on admissibility of electronically generated evidence.[60]

According to Ani, L.[61]

> The Evidence Act has become grossly inadequate to cover the present advancement in technology with the concomitant sophistication employed in the commission of economic and financial crimes. There is a need to reconsider the prohibitive aspects of our laws. The inadequacy of our legislation turns out to be even more serious when we consider the lack of analogy between most cyber crimes and their conventional network.… As Professor Yemi Osibanjo (SAN) observed "one specific problem that have arisen from the use of electronic financial transactions is the manner and procedure for proving the forms of evidence generated by these means or simply proof of such transactions themselves.

It is the writer's opinion that to effectively combat cybercrime the legislature, judiciary and law enforcement agencies have to take steps by utilizing every measure to fight it electronically in cyberspace.[62]

---

[59] Op cit.

[60] The writer's opinion is based on the premise that the commission and investigation of cybercrime takes place in cyber space which is an electronic eco system. Consequently, as the saying goes "when in Rome, you behave like the Romans."

[61] Ani, L.(2011) "*Cyber Crime and National Security: the Role of the Penal and Procedural Law in Law and Security in Nigeria*", Professor Azinge, E., SAN, et al (eds.) (ibid) p. 211.

[62] The writer's opinion is based on the premise that the commission and investigation of cybercrime takes place in cyber space which is an electronic eco system. Consequently, as the saying goes "when in Rome, you behave like the Romans."

3.13.3 Lack of proper training of Law enforcement agencies on investigation of acts or omissions which constitute cybercrimes

To effectively combat cybercrime, there is a need for proper training of investigators and prosecutors on how to investigate acts or omissions which constitute cybercrimes. This affects how they prosecute crimes in law courts.

Lack of proper training of Law enforcement agencies on investigation of acts or omissions which constitute cybercrimes militates against fighting cybercrimes.

The writer observes that most law enforcement officers lack basic computer knowledge; talk more of complex forensic knowledge on cybercrimes.

3.14 An overview of Nigeria's Cybercrime Act, 2015 and its relevance in International cooperation in combating cybercrime[63]

The cybercrime Act (the Act) was a bill sponsored by the Federal Ministry of Justice. The Act is a result of consolidated previous cybercrime bills which were not passed into law. The Act is meant to provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria; ensure the protection of critical national information infrastructure; and promote cyber security and the protection of computer systems and networks, electronic communications; data and computer programs, intellectual property and privacy rights.

The Act is made of 8 parts, 43 sections and a schedule and most of its provisions are similar with the Budapest Convention on Cybercrime. The parts consist of the following:

3.14.1 Part 1 - Object and Application: This part states that the purpose of the Act is to provide a unified legal, institutional, regulatory regime for the prevention, detection, investigation, prosecution and punishment of cybercrimes in Nigeria. The Act ensures the

[63]See pinigeria.org/download/cybercrime accessed on 28th April, 2014 by 9:00pm.

protection of critical national information infrastructure; promote cyber security and protect computer systems and networks, electronic communication systems and intellectual property and data. The object and application of the act are all encompassing as they cover all forms of electronic communication and cyber activity. Communication through global system for mobile communications (GSM) is also protected from cybercriminals by the cybercrime Act, 2015.

3.14.2 Part 2 - Protection of Critical National Information Infrastructure: By this part of the Act, certain national information infrastructure may be categorized critical. This is on the basis that they are deem vital to the national security of Nigeria or the economic and social well being of its citizens. The categorization as critical national information infrastructure is done by the President on the recommendation of the National Security Adviser, by Order published in the Federal Gazette. This may create a lacuna as some important computer networks that require adequate protection from cybercrimes may be left with little or no protection as they may not have been categorized as "critical national information infrastructure".

The writer opines that the nature of cybercrimes or activities of cybercriminal have spiral effect. A single computer network may be attacked but the effect may resound throughout cyberspace. An example of this can be seen in the "love bug" saga which emanated from the Philippines and spread across the world, causing damage worth $10 billion within few hours. Computer networks are inter-dependent on each other and Designation of certain computer systems or networks as critical national information infrastructure may not enhance their protection against cybercrimes as shown in the Budapest Convention. The protection against cybercrimes should be holistic and not based on categorization of systems as "critical."

3.14.3 Part 3 - Offences and Penalties: This part consists of 16 offences.

The offences are in two categories; namely, offences against the confidentiality, integrity and availability of computer data and systems (Unlawful access to a computer, Unlawful interception of communications, unauthorized modification of computer program or data System interference and Misuse of devices) and Computer-related offences (Computer related forgery, Computer related fraud, Identity theft and impersonation, Child pornography and related offences, Cyber stalking, Cyber squatting, Cyber terrorism, Racist and xenophobic offences, Attempt, conspiracy, aiding and abetting.)

3.14.4 Nature and Scope of Offences Constituting Cybercrimes in Nigeria.

1. **Unlawful access to a computer**

This is contained in Section 6 of the Act. It makes comprehensive prohibition against having unlawful access to a computer. It provides appropriate penalties for having access to a computer without authorization or in excess of authorization. "Any Person, who without authorization or in excess of authorization, intentionally accesses in whole or in part, a computer system or network, commits an offence and liable on conviction to imprisonment for a term of 2 years or to a fine of not less than ₦5,000,000.00 or to both imprisonment and fine." Where the offence is committed with the intent of obtaining computer data, securing access to any program, commercial or industrial secrets or confidential information, the punishment shall be imprisonment for a term of 3 years or a fine of not less than ₦7,000,000.00 or to both imprisonment and fine. This section is in line with Article 2 of the Budapest Convention on cybercrime which states that each Party to the convention shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require

that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system. Another measure adopted under the Act to establish criminal offences is Section 36(8) of the Constitution of the Federal Republic of Nigeria which encourages the prohibition of criminal acts.

2. Unlawful interception of communications

This is contained in Section 7 of the Act. Any person, who intentionally and without authorization or in excess of authority, intercepts by technical means, transmissions of non-public computer data, content data or traffic data, including electromagnetic emissions or signals from a computer, computer system or network carrying or emitting signals, to or from a computer, computer system or connected system or network; commits an offence and liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than ₦5,000,000.00 or to both fine and imprisonment.

3. Unauthorized modification of computer data

By Section 8 of the Act, any person who directly or indirectly does an act without authority and with intent to cause an unauthorized modification of any data held in any computer system or network, commits an offence and liable on conviction to imprisonment for a term of not less than3 years or to a fine of not less than ₦7, 000,000.00 or to both fine and imprisonment. Any person who engages in damaging, deletion, deteriorating, alteration, restriction or suppression of data within computer systems or networks, including data transfer from a computer system by any person without authority or in excess of authority, commits an offence and liable on conviction to imprisonment for a term of not less than three years or to a fine of not less than ₦7, 000,000.00 or to both fine and imprisonment. For the purpose of this section, a

modification of any data held in any computer system or network takes place where, by the operation of any function of the computer, computer system or network concerned any:

(i) program or data held in it is altered or erased;

(ii) program or data is added to or removed from any program or data held in it; or

(iii) and act occurs which impairs the normal operation of any computer, computer system or network concerned.

4. System interference

By section 9 of the Act, any person who without authority or in excess of authority, intentionally does an act which causes directly or indirectly the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference in the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose, commits an offence and liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than ₦5, 000,000.00 or to both fine and imprisonment.

5. Misuse of devices

By section 10, any person who unlawfully produces, supplies, adapts, manipulates or procures for use, imports, exports, distributes, offers for sale or otherwise makes available any devices, including a computer program or a component designed or adapted for the purpose of committing an offence under this Act; a computer password, access code or similar data by which the whole or any part of a computer, computer system or network is capable of being accessed for the purpose of committing an offence under this Act, or any device designed primarily to overcome security measures in any computer, computer system or network with the intent that the devices be utilized for the purpose of

violating any provision of this Act, commits an offence and is liable on conviction to imprisonment for a term of not less than three years or a fine of not less than ₦7,000,000.00 or to both imprisonment and fine.

The Act also makes any person who with intent to commit an offence under this Act, has in his possession any devise or program referred to in subsection 1 of this section, commits an offence and shall be liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than ₦5, 000,000.00 or to both fine and imprisonment.

Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any computer or network for any unlawful purpose or gain, commits an offence and shall be liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than ₦5, 000,000.00 or to both fine and imprisonment. Where the offence under subsection (1) of this section results in substantial loss or damage, the offender shall be liable to imprisonment for a term of not less than five years or to a fine of not less than ₦10,000,000.00 or to both fine and imprisonment. Where a person who with intent to commit any offence under this Act uses any automated means or device or any computer program or software to retrieve, collect and store password, access code or any means of gaining access to any program, data or database held in any computer, commits an offence and shall be liable on conviction to imprisonment for a term of not less than five years or to a fine of not less than ₦10, 000,000.00 or to both fine and imprisonment.

6. Computer related forgery

By section 11, any person who knowingly accesses any computer or network and inputs, alters, deletes or suppresses any data resulting in inauthentic data with the intention that such inauthentic data will be considered or acted upon as if it were

authentic or genuine, regardless of whether or not such data is directly readable or intelligible, commits an offence and is liable on conviction to imprisonment for a term of not less than three years or to a fine of not less than ₦7,000,000.00 or to both fine and imprisonment.

7. Computer related fraud

Section 12 stipulates that any person who knowingly and without authority or in excess of authority causes any loss of property to another by altering, erasing, inputting or suppressing any data held in any computer, whether or not for the purpose of conferring any economic benefits for himself or another person, commits an offence and is liable on conviction to imprisonment for a term of not less than three years or to a fine of not less than ₦7, 000,000.00 or to both fine and imprisonment. When a person with intent to defraud sends electronic message to a recipient, where such electronic message materially misrepresents any fact or set of facts upon which reliance the recipient or another person is caused to suffer any damage or loss, commits an offence and shall be liable on conviction to imprisonment for a term of not less than five years or to a fine of not less than ₦ 10,000,000.00 or to both fine and imprisonment.

8. Identity theft and impersonation

By section 13 of the Act, any person who in the course of using a computer, computer system or network; knowingly obtains or possesses another person's or entity's identity information with the intent to deceive or defraud, or fraudulently impersonates another entity or person, living or dead, with intent to either gain advantage for himself or another person, obtain any property or an interest in any property; cause disadvantage to the entity or person being impersonated or another person; or avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice, commits an offence and liable on

conviction to imprisonment for a term of not less than three years or a fine of not less than ₦7,000,000.00 or to both fine and imprisonment.

9. Child pornography and related offences

By section 14 of the Act, any person that involves in pornography using children, involved in any way in pornography where children are used or the distribution of pornographic materials involving children will on conviction be liable to a fine of ₦ 20,000,000.00 or imprisonment or both, or a fine of ₦ 10,000,000.00 or imprisonment or both.

10. Cyber stalking

By section 15 of the Act, any person who by means of a public electronic network persistently sends threats or any message that is grossly offensive or of an indecent, obscene or menacing character or causes any such message or matter to be so sent; or he knows to be false, for the purpose of causing annoyance, inconvenience or needless anxiety to another or causes such a message to be sent; commits an offence under this Act and shall be liable on conviction to a fine of not less than ₦2,000,000.00or imprisonment for a term of not less than one year or to both fine and imprisonment.

11. Cyber squatting

Any person who, intentionally takes or makes use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by any individual, body corporate or belonging to either the Federal, State or Local Governments in Nigeria, on the internet or any other computer network, without authority or right, or for the purpose of interfering with their use by the owner, registrant or legitimate prior user, commits an offence under this Act and is liable on conviction to imprisonment for a term of not less than two years or a fine of not less than ₦5,000,000.00 or to both fine and imprisonment.

12. Cyber terrorism

By section 17 of the Act, Any person that accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and liable on conviction to life imprisonment. For the purposes of this section, "terrorism" shall have the same meaning under the Terrorism (Prevention) Act, 2011, as amended.

13. Racist and xenophobic offences

By section 18 (1) of the Act, "racist and xenophobic material" means any written or printed material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

Any person who distributes or otherwise makes available, any racist and xenophobic material to the public through a computer system or network, threatens, through a computer system or network, with the commission of a criminal offence -

(i) persons for the reason that they belong to a group, distinguished by race, colour, descent, national or ethnic origin, as well as, religion, if used as a pretext for any of these factors, or a group of persons which is distinguished by any of these characteristics; or distributes or otherwise makes available, through a computer system to the public, material which denies, approves or justifies acts constituting genocide or crimes against humanity, as defined under the Rome Statute of the International Criminal Court, 1998; commits an offence and shall be liable on conviction to imprisonment for a term of not less than five years or to a fine of not less than ₦10,000,000.00 or to both fine and imprisonment.

14. Attempt, conspiracy, aiding and abetting

By section 19 of the Act, any person who attempts to commit any offence under this Act; or does any act preparatory to or in furtherance of the commission of an offence under this Act; or abets, aids or conspires to commit any offence under this Act, commits an offence and is liable on conviction to the punishment provided for the principal offence under this Act.

By section 20 of the Act, a body corporate that commits an offence under this Act shall be liable on conviction to a fine of not less than ₦10,000,000.00 and any person who at the time of the commission of the offence was a chief executive officer, director, secretary, manager or other similar officer of the body corporate or was purporting to act in any such capacity shall be liable on conviction to imprisonment for a term of not less than two years or a fine of not less than ₦5,000,000.00 or to both fine and imprisonment.

It is apt to note that the offences stated in the proposed Act are not all encompassing as cybercrimes evolve every day. By Section 36(8) of the 1999 Constitution of Nigeria (supra) no one can be tried for an offence unless the act is criminalized. The writer observes that cybercriminals in Nigeria may likely explore the lacunas in the Act to commit novel cyber offences which are not criminalized under Nigerian law. In essence, there is still a possibility of cybercriminals committing offences and going scot-free. For example, what of the possibility of a cybercriminal committing cyber-murder (by hacking into a computer device and altering the drugs of a patient in a hospital, or by hacking into a computer and tampering with a medical device attached to a sick person.)

Part 4: Duties of Service Providers: By section 42 of the Act, any public or private entity that provides to users of its service the ability to communicate by means of a computer system, electronic communication devices, mobile networks; and any other

entity that processes or stores computer data on behalf of such communication service or users of such service is a service provider. The writer opines that this interpretation is all-encompassing as it covers GSM service providers and providers of electronic services generally involving the transmission of electronic data.

Part 5: Administration and Enforcement: By section 24 of the Act, the Office of the National Security Adviser shall be the co-coordinating body for all security and enforcement agencies under the Act. The Attorney-General of the Federation (in the Act referred to as "Minister") shall be the co-Minister for the effective implementation and administration of the Act and shall strengthen and enhance the existing legal framework to ensure the prosecution of cybercrimes and conformity of Nigeria's cybercrime and cyber security laws and policies with international standards and the African Union Conventions on Cyber security. The Minister is also saddle with the responsibility of conforming to international standards of cooperation in combating cybercrime.

The writer observes that the template for examining international standards for fighting cybercrime is not stated in the proposed Act. Furthermore it makes no reference to the Budapest Convention on cybercrime which today is the only international recognized international standard on cybercrime. Could it be that the Nigerian government never intends to be sign or ratify the Budapest Convention on Cybercrime?

A Cybercrime Advisory Council is also created under this Act. The Cybercrime Advisory Committee shall comprise of a representative each of the following Ministries, Departments and Agencies as follows:

(a) Federal Ministry of Justice;

(b) Federal Ministry of Finance;

(c) Ministry of Foreign Affairs

(d) Federal Ministry of Trade and Investment

(e) Central Bank of Nigeria;

(f) National Security Adviser;

(g) State Security Service;

(h) Nigeria Police Force;

(i) Economic and Financial Crimes Commission,

(j) Independent Corrupt Practices Commission;

(k) Nigerian Intelligence Agency;

(l) Nigerian Civil Defence Corps;

(m) Defence Intelligent Agency;

(n) Military Intelligent Agency;

(o) National Agency for the Prohibition of Traffic in Persons;

(p) Nigerian Customs Service;

(q) Nigerian Immigration Service;

(r) Nigerian Financial Intelligence Agency.

(s) National Space Management Agency

(t) Nigerian Information Technology Development Directorate

(u) Nigerian Communications Commission

The function and powers of the council is to formulate and provide general policy guidelines for the implementation of the provisions of the Act and advice on measures to prevent and combat computer related offences, cybercrimes, threats to national cyberspace and other cyber security related issues. The Council has the power to regulate it proceedings.

Part 6: Search, Arrest and Prosecution: By Section 27 of the Act, any authorized Officer via a warrant of arrest obtain ex-parte from a Judge can conduct a search and

arrest a suspect. An exception when a search or arrest need not be done by a warrant is in cases of urgency.

The Attorney-General of the Federation shall prosecute offences under this Act subject to the provisions of the Constitution of the Federal Republic of Nigeria, 1999.

Part 7: Jurisdiction and International Co-operation: The Federal High Court located in any part of Nigeria regardless of the location where the offence is committed or High Court of Federal Capital Territory shall have jurisdiction to try offences under this Act committed.

The propose Act encourages international co-operation in enhancing the fight against cybercrime. Specifically it encourages mutual assistance in investigating cybercrime or cooperating between Nigeria and other nations in the fight against cybercrime. This may be carried out whether or not any bilateral or multilateral agreements exist between Nigeria and the requested or requesting country.

3.15 Shortcomings of the Cybercrime Act, 2015

The writer observes that Act makes no reference to the Budapest Convention of Cybercrime, in a bid to encourage international cooperation in the fight against cybercrime. Even though cooperation between Nigeria and other countries in the fight against cybercrime is encouraged by the Act whether or not any bilateral or multilateral agreements exist between Nigeria and other countries, hence Nigeria is not signatory to the Budapest convention on Cybercrime, the requirement for international cooperation by the Cybercrime Act, 2015 is not binding on other countries. In essence, other countries are not bound to cooperate with Nigeria or render mutual assistance in any event there is a request for same from the Nigerian government over issues pertaining to Cybercrime. This is in spite of the fact that the Budapest Convention on Cybercrime settles the issue(s)

of international cooperation in the fight against cybercrime as it ensures that member countries co-operate to check-mate activities of cybercriminals when ever and where ever they occur. For instance, in a bid to prosecute a cybercriminal residing in the United States and broadcasting gay materials through the internet in member countries of the Budapest Convention, the cybercriminal can be easily apprehended and prosecuted hence parties to the treaty can readily cooperate to nip activities of cybercriminals in the bud.[64]

The writer opines that in spite of laws made to combat cybercrime by different countries, the Budapest Convention ensures that any nation can request and get mutual assistance in time, on issues of cybercrime.

No commission is set up to tackle new cybercrimes when they are discovered. A commission to make regulations on cybercrime would ensure that whenever a new cybercrime that is not covered by the Cybercrime Act, 2015 is discovered, a regulation would be made to tackle it, rather than going through the rigorous process of lawmaking while the newly discovered cybercrime continues to wreak havoc.

The Budapest Convention on cybercrime and its benefits are discussed in the next chapter.

[64]The writer believes that in the absence of a treaty on cybercrime, it would be difficult for nations to easily cooperate to fight cybercrime. For example, the stance of some countries in the West on the same sex marriage prohibition Act of Nigeria, 2013 would make it difficult for Nigeria to normally cooperate hence the United States of America threatened to sanction Nigeria over its passage if it was not repealed. See www.vanguardngr.com/2014/01/gay-marriage-law-us-threatens-sanction-nigeria/ accessed on 4th April, 2014 by 12:00pm. The writer opines that if most nations are parties to the Budapest Convention, frosty relationship arising due to any reason would be checked when it comes to cooperating to fight a cybercriminal by the nations.

CHAPTER FOUR
RELEVANCE OF THE BUDAPEST CONVENTION ON CYBERCRIME TO NIGERIA AND THE INTERNATIONAL COMMUNITY AND OTHER INTERNATIONAL ATTEMPTS ON FIGHTING CYBERCRIME

4.1 Introduction

The objective of this chapter is to give an overview discuss of pre-Budapest Convention attempts made in the fight against cybercrime by the United Nations, the African Union and the Economic Community of West African States (ECOWAS), the role of the Budapest Convention on cybercrime and international cooperation in the fight against cybercrime and the issues, challenges and prospects of the convention for nations. The chapter also makes comparism between the Budapest Convention on cybercrime and the Cybercrime Act, 2015 of Nigeria and discusses the implementation of the Convention in the United Kingdom.

4.2 International Cooperation in Fighting Cybercrime

Nations around the world are very concerned about cybercrime, a concern shared by many international organizations, including the United Nations, the G-8, the European Union, ECOWAS, African Union and the Council of Europe. Various international and national organizations have recognized the inherently trans-border nature of cybercrime, the ensuing limitations of unilateral approaches, and the need for international harmonization of legal, technical, and other solutions. In particular, the Organization for Economic Co-operation and Development (OECD),[1] the Council of Europe,[2] the European

[1] What is OECD, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, http://www.oecd.org/about/general/index.htm. "The original 20 members of the OECD are located in Western countries of Europe and North America. Next came Japan, Australia, New Zealand and Finland. More recently, Mexico, the Czech Republic, Hungary, Poland, Korea and the Slovak Republic have joined." Membership, http://www.oecd.org/about/general/member-countries.htm.

[2] See, e.g., About the United Nations, United Nations, http://www.un.org/aboutun/index.html (last visited Mar. 11, 2002).

Union,[3]the United Nations, ECOWAS, African Union and Interpol[4]have played leading and important roles in building international awareness and cooperation in this regard. The Organisation for Economic Co-operation and Development has been called a think tank, monitoring agency, rich man's club, an unacademic university. The OECD groups 30 member countries in an organisation that provides governments a setting in which to discuss, develop and perfect economic and social policy. They compare experiences, seek answers to common problems and work to co-ordinate domestic and international policies that increasingly in today's globalised world must form a web of even practice across nations. Their exchanges may lead to agreements to act in a formal way - for example, by establishing legally-binding codes for free flow of capital and services, agreements to crack down on bribery or to end subsidies for shipbuilding. But more often, their discussion makes for better informed work within their own governments on the spectrum of public policy and clarifies the impact of national policies on the international community. And it offers a chance to reflect and exchange perspectives with other countries similar to their own."

The Council of Europe is an intergovernmental organisation which aims:

i. To protect human rights, pluralist democracy and the rule of law;

ii. To promote awareness and encourage the development of Europe's cultural identity and diversity;

[3]"Interpol exists to help create a safer world. Our aim is to provide a unique range of essential services for the law enforcement community to optimise the international effort to combat crime." Vision, Interpol, http://www.interpol.int/Public/Icpo/default.asp (last modified Mar. 11, 2002). One hundred seventy-nine countries are members of Interpol. See Interpol Member States, Interpol, http://www.interpol.int/Public/Icpo/Members/default.asp (last modified Apr. 17, 2002).

[4]See UNITED NATIONS MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER-RELATED CRIME § II(C)(2) - ¶ 117, at 23 (1995), at http://www.uncjin.org/8th.pdf (May 10, 1999), http://www.uncjin.org/Documents/EighthCongress.html.

iii. To seek solutions to problems facing European society (discrimination against minorities, xenophobia, intolerance, environmental protection, human cloning, Aids, drugs, organised crime, etc.);

iv. To help consolidate democratic stability in Europe by backing political, legislative and constitutional reform.

The Council of Europe should not be confused with the European Union. The two organizations are quite distinct. The 15 European Union states, however, are all members of the Council of Europe.

The first comprehensive inquiry into the criminal law problems of computer crime on the international scale was initiated by the OECD. In 1983, a group of experts met and recommended that the OECD take the initiative in trying to achieve the harmonization of European computer crime legislation. From 1983 to 1985, the OECD carried out a study of the possibility of an international application and harmonization of criminal laws to address cybercrime and abuse.[5]The study resulted in the 1986 report titled "Computer-related Crime: Analysis of Legal Policy", which surveyed existing laws and proposals for reform and recommended a minimum list of abuses that countries should consider criminalizing.[6]This list was compiled as a result of a comparative analysis of substantive law around the world and outlined commonly recognized acts, which could constitute a shared basis for the different approaches taken by member states:

The input, alteration, erasure and or suppression of computer data and or computer programs made willfully with the intent to commit an illegal transfer of funds or of another thing of value; (2) The input, alteration, erasure and or suppression of computer data and or computer programs made willfully with the intent to commit a forgery; (3) The input, alteration, erasure and or suppression of computer data and or computer

[5]See ibid at § II(C)(2) - ¶ 117
[6]Ibid.

programs, or other interference with computer systems, made willfully with the intent to hinder the functioning of a computer and or of a telecommunication system; (4) The infringement of the exclusive right of the owner of a protected computer program with the intent to exploit commercially the program and put it on the market; (5) The access to or the interception of a computer and or telecommunication system made knowingly and without the authorization of the person responsible for the system, either by infringement of security measures or for other dishonest or harmful intentions.[7]

From 1985 to 1989, the Select Committee of Experts on Computer related Crime of the Council of Europe discussed the issues raised by cybercrime and drafted Recommendation 89(9), adopted September 13, 1989.[8]Recommendation 89(9) emphasized the importance of an adequate and quick response to cybercrime, the trans-border nature of which requires harmonization of law and practice and improved international legal cooperation.[9]It further emphasized the need for international consensus in criminalizing and addressing certain computer-related offenses.[10]The Recommendation featured a "minimum list" of crimes to be prohibited and prosecuted by international consensus, as well as an "optional list" that describes prominent offenses on which international consensus would be difficult to reach.[11]

[7]See ibid. at § II(C)(2) - ¶ 118. 8. See UNITED NATIONS MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER RELATED CRIME, ibid, note 165, at § II(C)(2) - ¶ 120 at 23-24("The guidelines for national legislatures include a minimum list, which reflects the general consensus of the Committee regarding certain computer-related abuses that should be dealt with by criminal law, as well as an optional list, which describes acts that have already been penalized in some States, but on which an international consensus for criminalization could not be reached"). See id. at § II(C)(2) - ¶ 121, at 24.

[8]Ibid.

[9]Cybercrime was discussed at Eighth UN Congress and at "the accompanying Symposium on thePrevention and Prosecution of Computer Crime, organised by the Foundation for Responsible Computing").

[10]8th U.N. Congress on the Prevention of Crime and the Treatment of Offenders, U.N., U.N. Doc. A/CONF. 144/L.11 (1990).

[11]Ibid at p. 162.

In 1990, the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders addressed the legal problems posed by cybercrime.[12]The Congress produced a resolution calling for Member States to intensify their efforts to combat computer crime by modernizing their national criminal laws and procedures, improving computer security and prevention measures, and promoting the development of a comprehensive international framework of guidelines and standards for preventing, prosecuting, and punishing computer-related crime in the future.[13]Most notably, the resolution called for Member States to intensify their efforts toward the modernization of national criminal laws and procedures, including measures to:

(a) Ensure that existing offences and laws concerning investigative powers and admissibility of evidence in judicial proceedings adequately apply and if necessary, make appropriate changes;

(b) In the absence of laws that adequately apply, create offences and investigative and evidentiary procedures, where necessary, to deal with this novel and sophisticated form of criminal activity;

(c) Provide for the forfeiture or restitution of illegally acquired assets resulting from the commission of computer-related crimes.[14]

In 1990, the Third Committee of the United Nations General Assembly drafted a resolution inviting governments to be guided by the resolutions adopted at the Eighth

[12]Ibid.

[13]Ibid at 163 (quoting Crime Prevention and Criminal Justice Report of the 3d Comm., U.N. GAOR, at 123, U.N. Doc. A/45/756 (1990).

[14]See Org. for Econ. Co-Operation and Dev., Recommendation of the Council Concerning Guidelines for the Security of Info. Systems, at http://www.oecd.org/dsti/sti/it/secur/index.htm (Nov. 26, 1992). accessed on 28th April, 2014 by 4:00pm.

United Nations Congress in "the formulation of appropriate legislation and policy directives."[15]The General Assembly adopted this resolution on December 14, 1990.[16]

In 1992, the Council of the OECD and 24 of its Member countries adopted the Recommendation of the Council Concerning Guidelines for the security of information Systems, intended to provide a foundational information security framework for the public and private sectors.[17]The Guidelines for the Security of Information Systems[hereinafter, "Guidelines"] were annexed to the Recommendation.[18]This framework includes laws, codes of conduct, provisions.[19]The Guidelines focus on the implementation of minimum standards for the security of information systems.[20]In parallel, however, the Guidelines request that Member States establish adequate penal, administrative or other sanctions for misuse of information systems, and develop means for mutual assistance, extradition and other international cooperation in matters of security of information systems.

In 1995 the United Nations Manual on the Prevention and Control of Computer Related Crime was published.[21]The Manual examines the phenomenon of computer crime, substantive criminal law protecting the holder of data and information, substantive criminal law protecting privacy, procedural law, crime prevention in the computer environment, and the need for and avenues to the Steering Committee (SC) was formed to co-ordinate and harmonise the various regional working party initiatives. It is represented

---

[15]See Recommendation of the Council Concerning Guidelines for the Security of info. Systems, supra note 179. technical measures, management and user practices, and public education

[16]Org. for Econ. Co-Operation and Dev., Recommendation of the Council Concerning Guidelines for the Security of Info. Systems, ibid, note 179.

[17]See Ibid.

[18]See U.N. MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER-RELATED CRIME, supra note 165.

[19]Ibid.

[20]See, e.g., SIEBER, supra note 134, at 188-89. In 1981, Interpol held its First Interpol Training Seminar for Investigators of Computer Crime. See, e.g., Schjolberg, ibid, note 164.

[21]See Interpol, Steering Committee for Information Technology Crime, http://www.interpol.int/Public/TechnologyCrime/WorkingParties/Default.asp#steeringCom:

by the Chairperson, Vice-Chairperson and a third member from each regional WP and is co-ordinated by the representative from the General Secretariat. The idea was to streamline the individual efforts of the member countries by avoiding unnecessary duplication and the resultant waste of human and financial resources. The SC has now gone a step further by contacting organisations outside of Interpol and involving them in our initiatives…to date we have thus achieved success most notably with the High Tech Crime Sub-group of the G8, the International Chamber of Commerce, UNAFEI (the United Nations Asia Institute for the Prevention of Crime and the Treatment of Offenders), as well as with several academic institutions international cooperation.[22]

In 1995, Interpol held its first international conference on computer crime.[23]The conference confirmed a high level of concern in the law enforcement community over the propagation of computer crime; Conference participants were especially troubled by the lack of a worldwide mechanism to address such crime effectively and efficiently.[24]

Interpol held subsequent conferences on computer crime in 1995, 1996, 1998 and 2000.Interpol's approach to cybercrime has been to harness the expertise of its members in the field of Information Technology Crime (ITC) through the vehicle of a 'working party' or a group of experts. In this instance, the working party consists of the Heads or experienced members of national computer crime units. These working parties have been designed to reflect regional expertise and exist in Europe, Asia, the Americas and in Africa. All working parties are in different stages of development. The first Interpol working party, the European Working Party on Information Technology Crime, was established in 1990; the other three working parties were established later. Interpol has

[22]See http://www.theregister.co.uk/2011/05/25/uk_ratifies_cybercrime_convention/ accessed on 21st April, 2014 by 4:00pm.
[23]See more at:http://www.information-age.com/technology/security/2089928/uk-gives-%C2%A3100k-to-implement-convention-on-cybercrime#sthash.NY2aiLkt.dpuf accessed on 21st April, 2014 by 4:00pm.
[24]See Council of Europe Convention on Cybercrime (signed 23 Nov. 2001).

also established a Steering Committee for Information Technology Crime, which coordinates and harmonizes the initiatives of the various working parties.

In 1995, the Council of Europe adopted Recommendation No. R (95)13 of the Committee of Ministers to Member states, spelling out the principles that should guide states and their investigating authorities in the field of information technology. The principles cover search and seizure, technical surveillance, obligations to co-operate with the investigating authorities, electronic evidence, use of encryption, research, statistics and training, and international cooperation. The document addresses these issues from the perspectives of investigating both cybercrime and traditional crimes where evidence may be found or transmitted in electronic form.

In 1996 and 1997, the European Commission issued several documents dealing with harmful and illegal content online and with the safe use of the Internet. On April 24, 1997, the European Parliament adopted a resolution on the European Commission's "communication on illegal and harmful content on the Internet, supporting the initiatives undertaken by the Commission and stressing the need for international co-operation in various areas, to be initiated by the Commission."And in April of 1998 the European Commission presented the European Council with a report on computer-related crime for which it had contracted.

In 1997, the Justice and Interior Ministers of the Group of Eight(G8) met in Washington and adopted ten Principles to Combat High-Tech Crime:

I. There must be no safe havens for those who abuse information technologies.

II. Investigation and prosecution of international high-tech crimes must be coordinated among all concerned States, regardless of where harm has occurred.

III. Law enforcement personnel must be trained and equipped to address high-tech crimes.

IV. Legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized.

V. Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.

VI. Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.

VII. Trans border electronic access by law enforcement to publicly available (open source) information does not require authorization from the State where the data resides.

VIII. Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed.

IX. To the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence.

X. Work in this area should be coordinated with the work of other relevant international fora to ensure against duplication of efforts.

The Ministers also adopted the Action Plan to Combat High-Tech Crime in which, among other things, they pledged to "review our legal systems to ensure that they appropriately criminalize abuses of telecommunications and computer systems and to promote the investigation of high-tech crimes."

In 1997, the OECD Directorate for Science, Technology and Industry directed a five-year review of the progress that had been made toward implementing the 1992

Guidelines for the Security of Information Systems, discussed above. The review was conducted by means of a questionnaire issued to OECD Member countries. The review disclosed, among other things, that the responding countries had experienced difficulties in developing laws and procedures relating to information security because of "differences in the various legal systems and how they deal with security matters such as computer crimes."The general consensus was that the Guidelines were still adequate and did not need to be revised.

Also in 1997, the Council of Europe's European Committee on Crime Problems (CDPC) created a new Committee of Experts on Crime in Cyberspace (PC-CY).The Committee of Experts on Crime in Cyberspace was assigned to examine - "in light of Recommendations No. R (89) 9 and No R (95) 13"- the problems "of criminal procedural law connected with information technology" including, inter alia, "cyberspace offences" and "other substantive criminal law issues where a common approach may be necessary for the purposes of international co-operation". The new Committee was also given the task of drafting "a binding legal instrument" dealing with these issues.

In May of 2000, the G8 held a cybercrime conference to discuss "how to jointly crack down on Internet crime."The conference, which brought together "about 300 Judges, Police, Diplomats and Business Leaders from the G8 states - the United States, Japan, Germany, Britain, France, Italy, Canada and Russia, drafted an agenda for a follow-up summit to be held in July. At the July, 2000 summit, the G8 issued a communiqué which declared, in pertinent part, that it would "take a concerted approach to high-tech crime, such as cyber-crime, which could seriously threaten security and confidence in the global information society."The communiqué noted that the G8's approach to these matters was set out in paragraph eight of the Okinawa Charter on Global Information Society:

> International efforts to develop a global information society must be accompanied by co-ordinate action to foster a crime-free and secure cyberspace. We must ensure that effective measures, as set out in the OECD Guidelines for Security of Information Systems, are put in place to fight cyber-crime. G8 co-operation within the framework of the Lyon Group on Transnational Organized Crime will be enhanced. We will further promote dialogue with industry. . . . Urgent security issues such as hacking and viruses also require effective policy responses. We will continue to engage industry and other stakeholders to protect critical information infrastructures.

The G8 also pledged to establish a "Digital Opportunity Taskforce" which would explore how to integrate the efforts of the G8 members into "a broader international approach."The Taskforce held meetings during the late 2000 and early 2001 and submitted a report containing their Proposed Plan of Action to the personal representatives of the G8 leaders in May, 2001.The report did not address cybercrime, but focused instead on the need to overcome the "digital divide."

In June of 2000, an Action Plan prepared by the European Commission and the European Council was adopted by the Feira Summit of the European Council. Among other things, the Action Plan called for the "establishment of a co-ordinate and coherent approach to cybercrime by the end of 2002."A Commission report issued subsequently explained that "an EU legislative instrument approximating substantive criminal law in the field of computer-related crime has been on the EU agenda" since October, 1999.The report noted that the "Commission has followed the work of the Council of Europe on" the Draft Convention on Cyber-Crime discussed above. It also explained that the European Union's planned approximation on substantive cybercrime law "could go further than the Council of Europe Convention, which will represent a minimum of international cooperation", could "be operational within a shorter period of time" and "would bring computer crime within the realms of EU law and introduce EU law enforcement mechanisms."This portion of the report then goes on to announce four measures the European Commission plans to:

1) Introduce a proposal for a Council Framework Decision that will include provisions for the approximation of laws on child pornography on the Internet, laws that go further than the measures contemplated by the Council of Europe's Draft Convention on Cyber-crime;
2) Bring forward a proposal to approximate high tech offenses, notably "hacking and denial of service attacks", which will include standard definitions and "go further than the draft Council of Europe Convention by ensuring that serious cases of hacking and denial of service attacks are punishable by a minimum penalty in all Member States";
3) Examine the scope for action against racism and xenophobia on the Internet with a view to bringing forward a proposal for a Council Framework Decision . . . covering both off-line and on-line racist and xenophobic activity";
4) Consider "how to improve the effectiveness of efforts against the illicit drugs trade on the Internet."

4.3 Continental Cooperation on the Fight against Cybercrime

At the continental level in Africa, the 1st African regional forum on cyber security was held at Yamoussoukro, Cameroun in November, 2008. The aim of this forum was to discuss measures of fighting cybercrime at the continental level and possibly come up with a regional convention on cybercrime.

In October, 2012, the1st African Internet Governance Forum took place in Cairo, Egypt. This forum emphasized that cooperation is important in the fight against cybercrime.

Also, several declarations have been made on issues pertaining cooperation against cybercrime in Africa. They are:

1. The Oliver Tambo Declaration(Ext/CITMC/Min/Decl.(I) Johannesburg, South-Africa, 5 Nov. 2009).
2. The 14th AU Summit of Head of State and government Declaration on "Information and Communication Technologies in Africa: Challenges and Prospects for Development" ([Assembly/AU/11(XIV)], Addis Ababa, Ethiopia, 31 January - 2 February 2010).
3. The Abuja Declaration, CITMC-3([AU/CITMC/MIN/Decl.(III)], Abuja (Nigeria), 03-07 August 2010.
4. The Khartoum Declaration(AU/CITMC-4/MIN/Decl.(IV)Khartoum, the Sudan, 2-6 September 2012.

The first West African Cyber Crime Summit was convened on 30th November, 2011 to 2nd December, 2011 in the Nigeria capital, Abuja. The Summit, organized by the Economic and Financial Crime commission (EFCC) in collaboration with United Nation on Drugs and Crime (UNODC), the Economic Community of West African States (ECOWAS) and Microsoft, focused on the theme, "The Fight against Cybercrime: Towards Innovative and Sustainable Economic Development". Participants from all over the world considered local and international cybercrime strategies and policies with a view to strengthening international cooperation and developing a regional road map that tackles cyber crime and foster economic growth. Over 450 people were in attendance from across the world including Togo, Guinea, Guinea Bissau, Gambia, Ghana, Senegal, Ivory Coast, Niger, Austria, UK, France,

USA, Turkey, South Africa, UAE, Tunisia and Nigeria. Various international and regional organizations were present, including United Nation on Drugs and Crime (UNODC), Council of Europe (CoE), INTERPOL, US Federal Bureau of Investigation, US Federal Trade Commission, US Department of Homeland Security, Economic

Community of West African States (ECOWAS), European Union and FRANCOPOL. The summit focused on how to:

i. Position the fight against cybercrime as a national priority to help the economic development in the region.
ii. Provide a platform to develop capacity building with scalable and sustainable resources.
iii. Strengthen trust by developing partnerships among various stakeholders at the national and international level; government, civil society, academics, industry and international organizations.
iv. Showcase best practices and case studies of partner organization in combating cybercrime.

The writer observes that in spite of these efforts on international cooperation to fight cybercrime, little has been achieved in the fight against cybercrime because many countries do not have cybercrime specific laws.

4.4 An Appraisal of the Budapest Convention on Cybercrime

The Convention on Cybercrime was conceived in Strasbourg, France, with the active participation of the Council of Europe, Canada, Japan, South Africa and the USA. It was developed in 2001 to address several categories of crimes committed via the Internet and other information networks. It is the first - and only treaty on this issue and its primary goal is to:"pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation."

Signatories to the convention must define criminal offenses and sanctions under their domestic laws for four categories of computer- related crimes:

(1) Security breaches such as hacking, illegal data interception and system interferences that compromise network integrity and availability;

(2) Fraud and forgery;

(3) Child pornography; and

(4) Copyright infringements.

The convention also requires signatories to establish domestic procedures for detecting, investigating, and prosecuting computer crimes, as well as collecting electronic evidence of any criminal offense. It also requires that signatories engage in international cooperation "to the widest extent possible."The birth of the Convention on Cybercrime was gleaned from the mutual recognition of a need for "co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies."[25]

After four years and twenty-seven drafts**,** the then forty-one nations Council of Europe adopted the Convention on Cybercrime on November 8, 2001.The Convention was opened for signature in Budapest, on November 23, 2001. Thirty countries signed the Convention (including fournon-members of the Council of Europe which participated in the negotiations: Canada, United States, Japan and South Africa). By January, 2013, 47 Countries have signed and 31 have ratified the Convention on Cybercrime. Its provisions particularly deal with infringements of copyrights, computer-related fraud, child pornography, and violations of network security. Its main objective, set out in the preamble, is to "pursue a common criminal policy aimed at the protection of society against cybercrime especially by adopting appropriate legislation and fostering international co-operation." The Convention is broken up into four main chapters, with each segment consisting of several articles. The first chapter defines the terms commonly

[25]Ibid, p.1

used in cyber technology and may have lead to ambiguity if left undefined. The second chapter outlines the substantive criminal laws and the common legislation all ratifying countries must adopt to prevent these offenses. The second chapter also frames the procedural requirements to which individual States must adhere. The third chapter contains the provisions concerning traditional and computer crime-related mutual assistance as well as extradition rules. It covers traditional mutual assistance in two situations: where no legal basis (treaty, reciprocal legislation, etc.) exists between parties and where such a basis exists. Finally, the fourth chapter contains the final clauses, including articles pertaining to the signing of the Convention, territorial application of the Convention, declarations, amendments, withdrawals, and federalism. The Convention aims principally at harmonizing the domestic criminal substantive law elements of offenses and connected provisions in the area of cyber-crime; providing domestic criminal procedural law powers necessary for the investigation and prosecution of such offenses; as well as other offenses committed by means of a computer system or evidence in relation to which is in electronic form; and, setting up a fast and effective regime of international co-operation. As such, the Convention defines cyber crime offenses such as illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offenses related to child pornography, and offenses related to copyright and neighboring rights. Such is the broad appeal of the Convention. Countries like Argentina, Pakistan, Philippines, Egypt, and Botswana have already drafted parts of their legislation in accordance with the Convention. Although those countries have not yet signed the Convention, they are supporting the harmonization and standardization process intended by the drafters of the Convention.

4.4.1 Benefits and Relevance of the Budapest Convention on Cybercrime to Nigeria and the International Community

The Internet is akin to a gold rush. Like a gold rush, the Internet has brought with it opportunities and millions of new jobs. The Internet also brings with it very real dangers. Although the specific dangers may be different from those associated with a gold rush, a web surfer's exposure to dangers which are new, difficult to police, and difficult to prevent, is very similar. The only significant difference may be that the Internet is a virtual society rather than a tactile one; a virtual society existing only in networks and information packets. However, the harms committed against both individual citizens and businesses are very real. These citizens are extremely vulnerable as criminal activity on the Internet continues to run rampant.

Cybercrimes are not confined within national borders. A criminal armed with a computer and a connection has the capability to victimize people, businesses, and governments anywhere in the world. The criminal can commit violent crimes, participate in international terrorism, sell drugs, commit identity theft, send viruses, distribute child pornography, steal intellectual property and trade secrets, and illegally access private and commercial computer systems. These criminals can hide their tracks by weaving their communications through numerous ISPs. For example, consider a computer hacker in Lagos, Nigeria who disrupts a corporation's communications network in Abuja, Nigeria. Before accessing the corporation's computer, he routes his communication through ISPs in Japan, Italy, and Australia. In such a case, Nigerian law enforcement would need assistance from authorities in Tokyo, Rome and Sydney before discovering that the criminal is right in their own backyard. The benefit of being a party to the cybercrime convention is that it helps countries fight cybercrime in the following ways:

i. The Budapest Convention provides for substantive criminal law measures, including offences against the confidentiality, integrity and availability of

computer data and systems (e.g. illegal access, illegal interception, data interference, system interference, misuse of devices), computer-related offences (e.g. computer-related forgery, computer-related fraud), content-related offences (child pornography), and infringement of copyright and related rights.

ii. The Budapest Convention provides for procedural criminal law measures, including offences against the confidentiality, integrity and availability of computer data and systems (e.g. illegal access, illegal interception, data interference, system interference, misuse of devices), computer-related offences (e.g. computer-related forgery, computer-related fraud), content-related offences (child pornography), and infringement of copyright and related rights. Procedural law, that is, measures for more effective investigations of cybercrime. These include expedited preservation of stored computer data, partial disclosure of traffic data, production orders, search and seizure of stored computer data, real-time collection of traffic data and interception of content data. The procedural measures are to apply to any offence committed by means of a computer system, and to the collection of evidence in general. Conditions and safeguards are intended to prevent the abuse of such powers. International cooperation, including general principles (related to extradition, mutual legal assistance, spontaneous information etc.), and specific measures (expedited preservation of stored computer data, expedited disclosure of preserved computer data, mutual assistance regarding accessing stored computer data, trans-border access to stored computer data, mutual assistance in the real-time collection of traffic data, mutual assistance regarding

interception of content data, and 24/7 points of contact). The Budapest Convention on Cybercrime is thus comprehensive, not only in terms of its substantive law, but in terms of its procedural law. Furthermore, in international cooperation it combines the traditional mutual assistance regime with urgent measures to allow efficient cooperation, and follows the principle of subsidiarity (that is, that existing bi-or multilateral agreements may be used first before resorting to the provisions of the Convention). Full implementation of this treaty will ensure a coherent national approach to legislation on cybercrime, facilitate the gathering of electronic evidence, facilitate the investigation of cyber laundering, cyber terrorism and other serious crime, ensure the harmonisation and compatibility of criminal law provisions on cybercrime with those of other countries.

iii. **The Convention has the advantage of flexibility:** It has been supplemented by an Additional Protocol covering the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS189). Further protocols can be added in the future to address emerging challenges should the need arise.

iv. **The Convention serves as a guideline or model law for the development of national legislation**

The Budapest Convention on cybercrime serves as a guideline or model law for the development of national legislation, even if a country does not actually become a party to this treaty. Model laws, guidelines and handbooks are based on this treaty. However, actual accession to the Convention on Cybercrime creates additional benefits.

v. **It serves as a legal basis for international cooperation in cybercrime cases**

Parties to the Convention can make full use of the provisions of chapter III on international cooperation, ranging from police to judicial cooperation. These provisions are not limited to cybercrime in the narrow sense, but can support cooperation in tackling all crime involving computer systems or electronic evidence. For this reason the Financial Action Task Force, in their newly consolidated 40 Recommendations, encourage accession to the Budapest Convention to facilitate cooperation against money laundering and the financing of terrorism.

vi. **Parties to the Convention participate in the Cybercrime Convention Committee (T-CY)**

This Committee follows the implementation of the Convention and initiates future work related to the Convention, such as the preparation of additional protocols. This means that countries that have not been involved in the drafting of the original treaty would still be involved in the elaboration of future international cybercrime standards, if they become a party. The Convention also serves as a standard of reference for the European Court of Human Rights.

vii. **The treaty is a platform facilitating public-private cooperation in cybercrime investigations**

The Convention has received strong support from the European Union, Interpol, the Asia-Pacific Economic Cooperation, the Organisation of American States and other organisations and initiatives, as well as the private sector. Thus, the Convention on Cybercrime provides a clear and comprehensive solution which has been used by many countries and has proven to function. Some fifty countries covering about one third of

current internet users have ratified, signed or been invited to accede to this treaty. In the majority of countries globally, legal and technical experts make extensive use of it.

4.4.2 Fields of intervention

Experience suggests that capacity building programmes for cybercrime prevention and criminal justice could address the following:

i. Cybercrime policies and strategies

ii. Comprehensive and coherent approaches to cybercrime

iii. Engagement by decision-makers

iv. Synergies and links with cyber security strategies

v. Multi-stakeholder participation

vi. Contributions by donors and cooperation with partners

vii. Human rights and rule of law requirements

viii. Management of implementation, and monitoring and assessment of results and impact.

4.4.3 Technical Assistance in the Fight against Cybercrime under the Budapest Convention of Cybercrime

Agreements, tools and good practices to meet the challenge of cybercrime are already available and can be applied by any country. These include in particular the Budapest Convention. However, there are also other instruments on cybercrime and related matters such as organized crime, the exploitation of children, the terrorist use of the internet, financial investigations, money laundering and the protection of personal data. Numerous tools for law enforcement and judicial training, for public/private cooperation and for international cooperation have been developed. A major capacity building effort to help countries worldwide make use of existing tools, instruments and good practices is the most effective way ahead. A global approach is required to respond

to needs in a pragmatic manner, follow up on expressed commitment by governments, react to incidents, generate or build on momentum in a given country or region, and exploit opportunities to engage in cooperation against cybercrime. The Octopus Conference 2010 and the United Nations Congress on Crime Prevention and Criminal Justice (Salvador, Brazil, April 2010) underlined broad international consensus on the need for technical assistance aimed at strengthening the capacities of States to counter cybercrime.

4.5 Overview of National implementation of the Budapest Convention in the United Kingdom

The Convention entered into force for the United Kingdom on 1st September 2011.[26] Consequently, the convention is now in full force in the United Kingdom. To ensure that its citizens and law enforcement agents are trained to combat cybercrime and for effective implementation of the convention, the UK's Foreign and Commonwealth Office has committed £100,000 to implementing the Council of Europe's Convention on Cybercrime, a set of standardized rules for policing electronic crime. By ratifying the convention, the United Kingdom is obliged to ban activities such as hacking, distributing child pornography and intellectual property theft.[27]

The Foreign Office said that the £100,000 investment would fund workshops and other activities to strengthen legislation, training for law enforcement agencies and judiciary, and promotion of public-private cooperation and international cooperation.

On the implementation of the convention in the United Kingdom, Foreign Secretary William Hague stated as follows:[28]

---

[26] See http://www.theregister.co.uk/2011/05/25/uk_ratifies_cybercrime_convention/ accessed on 21st April, 2014 by 4:00pm.

[27] See more at: http://www.information-age.com/technology/security/2089928/uk-gives-%C2%A3100k-to-implement-convention-on-cybercrime#sthash.NY2aiLkt.dpuf accessed on 21st April, 2014 by 4:00pm.

[28] Ibid.

> At the London Conference on Cyberspace, I made clear that the rapid rise of cybercrime is a growing threat to people across the world and I made clear the need for coordinated response to improve security, enhance cooperation between states and ensure a collective undertaking to address this threat… I am therefore delighted that the UK will be supporting the Council of Europe Global Project on Cybercrime to further implementation of the Budapest Convention on Cybercrime.

Acts in the United Kingdom which reflect provisions of the Budapest convention on cybercrime are the Computer Misuse Act, 1990 (as amended), Protection of Children Act 1978 (as amended) and The Police and Justice Act 2006. By section 1 of the Computer Misuse Act, 1990 (as amended) it is a crime to do any act with the intention to have unauthorized access to computer data and carries a maximum sentence of two years. Section 2 makes it an offence to have unauthorized access with intent to commit or facilitate commission of further offences. The offence carries a maximum punishment of 5 years.

Under the Protection of Children Act 1978 (as amended), in the United Kingdom the taking, making, distribution, showing and possession with a view to distribution of any indecent photograph or pseudo-photograph of a child under 18 is absolutely prohibited and such offences carry a maximum sentence of 10 years imprisonment. Section 160 of the Criminal Justice Act 1988 also makes the simple possession of indecent photographs or pseudo-photographs of children an offence and carries a maximum sentence of 5 years imprisonment. Making, supplying or obtaining articles for use is an offence under section 1 or 3 which carries a maximum sentence of 2 years.

The Police and Justice Act 2006 (which covers broader issues than computer crime alone) included amendments to the Computer Misuse Act. The maximum prison sentence under section 1 of the original Act was increased from six months to two years. Section 3 of the Act (‘unauthorised modification of computer material’) was amended to

read ‘unauthorised acts with intent to impair or with recklessness as to impairing, operation of computer, etc.’ and carries a maximum sentence of ten years.

The Act also added another section, ‘Making, supplying or obtaining articles for use in computer misuse offences’, carrying a maximum sentence of two years. This section states:

1. A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 1 or 3.
2. A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1 or 3.
3. A person is guilty of an offence if he obtains any article with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 1 or 3.
4. In this section “article” includes any program or data held in electronic form.

4.6 General Issues and Challenges in the Fight against Cybercrime

In the fight against cybercrime, several issues and challenges have been encountered. These issues militate against international, continental and national efforts in the fight against cybercrime. The issues are:

4.6.1 Some nations are safe havens for those who abuse information technologies

Some nations of the world are safe havens for those who abuse information technologies. A very good example of this can be seen from the “love bug” virus that emanated from the Philippines and spread all across the world. In early May of 2000, a computer virus known as the "love bug" emerged and spread rapidly around the globe.

According to one report, the virus, which was designed to disseminate itself and to destroy various kinds of files on a victim's computer, "infected at least 270,000 computers in the first hours" after it was released. The "love bug" forced the shutdown of computers at large corporations such as Ford Motor Company and Dow Chemical Company, as well as the computer system at the House of Lords.

After security experts determined that the virus had come from the Philippines, investigators from the Philippines and from the United States set about tracking down the person(s) who created and disseminated it. They were frustrated in this effort by the Philippines' lack of computer crime laws: For one thing, it took days for investigators to obtain a warrant to search the home of their primary suspect; local prosecutors had to comb through Philippines statutes to find laws that might apply to the dissemination of the virus, and then had to persuade a judge to issue a search warrant on the basis of one possibility. For another, when a suspect-Onel de Guzman-was eventually apprehended, there were no laws criminalizing what he had done. The Philippines had no statutes making it a crime to break into a computer system, to disseminate a virus or other harmful software or to use a computer in an attempt to commit theft. Lacking the ability to charge de Guzman with precisely what he had done-e.g., with disseminating a virus-Philippine prosecutors charged him with theft and with violating a statute that covered credit card fraud. Those charges were eventually dropped after the Department of Justice determined that "the credit card law did not apply to computer hacking and that investigators did not present adequate evidence to support the theft charge." The "love you bug" destroyed files and impeded e-mail traffic in more than twenty countries. Some estimated that the virus caused $10 billion in damage, much of that in lost productivity. The episode prompted the Philippines to adopt a cybercrime law that established fines and prison sentences for those hacked into computer systems and/or disseminated viruses or other harmful programs.

The new law could not be applied retroactively against the individual suspect of disseminating the "love bug" virus, so that crime went uncharged.

4.6.2 Investigation and prosecution of international cybercrimes are not coordinated among all concerned States, regardless of where harm has occurred

Cybercrimes differ from terrestrial crimes. They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal."[29]They also pose far greater challenges for law enforcement:

> Effective law enforcement is complicated by the transnational nature of cyberspace. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cyber criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cyber crimes.

One major reason why Investigation and prosecution of international high-tech crimes are not coordinated among all concerned States, regardless of where harm has occurred is because cybercrimes are not criminalized in some nations. Another reason is because most nations are not signatory to treaties on cybercrime, for instance an international treaty like the Budapest Convention. Hence, it is very difficult to investigate and prosecute high-tech crimes among all concerned states as there is no agreement on the prosecution and investigation of cybercrimes between them. (See the "love bug" saga.) For instance, Nigeria is not yet a signatory to the Budapest Convention and this is militating against the investigation and prosecution of international cybercrimes committed within Nigeria or outside Nigeria.

[29]"*Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information*", ibid, note 1.

4.6.3 Law enforcement personnel are not trained and equipped to address cyber crimes

Law enforcement personnel have to be trained and equipped to address cybercrimes.

Real-world crime and cybercrime differ in several ways. These differences make it difficult to apply traditional principles of criminal law and law enforcement to cybercrime.

For real-world crimes, for the criminal to successfully execute the crime, the proximity between him and the victim matters. He has to be very close to the victim before he can execute the crime. In the cyber world, "no Island is an Island"[30]and proximity does not matter.

The perpetrator of a crime has limited scale of carrying out his criminal intent. This is not so for cybercrimes perpetrated via computers. A criminal in the real-world may attack one victim at a time. Cybercriminals have the potential to reach hundreds of thousands of victims within minutes. For example, Thomas and Janice Reedy, based in the United Kingdom provided a gateway to child porn sites. They had 350,000 subscribers across the world, Nigeria inclusive. Cybercriminals are evolving every day and come up with various tactics of luring their victims, while the patterns of real-world criminals is already well known by law enforcement agents.[31]Perpetrators of crimes in the real-world are not faceless. In the cyber world, perpetrators of cybercrimes are mostly anonymous and find it easier to avoid leaving traces. Cybercrimes are committed quickly and more easily concealed. Consequently, cybercriminals can enter and exit a "crime scene" without been identified, without a trace and quickly.

---

[30]McConnell international, ibid.

[31]Brenner S.W. (2000) "*Cybercrime challenges of law enforcement agents*", www.efcon.org accessed on 23/1/13 by 12:52pm, page 30.

4.6.4 Legal systems do not protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized

Legal systems do not protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized. This bothers on the fact that most nations of the world today do not have cybercrime specific laws to protect the confidentiality, integrity and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized.

4.6.5 Legal systems do not permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime

For a cybercrime to be prosecuted, it has to be thoroughly investigated. Investigations of cybercrimes involve the use of sophisticated machines and complex electronic forensic analysis. In the course of investigating a cybercrime, the computer(s) and network(s) involved have to be processed. It takes 80 hours to process one computer, which is only part of prosecuting. By the time a computer is processed, the cybercriminal would have had the opportunity to move to a country that does not recognize the criminalization of conduct in cyberspace. At the end of it all, the investigation been carried out will amount to nothing as the cybercriminal will be nowhere to be found.

4.4.6 Mutual assistance regimes do not ensure the timely gathering and exchange of evidence in cases involving international cyber crime

In the course of investigating a cybercrime, it takes 80 hours to process a single computer.

Article 33(1) of the Budapest Convention provides for mutual assistance in the course of investigating cybercrime. Investigation of crimes ought to be timely, and this applies to cybercrimes. In the Budapest convention, there is no time frame for investigation of cybercrimes in the course of provision of mutual assistance. Article 27 (2) Rather states as follows:“In the event of urgency,” however, “requests for mutual

assistance...may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party,"

A copy of such request will be sent simultaneously to the requested Party's central authority through the central authority of the requesting Party. However, this may take a very long time as there is no time frame within which such an investigation should take place. This poses a problem as any proper investigation is time-bound. Investigation of crime is not *ad-infinitum.* Hence, there is a need to ensure the timely gathering and exchange of evidence in cases involving international cyber crime.

4.6.7 Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions are not developed

There are forensic standards for retrieving and authenticating evidence in real world crimes. These include collecting and tagging evidence recovered from crime scenes. For cyber crime, there are not yet any standards for collecting and tagging electronic evidence.

4.6.8 Information and telecommunications systems are not designed to help prevent and detect network abuse, and do not facilitate the tracing of criminals and the collection of evidence

To be effective, the fight against cybercrime ought to be proactive and not reactive. Emerging model of law enforcement is a shift from law enforcement, primarily reactive model, to a collaborative preventive-reactive model. There is a need for this methodology of fighting cybercrime because prevention of cybercrime prevents the difficulties that are associated with reacting to cybercrime.

4.6.9 Duplication of efforts in international *fora* in the fight against cybercrime

In the fight against cybercrime, there is a need for proper coordination among the international community to avoid duplication of efforts.

CHAPTERFIVE

SUMMARY, CONCLUSION, FINDINGS AND RECOMMENDATIONS

5.1 SUMMARY

Internet is one of the greatest technological advancements of all time and it has tremendous impact on humans. This is because as shown in this work, the internet has brought people in the world closer and has made communication much easier than it ever was. Cybercriminals however, despite the positive effect of the internet have come up with ways of committing cybercrimes through the internet. It is easy to commit crime through the internet due to its virtual and borderless nature, lack of appropriate laws to punish cybercriminals who use the internet for crime, lack of proper training of law enforcement agents to investigate and prosecute cybercrimes and issues of cyber jurisdiction. In the forefront of combating cybercrime in the world today is the Budapest Convention on cybercrime which as at today is the only treaty on cybercrime. The treaty provides for laws against cybercrime and also encourages international cooperation against cybercrime. The treaty can be amended subsequently if the need arises and it serves as a template for cybercrime specific laws to all countries. In this research titled "An Appraisal of the Legal Framework for Combating Cybercrime in International Law" the writer in Chapter one, provided the benefits of this work toinclude the making of adequate cybercrime specific laws fashioned after the Budapest Convention on cybercrime, subject to local circumstances.

The writer argued that this work will be of tremendous importance to Law

Teachers and students, who are interested in carrying out further research in this area. This strong assertion led to the explanation of what cybercrime is and the concepts and terms common with cybercrime in particular and the internet in general as contained in Chapter Two of this work. Most crime Statutes of most nations date back to the pre-

colonial and or pre-internet boom. To simply put, they are archaic. The writer further made it clear that cybercrimes are offences related to advancement in technology and there are no cybercrime specific laws in most nations of the world and cyber jurisdiction is a great challenge in the fight against cybercrime even as technology advances every day. Most existing criminal laws target real-world crimes of stealing, money laundering, murder, advance fee fraud, et cetera. This makes it difficult to tackle acts or omissions which constitute cybercrime among nations.

The writer in Chapter 3 of this research x-rays the most relevant Statutes that would enable Nigeria cooperate effectively in fighting cybercrime among the comity of nations, to reveal their short comings in international cooperation in combating cybercrime.

In view of the above, the writer in Chapter 4 of this research identifies the specific benefits of the Budapest Convention on Cybercrime to parties, so as to weigh the possibilities of attaining the same benefits to nations. This is why comparism is made between the Budapest Convention on Cybercrime and the cybercrime Act, 2015.

5.3 Conclusion

In conclusion, it is apt to note that laws are made *mutatis mutandis* the needs of every society. Hence cybercrime is a challenge faced by all nations in the world today; continuous attempts ought to be made to nip it in the bud depending on the needs of every nation.

5.4 Findings

From the above analysis, the following findings are made:

a. There are no cybercrime specific laws in most Nations and current law of crimes in most nations are outdated

The statute books of most nations and that of Nigeria inclusive are outdated or a compendium of colonial relics, in most ex-British colonies, now, long consigned to the

archives made references to, only for historical purposes. Lack of cybercrime specific laws in Nations are one of the motives for cybercriminals to commit cybercrime.

b. Lack of proper training of Law enforcement agencies on investigation of acts or omissions which constitute cybercrimes and lack of classification methods for cybercrimes in most nations

To effectively combat cybercrime, there is a need for proper training of investigators and prosecutors on how to investigate acts or omissions which constitute cybercrimes. This affects how they prosecute crimes in law courts. Lack of proper training of Law enforcement agencies on investigation of acts or omissions which constitute cybercrimes militates against fighting cybercrimes in most nations. Most law enforcement officers lack basic computer knowledge; talk more of complex forensic knowledge on cybercrimes. Cybercriminals are always perfecting ways of carrying out cybercrimes and with sophistication in technology; they seem to be limitless in their endeavour. On the other hand, law enforcement agencies the world over daily grapple to comprehend cybercrimes committed and how the cybercriminal operates. Though efforts are made to fight real-world money laundering activities, opportunities to launder money through the internet increase every day as cybercriminals are always coming up with new methods of committing these crimes. Consequently, only when proper classification of the fraudulent acts or omissions carried out by criminal minded individuals that law enforcement agents will tackle them head-on. It is also paramount to state that criminalizing these acts carried out by criminal minded individuals would enhance the fight against acts or omissions constituting cybercrimes.

c. Jurisdiction is hard to determine when investigating cybercrimes

The writer observes that the international community battles with the challenge of jurisdiction in issues of cybercrime. Cyberspace is vast and has no limit and cybercriminals utilize this opportunity to commit crimes anywhere in the world, from

anywhere in the world. In essence, cybercrimes are borderless crimes and this makes it hard to resolve issues of jurisdiction when investigating cybercrimes.

d. There is friction among the various local and international law enforcement agencies and private organizations in the cause of investigating an act categorized as a cybercrime under the Budapest Convention. For example, from the omnibus clause in section 7(f) of the EFCC Act, particularly the phrase that "any other law or regulations relating to economic and financial crimes…" the EFCC has unlimited powers to fight cybercrime. This omnibus clause causes friction between the EFCC and other law enforcement agencies or private organizations when the issue of jurisdiction to fight cybercrime comes up.

e. The Cybercrime Act 2015 does not create a commission responsible for making regulations on issues of cybercrime. This has made it difficult to tackle cybercrimes not covered by the Act whenever they are discovered.

f. Human beings are social in nature and there is always a desire to interact socially in every human being. Most people in the world today are gradually becoming individualistic. For instance most people in developed nations have lost family values and hardly interact with their family members and tight work schedules and keeping many jobs to make ends meet have made interaction via social media more convenient. In such a situation as this, it is very easy for people to fall prey to cybercriminals who are always lurking behind a computer screen to perpetuate cybercrimes.

g. Most people today, particularly children who fall prey to pedophiles on the internet are not aware of the dangers of using the internet. Ignorance of the activities of cybercriminals has made many people not use computer antivirus/internet security protection for their computer and their smart phones only fall prey to the plans of cybercriminals and only later realize that they were victims of a cybercriminal.

5.3 Recommendations

From the above assessment and operations of the current legalframework of the criminal jurisprudence the following recommendations are stated below:

a. There is a need for most nations to pass into law a specific cybercrime law. This law should classify cybercrimes as this would make it easier for law enforcement agents to investigate and prosecute cybercrimes.

b. Law enforcement agencies should be properly trained to investigate and prosecute cybercrimes. This might be through workshops or specialized training abroad on cyber forensics.

c. Ratification and domestication of the Budapest convention on cybercrime is paramount. This would enhance international cooperation in the fight against cybercrime and go a long way in resolving issues of jurisdiction when a cybercrime is committed and has to be prosecuted. In fact, ratification and domestication of the convention would further encourage the members of theinternational community to report incidences of cybercrime to the law enforcement agencies, no matter how small any sum of money stolen from them might be. Being that a crime is an offence against the state; the resources to investigate and prosecute any cybercrime need not be from the victim of the cybercrime. Issues of jurisdiction and investigation of cybercrime will be easier if the Budapest convention is ratified and domesticated by nations of the world.

d. There is a need for an over-arching legislation which would clearly specify the duties and boundaries of all the law enforcement agencies in most nations. This legislation should also contain provisions encouraging mutual cooperation among law enforcement agencies and private bodies in the fight against cybercrime.

e. There is a need to create a commission responsible for the implementation of the provisions of the Cybercrime Act, 2015 and to make regulations on issues bothering on cybercrime.

f. In a bid to combat cybercrime, real social interaction and not virtual interaction should be encouraged. Human beings are social in nature and there is always a desire to interact socially in every human being. New practices like online dating should be outlawed and in its place, dating should be encouraged only when the parties involved have met each other physically. This would go a long way in combating cyber crime as most victims of cybercrimes feel prey to cybercriminals who were posing as responsible prospective wives or husbands.

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

BIBLIOGRAPHY

A. TEXTBOOKS

An Annotated Bibliography Prepared by the Federal Research Division, Libraryof Congress under an InteragencyAgreement with the NationalInstituteof Justice, November, 2009

Brenner, S.W. (2000)" *Cybercrime Investigation and Prosecution: the Role of Penal and Procedural Law"*26. University of Dayton Law School, Dayton,unpan1.un.org/../unpan003073.pdf.

Chukkol, K.S. (1988) "*The Law of Crimes in Nigeria"* (2nd edition)Ahmadu Bello University, Zaria.

Glanville Williams (1983) "*The Text Book of Criminal Law*," 2nd ed. Stevens & Sons, London.

Jonathan C. (2006)*"Principles of Cybercrime*"(2nd edition), Cambridge University Press, United Kingdom.

Kristine M.F. et al (2015) *"Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement"*https://www.fas.org/sgp/crs/.../R4257.pdf

Okonkwo, et al (1994) "*Criminal Law in Nigeria*," (2nd edition) Spectrum Law Publication Ltd., Ibadan.

M.T. Ladan (2015) "*Cyberlaw and Policy on Information and Communications Technology in Nigeria and ECOWAS*" ABU Press Ltd., Zaria.

Marc D. G. and Brenner S. (2000)*"The Emerging Consensus on Criminal Conduct in Cyberspace"*ijlit.oxfordjournals.org/…/10/…/139.full. …

United Nations Office on Drugs and Crime Study title *"Comprehensive Study on Cybercrime" (Draft, February 2013)*", www.unodc.org.

B. ARTICLES IN JOURNAL PUBLICATION

Acta Universitatis Danubius Journal, vol. 9, no. 1/2013, pp. 15-37.

Ani, L. (2011) in "*Law and Security in Nigeria", Professor Azinge, E., SAN, et al (eds.)* Nigerian Institute of Advanced Legal Studies Press, Lagos, 2011,pp. 197-234

Azeez N. A. et al (2009) "*Towards Ameliorating Cybercrime And Cybersecurity*" in (IJCSIS) International Journal of Computer Science and Information Security, Vol. 3, No. 1, pp.1-11.

Golak P. S: (2009) "*Jurisdictional Jurisprudence and Cyberspace*' in: Assam University Journal of Science &Technology: Physical Sciences and Technology Vol. 4 Number II, p. 58.

Paust J. (2007) '*Panel:Cybercrimes and the domestication of international criminal law'* 5 *Santa Clara Journal of International Law* 432, 442.

Ribadu N. (2007) "*Cybercrime and Commercial Fraud: A Nigerian Perspective*" a presentation at Modern Law for Global Commerce Congress to celebrate the fortieth annual session of UNCITRAL Vienna.

Soma, J.T et al (1997)'*Transnational extradition for computer crimes: Are new treaties and laws needed?'* 34 Harvard Journal on Legislation 317,324–6.

C. WEBSITES

http://www.bjournal.co.uk/BJASS.aspx accessed on 4/4/13 9:00pm.

online@http://www.interesjournals.org/JRPGD and accessed on 23/5/13 by 7:00pm.

http://go.warwick.ac.uk/jilt/2009_1/chawki**,** retrieved on 8/4/2013.

www.suffolkedu/.../accessed on 12/1/2013 by 9:00pm.

http://www.internetworldstats.com/emarketing.html accessed on 22/1/2014 by 9:10 pm.
www.mcafee.com,p.5 accessed on 22/1/2013 by 8:00pm.

www.unodc.org.

http://www.nap.edu/catalog/12997.htmlaccessed on 28/3/13 by 5:00pm

http://hub.coe.int/what-we-do/rule-of-law/cybercrime

http://www.usatoday.com/life/cyber/tech accessed on 12/6/13 by 8:00pm

www.cybercrimes.net accessed on 23/1/13 by 5:59pm.

www.crs.gov page 4 accessed on 18/1/2013 by 8:00pm.

www.pwc.com/crimesurvey accessed on 12/5/13 by 9:00pm.

www.unodc.org**,** www.11uncongress.org**.** visited on 12/8/13 by 9:00am

www.africa-union.orgvisited o 23/1/14 by 1:00am.

www.EzineArticles.com.2011.

http://conventions.coe.intaccessed on 25/1/13 by 8:00pm.

www.garlik.com/file/cybercrime_report accessed on 12/1/14 by 11:00pm.

ijlit.oxfordjournals.org/content/10, p. 18, accessed on 10/2/13 by 8:00pm

www.saycocorporativo.com/saycoUK/BIJ/journal/Vol3No1/Article_7 accessed on 12/1/14 by 10:00pm.

www.pwc.com/crimesurvey accessed on 23/1/14 by 8:00pm.

Seehttp://www.nap.edu/catalog/12997html accessed on 12/1/14by8:00pm.

unpan1.un.org/../unpan003073.pdf accessed on 12/3/2-13 by 8:00pm.

www.coe.int/cybercrime, Strasbourg,7 December,2012 accessed on 24/5/13 by 9:00pm.

ijlit.oxfordjournals.org/content/10 accessed on 24/5/13 by 9:00pm.

www.mcafee.com accessed on 13/1/14 by 8:00pm.

www.crs.gov accessed on 23/5/13 by 8:00pm.

www.mcconnellinternational.com (2000) accessed on 23/3/13 by 8:00pm.

http://www.cybercrimes.net accessed on 12/2/14 by 8:00pm.

www.itu.int/ITU.D/cyb/ accessed on 12/2/14 by 8:10pm.

www.mcafee .com

http://journal.sapub.org/computer accessed on 12/2/14 by 8:00pm.

www.norton.com

www.unodc.org. accessed on 12/1/14 by 7:00pm.

www.cambridge.org/9780521899253 accessed on 30/1/14by 8:00pm.

http://dictionary.reference.com/browse/Cyberaccessed on 23/9/13 by 5:00pm.

http://en.wikipedia.org/wiki/Law accessed on 23/1/13 by 10:00pm.

http://definitions.uslegal.com/c/cyber-law/-Cyber Law & Legal Definition, 2013 accessed on 23/1/13 by 10:00pm.

http://www.maths.luc.edu/ethics96/papers/sackson.doc. accessed on 12/2/13 by 8:00pm.

http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. accessed on 12/2/13 by 8:00pm.

http://en.wikipedia.org/wiki/CyberspaceCyberspace, 2013, p. 2.

unpan1.un.org/../unpan003073.pdf .accessed on 3/6/13 by 8:00pm.

En.m.wikipedia.org/wiki/personal_jurisdiction_of_international_defendants_in_the_United_States. Visited on 12/1/14 by 3:00am.

www.itu.int/ITU.D/cyb/**,** p. 45.accessed on 19/3/13 by 9:00pm.

See http://www.ebay.com visited on 12/3/14 by 1:00am

konga.com, cheki.com visited on 12/3/14 by 1:10am

nairaland.com, visited on 12/3/14 by 1:15am

jumia.com.ng visited on 12/3/14 by 1:20am

inspiredmotors.com visited on 12/3/14 by 1:34am

http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf accessed on 13/12/13by 8:00pm.

http://www.ftc.gov/bcp/reports/int-auction.pdf.accessed on 13/12/13 by 8:45pm.

http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html;

http://www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20iddidentity%20theft%20paper%2022%20nov%2007.pdf.

http://ireporterstv.co/president-goodluck-jonathan-awards-40-million-contract-t0-israeli company-for-internet-communication-monitoring -in-nigeria/ accessed on 21/1/2014 by 7:00pm

http://mtladan.blogspot.com/accessed on 7/5/14 by 8:00pm.

http://callcenterinfo.tmcnet.com/news/2006/04/14/1573060.html

http://www.efccnigeria.org/index.php?option=com_contact&catid=4&Itemid=3.

Accessed on the 20th April, 2014 by 8:00pm.

www.cybercrimejournal.com16.

See www.nigeriavillagesquare.com/forum/.... accessed on 20th April, 2014 by 8:00am.

www.nfiu.gov.ng/ access on 20th January, 2014, 4:00pm.

ttp://www.scuml.org/userfiles/SCUML%20FINAL%20REGULATORY%20DOCUMENT%5B1%5D.pdf retrieve on5/4/14 by 5:00am.

http://www.nassnig.org/nass2/news.php?id=191**,** retrieved on 10/9/2013

http://www.thisdaylive.com/articles/efcc-nba-back-anti-cyber-crime-bill/139206/ both retrieve on 20th January, 2014.

en.wikipedia.org/wiki/internet_and_terrorism

www.itu.int/ITU.D/cyb/, p. 55. retrieve on 8th November, 2013 by 4:09pm.

www.saycocorporativo.com/saycoUK/BIJ/journal/Vol3No1/Article_7, p.2. retrieve on 8th November, 2013 by 4:00pm.

http://www.balancingact-africa.com/news/en/issue-no-302/computing/nigeria-ranked

third/en#sthash.TdPUGs7Z.dpuf, retrieve on 27th January, 2014 by 8:00pm

http://www.balancingact-africa.com/news/en/issue-no-518/computing/fg-okays establishment#sthash.I0zOlg0r.dpuf. retrieve on 30th December, 2013 by 2:00pm.

http://www.cipaco.org/spip.php?article1272retrieve on 6/2/14 by 8:00pm.

www.cenbank.org/cashless/ accessed on 28th April, 2014 by 8:00pm.

www.thisdaylive.com accessed on 10/3/2015 by 3:42pm.

pinigeria.org/download/cybercrime accessed on 28th April, 2014 by 9:00pm.

www.vanguardngr.com/2014/01/gay-marriage-law-us-threatens-sanction-nigeria/ accessed on 4th April, 2014 by 12:00pm.

http://www.interpol.int/Public/Icpo/Members/default.asp (last modified Apr. 17, 2002).

http://www.uncjin.org/8th.pdf (May 10, 1999),

http://www.uncjin.org/Documents/EighthCongress.html.

http://www.oecd.org/dsti/sti/it/secur/index.htm (Nov. 26, 1992). accessed on 28th April, 2014 by 4:00pm.

http://www.interpol.int/Public/TechnologyCrime/WorkingParties/Default.asp#steeringCom

http://www.theregister.co.uk/2011/05/25/uk_ratifies_cybercrime_convention/ accessed on 21st April, 2014 by 4:00pm

http://www.information-age.com/technology/security/2089928/uk-gives-%C2%A3100k-to-implement-convention-on-cybercrime#sthash.NY2aiLkt.dpuf accessed on 21st April, 2014 by 4:00pm.

http://www.theregister.co.uk/2011/05/25/uk_ratifies_cybercrime_convention/ accessed on 21st April, 2014 by 4:00pm.

http://www.information-age.com/technology/security/2089928/uk-gives-%C2%A3100k-to-implement-convention-on-cybercrime#sthash.NY2aiLkt.dpuf accessed on 21st April, 2014 by 4:00pm.

www.efcon.org accessed on 23/1/13 by 12:52pm, page 30.

http://ssrn.com accessed on 16th March, 2016.