AN APPRAISAL OF THE EFFICACY OF THE LEGAL AND INSTITUTIONAL FRAMEWORKS FOR COMBATING CYBERCRIMES IN NIGERIA

BY

Is'haq ABUBAKAR
PhD/LAW/2663/2009 - 2010

A THESIS SUBMITTED TO THE SCHOOL OF POSTGRADUATE STUDIES, AHMADU BELLO UNIVERSITY, ZARIA IN PARTIAL FULFILLMENT FOR THE AWARD OF THE DEGREE OF DOCTOR OF PHILOSOPHY IN LAW - PhD

DEPARTMENT OF PUBLIC LAW
FACULTY OF LAW
AHMADU BELLO UNIVERSITY,

ZARIA

JANUARY, 2017

DECLARATION

I declare that the work in this Thesis entitled *An Appraisal of the Efficacy of the Legal and Institutional Frameworks for Combating Cybercrimes in Nigeria* has been carried out by me. The information derived from the literature has been duly acknowledged in the text and a list of references provided. To my knowledge no part of this Thesis was previously presented for another degree at this or any other University.

_____ _____

Is'haq ABUBAKAR **Date**

CERTIFICATION

This Thesis entitled *An Appraisal of the Efficacy of the Legal and Institutional Frameworks for Combating Cybercrimes in Nigeria* by Is'haq ABUBAKAR meet the regulations governing the award of the Degree of Doctor of Philosophy in Law (Ph.D) of the Ahmadu Bello University, and is approved for its contribution to knowledge and literary presentation.

_____ _____

Professor K. S. Chukkol Date
Chairman, Supervisory Committee

_____ _____

Dr. B. Babaji Date
Member, Supervisory Committee

_____ _____

Dr. A.I. Bappah Date
Member, Supervisory Committee

_____ _____

Dr. K. M. Danladi Date
Head, Department of Public Law

_____ _____

Professor Kabir Bala Date
Dean, School of Post Graduate Studies

DEDICATION

To Allah (S.W.T) for the bounty of mercies He bestow on me; to my beloved parents, family members and all the people who in one way or the other contributed in seeing through my education to this level.

ACKNOWLEDGEMENTS

My profound gratitude go to the underlisted who have contributed immensely in keeping me on the good side of life during my academic pursuit in Ahmadu Bello University, Zaria. To you all I say thank you very much. With a heart full of gratitude, I acknowledge:

My Supervisors: Professor K. S. Chukkol, Dr. B. Babaji and Dr. A. I. Bappah for their academic, professional and moral counseling and the kind assistance rendered to me. They found time to go through this study notwithstanding their tight schedules and commitments. Thanks for your fatherly and brotherly mentoring.

To my lecturers and senior colleagues: Prof. M. G. Yakubu, Prof. I.N. Sada, Prof. Y. Aboki, Prof. M. T. Ladan, Prof. I J. G. Irokalibe, Prof. B. Y. Ibrahim, Prof. I. A. Aliyu, Prof. S. Idris, Prof. Y. Y. Bambale, Prof. M. N. Jamo, Prof. (Mrs) J. A.M. Audi, Prof. M. B. Uthman, Dr. P. A. Ocheme, Dr. M.B. Dalhatu (late), Dr. F. F. Cho Dr. Y. Dankofa, Dr. A.A. Akume, Dr. M. S. Abubakar, Dr. H. L. Ali, Dr. A. R. Agom, Dr. I. Shehu, Dr. A. M. Madaki, Dr. M. Arsalan, Dr. (Mrs) I. F. Akande, Dr. S. Apinega, Dr. K. M. Danladi, Dr. D. C. John, Dr. I. Abdulkarim, Dr. P. Onuh. Barr. A. S. Ningi, Barr. B. Ibrahim, Dr. U.S. Muhammad, Barr. S.K Musa, Barr. I. Iloba-Aninye, Barr. F. A. Kera, Barr. Zainab Haruna, Barr. Dalhat Idris, Barr. M. T. Jibril, Barr. M. M. Audi, Barr. S. Abdullahi, Barr. S. U. Bebeji, Barr. S. B. Magashi, Barr. A. Mohammed, Barr. D. M. Sani, Barr. H. Bala and Barr. Jamila Shu'aibu, I say thank you very much for your academic drilling and positive support.

My Taekwondo coaches and co-trainees: Coaches Steven T. Ihom (late), Jibril D. Yero, Tony Wakyu, Adamu Buba, Danladi Jigawa and Mas'ud. Captain Akeem Shonibare, Alh. Sani Lawal (Bradee), Yusuf Sirajo, Muhammad Lawal Ibrahim, Dr. Keneth Shenge, Comrade Aminu Barashi, Mohammed G. Garba, Emmanuel Aondonna, Mrs Grace Agada (the only daughter of my mother) and others whose names I could not remember here, I

cannot help but to remember the steadfast support and encouragement you all gave me in the pursuit of my study and Taekwondo carrier.

My family members: my mother, Hadiza (late), Salamatu, Mariya, Ani and Fatima (late), Fatima and my father Alhaji Musa Maiyaki (late), Mal. Salisu (late), Mal. Mazi, Mal. Danjuma, Prof. Aboki, Mal. Abubakar Sabo and all their children and siblings, I say thank you very much for your moral and financial support.

Very special thanks go to Their Lordships, Hon. Justice M. L. Bello, Hon. Justice Balkisu Mohammed and Hon. Justice M. L. Shu'aibu. To my Principal Partner Dr. K. A. Adedokun, my very special brother Mohammad Salisu Mayyaki, Mr. Abdulkarim Chukkol, Barr. J. Bwala, Barr. B. M. Buhari, Barr. Fatsuma Mohammed, Barr. M. S. Abubakar (of the EFCC), Barr. Kasim Balarabe and Late Alhaji Maye (Law Library); may Allah (S.W.T.) continue to bless and guide you all in all your endeavours.

TABLE OF CASES

1. *American Banana Co. vs. United Fruit Co*. (1909) 213 U.S. 347 at 356 - - - - - - - - 62

2. *Dr Abiodun Olusanya vs Eco Bank Plc*, Suit No. KDH/Z/182/2009 (Unreported) - - - - - - - 120

3. *Egbue vs. Araka,* (1996) 2 NWLR (pt 433) 710 - - 179

4. *Fani Kayode vs. FRN*, (2010) 14 NWLR (Pt. 1214) 481 - 180

5. *Federal Polytechnic Ede & Ors vs. Alh. Lukman Ademola Oyebanji* (2012) LPELR-19696 - - - - 181

6. *FRN vs. Churchill Joshua Essien (Alias Michelle Logan)*, Suit No. FHC/KD/73C/2008 (Unreported) - - 101, 103, 155

7. *FRN vs. Emejuru Prince Patrick,* Suit No. FHC/KD/119C/2008 (Unreported) - - - - - - 102, 103, 155

8. *FRN vs. Helen Laoye*, (2007-2011) ECLR 69 - - 96

9. *FRN vs. Imoh Idiong*, Suit No. FHC/KD/107C/2008 (Unreported) - - - - - - - 90

10. *FRN vs. Imonina Kingsley*, Suit No. FHC/KD/91C/2008 (Unreported) - - - - - - - 92

11. *FRN vs. Iriobekhai Jude Collins*, Suit No. FHC/KD/158C/2008 (Unreported) - - - - - - - 103

12. *FRN vs. Maduka Nnamdi Stanley,* Suit No. FHC/KD/112C/2008 (Unreported) - - - - - - - 107

13. *FRN vs. Nnachi Ephraim*, Suit No. FHC/KD/95C/2008 (Unreported) - - - - - - - 105

14. *FRN vs. Nvene*, (2005 – 2010) ECLRI - - - 95, 96, 184

15. *FRN vs. Olasaidi Dare*, Suit No. FHC/KD/68C/2008 (Unreported) 94, 155

16. *FRN vs. Oyekwere Peter Ndigwe*, Suit No. FHC/KD/116C/2008

(Unreported) - - - - - - - 99

17. *FRN vs. Prince Onyechere,* Suit No. FHC/KD/93C/2008
(Unreported) - - - - - - - 104

18. *FRN* vs. *Prince Rapheal Akpiaifo,* Suit No. K/EFCC/03/201
(Unreported) - - - - - - - 87, 164

19. *FRN vs. Usman & 3 Ors,* (2010) ECLR 184 - - - 98

20. *Hartford Fire Insurance Co. vs. California,* (1993) 509 U.S. 704 70

21. *Ibori vs. FRN,* (2009) All FWLR (pt. 487) 159 - - 163

22. *Ijuaka vs. C.O.P* (1976) NSCC 285 - - - - 42

23. *Moore vs. EFCC,* (*2010)* ECLR 312 at 314 - - - 150

24. *Nabore Properties Ltd vs. Peace-cover Nig. Ltd & Ors* (2014)
LPELR 22586 - - - - - - 166

25. *Obikoya vs. Wema Bank* (1989) 1NSCC 113 - - 166

26. *Odiawa vs. FRN,* (2010) ECLR 19 - - - - 89, 92

27. *Oguma vs. Associated Co. Nig. Ltd.* (1998) 1 NSCC 395 - 179

28. *Patrick Jacob Osoba vs. The Queen* (1961) 1 N.L.R., 1 - 63

29. *Patrick Njovens & 3 Ors vs. The State* (1973) N.S.C.C. 257 - 63

30. *R. vs. Tyler* 2 Q B 594 - - - - - 185

31. *R. vs. Gold and Schifreen, (*1988) 2 WLR 984 - - 124

32. *R. vs. Whitely,* (1991) 1993 CAR 25 CA - - - 125

33. *Robins vs. Lower Merion School District,* US Eastern District
of Pennsylvania - - - - - - 132

34. *State of Michigan vs. Dudley,* (2003) 354 SC 514 - - 67

35. *Sunday Okoro vs. A.G. Western Nigeria,* (1966) N.M.L.R 13- 63

36. *Tolliver vs. FRN,* (1969) 1 NMLR 194 SC - - - 179

37. *Trade Bank Plc vs. Chani* (2003) 13 NWLR (Pt. 836) 216 - 181

38. *UBA Plc vs. Sani Abacha,* (2004) 3 NWLR (pt 861) 561 at 543 179

39. *Udeozor vs. FRN*, (2007) 10 QCCR 135 - - - 176

40. *Uma & Ors vs. Effiom & Ors* (2013) LPELR 21407 - 166

41. *United States vs. Albert Gonzalez* 08 CR 10.2.2.3 - - 133

42. *United States vs. Delmark,* 99F.3d.80 (2d Gr.1996) - - 132

43. *United States vs. Kaczowski,* (2000) 114 F. Supp. 2d 143 - 70

44. *United States vs. Morris*, 982 F.2d 504 - - - 132

45. *United States vs. Nosal*, 676 F.3e 854 (9th Cir.2012) - - 133

46. *United States vs. PFC Bradley E. Manning* - - - 133

47. *United States vs. Sablan*, 92F.3d 865 (9th Cir.1996) - - 133

48. *United States vs. Sullivan*, 40 Fed. Appx. 740 (4th Cir.2002) - 133

49. *Yusuf vs. ACB Ltd.* (1976) 1SC 45 - - - - 181

TABLE OF STATUTES

1. *Advance Fee Fraud and Other Fraud Related Offences Act (AFFA 2006)* - - - - 12, 41, 83, 96, 151, 153, 154, 187

2. *Advance Fee Fraud and Other Fraud Related Offences Act,1995* 85

3. *Anti-Fraud Act 2006* - - - - - - 193

4. *Californian Penal Code* - - - - - 129

5. *Companies and Allied Matters Act (CAMA) 2004* - - 109

6. *Computer Fraud and Abuse Act 1986* - - 129, 130, 133, 134

7. *Computer Misuse Act (CMA) 1990* - - 19, 67, 109, 124, 125

8. *Computer Security and Critical Infrastructure Protection Bill 2005* - - - - - - - 110, 187

9. *Copyright Act* Cap. C28 LFN 2004 - - - - 38

10. *Criminal Code Act* Cap. C38 LFN 2004 - - - 33

11. *Criminal Law of Lagos State, 2011* - - - - 109

12. *Cybercrimes (Prohibition, Prevention, etc) Act, 2015* - 117

13. *Cyber Security and Data Protection Agency Bill 2008* - 111, 187

14. *Economic and Financial Crimes Commission Act 2004 Cap. E1 LFN 2004* - - - - - - 12, 25 82

15. *Electronic Communications and Transactions (ECT) Act 2002* 137

16. *Electronic Fraud (Prohibition) Bill 2008* - - - 113, 187

17. *Evidence Act, 2011* - - - - - 100, 179, 180, 181

18. *Extradition Act* Cap. 125 LFN 1990 - - - - 161, 176

19. *Foreign Intelligence Surveillance Act* - - - 135

20. *Forgery and Counterfeiting Act (FCA) 1981* - - - 124

21. *Homeland Security Act 2002* - - - - - 135, 136

22. *Indian Information Technology Act*, 2000 - - - 136, 137

23. *Indian Penal Code 1860* - - - - - 136

24. *Miscellaneous Offences Act 2004* - - - - 95, 188

25. *National Information Technology Development Agency Act 2007* 143

26. *National Security Agencies Act* Cap. N 74 LFN 2004 - 156

27. *Nigerian Communications Act* Cap. N 97 LFN 2004 - 149

28. *Nigerian Cybercrimes Bill, 2005* - - - - 142

29. *Nigerian Cybercrimes Bill, 2013* - - - - 116

30. *Penal Code Act* Cap. P 3 LFN 2004 - - 33, 83, 92, 164, 165

31. *Singapore Computer Misuse Act* - - - - 67

32. *Terrorism (Prevention) Act, 2011* - - - - 84

33. *Terrorism (Prevention) (Amendment) Act, 2013* - 84

34. *Theft Act 1968 and 1978* - - - - 125, 126, 128

35. *UK Fraud Act 2006* - - - - - - 125,129

36. *United Nations Convention against Transnational Organized Crime* - - - - - - - - 62

37. *United Nations Convention for the Suppression of the Financing of Terrorism, 1999* - - - - - - 84

38. *United States Patriot Act, 2001* - - - - 134

39. *West Virginia Computer Crimes and Abuse Act 2004* - 65, 129

40. *Wire Act* - - - - - - - 70

LIST OF ABBREVIATIONS

AFF	-	Advance Fee Fraud
AGF	-	Attorney General of the Federation
AI	-	Artificial Intelligence
ATM	-	Automated Teller Machine
CAMA	-	Companies and Allied Matters Act
CBN	-	Central Bank of Nigeria
CCPU	-	Computer Crime Prosecution Unit
CCTV	-	Closed-Circuit Television
CD	-	Compact Disk
CDS	-	Chief of Defence Staff
CERT	-	Computer Emergency Response Team
CFAA	-	Computer Fraud and Abuse Act
CIA	-	Central Intelligence Agency
CMA	-	Computer Misuse Act
COE	-	Council of Europe
CPU	-	Central Processing Unit
DDOS	-	Distributed Denial of Service
DHQ	-	Defence Headquarters

DIA	-	Defence Intelligence Agency
DID	-	Department for International Development
DOS	-	Denial of Service
DSS	-	Department of State Security
DVD	-	Digital Video Disk
ECOWAS	-	Economic Community of the West African States
ECT	-	Electronic Communications and Transactions Act
EFCC	-	Economic and Financial Crimes Commission
ESW	-	Early Warning System
FATF	-	Financial Action Task Force
FBI	-	Federal Bureau of Investigation
FCA	-	Forgery and Counterfeiting Act
FCT	-	Federal Capital Territory
FEC	-	Federal Executive Council
FHC	-	Federal High Courts
GSM	-	Global System of Mobile Communication
ICT	-	Information and Communication Technology
IDC	-	Institute of Digital Communications
IGCI	-	Interpol Global Complex for Innovations
IGP	-	Inspector General of Police

Interpol	-	International Police
IP	-	Internet Protocol
IPO	-	Investigating Police Office
IRC	-	Internet Relay Chat
ISP	-	Internet Service Provider
IT	-	Information Technology
ITA	-	Information Technology Act
LPOs	-	Local Purchase Orders
MLAT	-	Mutual Legal Assistance Treaties
NAN	-	News Agency of Nigeria
NATO	-	North Atlantic Treaty Organisation
NCC	-	Nigeria Communications Commission
NCS	-	Nigeria Computer Society
NCWG	-	Nigeria Cybercrimes Working Group
NDC	-	National Defence Council
NFIU	-	Nigerian Financial Intelligence Unit
NGOs	-	Non-Governmental Organisations
NIA	-	National Intelligence Agency
NITDA	-	National Information Technology Development Agency
NSA	-	National Security Agency

NTC	-	National Technical Committee
OECD	-	Organisation for Economic Cooperation and Development
OII	-	Object Identifiable Information
ONSA	-	Office of the National Security Adviser
PC	-	Personal Computer
PII	-	Personally Identifiable Information
PIN	-	Personal Identification Number
PPP	-	Public Private Partnership
SMS	-	Short Message Service
SOCA	-	Serious Organised Crime Agency
SSS	-	State Security Service
TCP	-	Transmission Control Protocol
TLD	-	Top Level Domain
UK	-	United Kingdom
UN	-	United Nations
UNCITRAL	-	United Nations Commission on International Trade Law
UNODC	-	United Nations on Drugs and Crime
VSAT	-	Very Small Aperture Terminal
WACCS	-	West African Cybercrimes Summit

ABSTRACT

Advances in Artificial Intelligence are credited to have given the world computers that can defeat people at chess as well as drive cars and manage calendars. However, despite the progress made, scientists are still unable to develop machines that are capable of replacing human beings. Cyberspace, credited to be network of interdependent information technology, infrastructures, telecommunication networks and computer processing system, have provided new opportunities for new crimes to emerge. Cybercrimes are 'new genus of crimes which use computers for criminal activities. They are crimes committed by means of a special knowledge of computer technology.' Cybercrimes became a source of concern with the proliferation of computer technology in Nigeria. Some youths in Nigeria have used the new communication channels for crimes and they are noted to be sending fraudulent proposals to people and organizations, the world over. The youths have succeeded in carving for Nigeria negative names and appellations among nations, with global anti-crime bodies such as the International Police (Interpol) and Financial Action Task Force (FATF) blacklisting Nigeria as one of the most crime vulnerable countries in the World. Nigeria has in place legal regimes and institutional measures for combating cybercrimes. The aim of this study is to examine the legal regimes and institutional measures adopted by the Nigerian Government in combating cyber and computer related crimes with the view to determine their efficacy or otherwise. To achieve this, the study relied on information such as books, journals, conference papers, newspapers and internet materials. The findings revealed the inadequacy of the legislative measures to combat the various cyber specific offences; some of the legislation were enacted to provide for offences of cheating, obtaining property by false pretences, fraud and related offences and did not envisage the circumstances where such offences could assume the sophistication and extra-territoriality they are presently. These shortcomings, coupled with the dearth of trained personnel with the technical skills, knowhow and resources to investigate and prosecute offenders, created additional challenges to the enforcement institutions established to combat the crimes. Equally, the pre-May, 2015 state of Nigerian cyber related legislation exhibited lack of political will on the part of the Nigerian Government to combat the scourge of cybercrimes as it took the Nigerian Government ten years to enact the Nigerian Cybercrimes Act 2015. Besides, the increasing incidence of crimes and cybercrimes in particular cannot be divorced from the high rate of corruption, unemployment and extreme poverty bedeviling the Nigerian society. These societal ills breed criminality in the country. The study recommends the enactment of additional legislation that will reduce cybercrimes and criminality and provide adequate security and safety to internet and cyberspace users. It is equally recommended that enforcement institutions be equipped by the Nigerian Government with skills, manpower and technological knowledge required for investigation and prosecution of cybercrimes. Again, effort should be made to reduce the socio-economic injustices that allow crime and criminality to flourish in Nigerian society.

TABLE OF CONTENTS

Title Page - - - - - - - - - i

Declaration - - - - - - - - - ii

Certification - - - - - - - - - iii

Dedication - - - - - - - - - iv

Acknowledgment - - - - - - - - - v

Table of Cases - - - - - - - - - vii

Table of Statutes - - - - - - - - - x

List of Abbreviation - - - - - - - - - xii

Abstract - - - - - - - - - xvi

Table of Content - - - - - - - - - xvii

CHAPTER ONE

GENERAL INTRODUCTION

1.1 Background to the Research - - - - - - 1

1.2 Statement of the Research Problem - - - - - 10

1.3 Aims and Objectives of the Research - - - - 13

1.4 Justification of the Research - - - - - - 13

1.5 Scope of the Research - - - - - - - 13

1.6 Research Methodology - - - - - - 14

1.7 Literature Review - - - - - - 14

1.8 Organizational Layout - - - - - - 24

CHAPTER TWO

CONCEPTUAL CLARIFICATION OF RELEVANT KEY TERMS

2.1 Introduction - - - - - - - 26

2.2 The Concept of Artificial Intelligence (AI) - - - - 26

2.3 The Concept of Cyber Space - - - - - - 28

2.4 The Concept of Crime - - - - - - 32

2.5 The Concept and Nature of Cybercrimes - - - - 35

2.5.1 The Concept and Nature of Criminal Responsibility in Cybercrimes- 40

2.5.2 Motivations for Cybercrimes - - - - - - 43

2.5.3 Classifications/Taxonomies of Cybercrimes - - - - 45

2.5.4 Distinctions between Cybercrimes and Other Traditional Forms of Crimes - - - - - - - - - 58

2.6 The Concept of Cyber Jurisdiction - - - - - 61

2.7 The Concepts of Cyber Law and Cyber Security - - - 70

2.8 Relationship between Cybercrimes, Economy and National Security 72

2.8.1 Cyber Threats against the Private Sector - - - - 72

2.8.2 Cyber Threats to Critical Infrastructure - - - - 73

2.8.3 Intellectual Property Theft and Supply Chain Risks - - 73

2.8.4 Botnets - - - - - - - - 73

2.8.5 The "Not for Profit" Cybercriminals - - - - - 75

2.8.6 Cyber Warfare- - - - - - - - 76

2.8.7 Financial Estimates of Damages - - - - - 77

2.9 Concluding Remarks - - - - - - - 79

CHAPTER THREE

AN APPRAISAL OF THE LEGAL FRAMEWORK FOR COMBATING CYBERCRIMES IN NIGERIA

3.1 Introduction - - - - - - - 82

3.2 Existing Legislation on Cybercrimes in Nigeria - - - 82

3.2.1 The Economic and Financial Crimes Commission Act, 2004 - 82

3.2.2 The Advance Fee Fraud and Other Fraud Related Offences Act, 2006 85

3.2.3 The Criminal Law of Lagos State - - - - - 109

3.3 An Overview of Developments of Legislation for Combating Cybercrimes in Nigeria - - - - - - 110

3.3.1 Computer Security and Critical Infrastructure Protection Bill 2005 - 110

3.3.2 Cyber Security and Data Protection Agency Bill 2008 - - 111

3.3.3 Electronic Fraud (Prohibition) Bill 2008 - - - - 113

3.3.4 Cyber Security Bill 2011 - - - - - - 115

3.3.5 Nigerian Cybercrimes Bill, 2013 - - - - - 116

3.4 Cybercrimes (Prohibition, Prevention, etc) Act, 2015 - - 117

3.5 Nigeria's National Cyber Security Policy and Strategy 2014 - 122

3.6 Selected Municipal Legislation for Combating Cybercrimes- - 124

3.6.1 The United Kingdom Computer Misuse Act, 1990 - - - 124

3.6.2 The United Kingdom Fraud Act, 2006 - - - - 125

3.6.3 The United States Computer Fraud and Abuse Act, 1986 - - 129

3.6.4 The United States Patriot Act, 2001 - - - - - 134

3.6.5 The United States Homeland Security Act, 2002 - - - 135

3.6.6 The Indian Information Technology Act, 2000 - - - 136

3.6.7 The South African Electronic Communications and Transactions Act 137

3.7 Concluding Remarks - - - - - - - 139

CHAPTER FOUR

AN EXAMINATION OF THE EFFICACY OF THE INSTITUTIONAL FRAMEWORK FOR COMBATING CYBERCRIMES IN NIGERIA

4.1 Introduction - - - - - - - 141

4.2 National Institutional Framework for Combating Cybercrimes - 141

4.2.1 Nigeria Cybercrimes Working Group (NCWG) - - - 141

4.2.2 National Information Technology Development Agency (NITDA) - 143

4.2.3 Nigerian Communications Commission (NCC) - - - 149

4.2.4 Economic and Financial Crimes Commission (EFCC) - - 150

4.2.5 Office of the National Security Adviser, Department of State Security and Directorate of Cybersecurity - - - - - 156

4.2.6 Nigeria Police Special Fraud Unit - - - - - 159

4.2.7 Computer Crime Prosecution Unit, Federal Ministry of Justice - 159

4.2.8 The Central Bank of Nigeria - - - - - - 161

4.2.9 The Judiciary - - - - - - - - 162

4.3 International Institutional Collaborations in Combating Cybercrimes 168

4.3.1 International Police (Interpole) - - - - - 169

4.3.2 Financial Action Task Force (FATF) - - - - - 171

4.4 Problems and Challenges of Enforcement - - - - 174

4.4.1 Cyber Jurisdictions - - - - - - - 174

4.4.2 Problems of Investigation - - - - - - 177

4.4.3 Evidential Issues - - - - - - - 178

4.5 Concluding Remarks - - - - - - - 181

CHAPTER FIVE

SUMMARY AND CONCLUSION

5.1 Introduction - - - - - - - 183

5.2 Summary - - - - - - - - 183

5.3 Findings - - - - - - - - 189

5.3.1 The Use of AFFA 2006 to Combat Cybercrimes in Nigeria - - 190

5.3.2 Lack of Judicial Consistency in Terms of Punishment of Cyber Offenders 190

5.3.3 Absence of Political Will on the Part of Nigerian Government at Combating the Menace of Cybercrimes - - - - 190

5.3.4 Dearth of Trained Staff or Personnel with Necessary Technical Skills and Tools for Response to Cyber Attacks - - - - 191

5.3.5 Absence of Public Awareness and Enlightenment on the Ills of Cybercrimes - - - - - - - - 191

5.3.6 Absence of Reliable System for Cooperation between and/or Among the Enforcement Institution within and without the Country - 192

5.3.7 Corruption, Poverty and Unemployment - - - - 192

5.4 Recommendations - - - - - - 192

5.4.1 Legislative Reform - - - - - - - 193

5.4.2 Institutional Reform - - - - - - - 194

5.4.3 Need for Strategic Implementation and Enforcement of the Anti-Cybercrimes Legislation and the Support of the General Public 196

5.4.4 Coalition and Collaborative Approach in Combating Cybercrimes - 196

5.4.5 Role of Press, Civil Societies, Organisations and Workshops - 197

5.5 Conclusion - - - - - - - - 199

BIBLIOGRAPHY - - - - - - - 200

CHAPTER ONE

GENERAL INTRODUCTION

1.1 Background to the Research

Advances in artificial intelligence (AI),[1] are credited to have given the world computers that can beat people at chess,[2] as well as drive cars and manage calendars.[3] But despite the progress, scientists are years away from developing machines that are self aware. It is believed that the resulting technological advancement will eradicate poverty and disease, while on the other hand, it is warned that it could endanger human survival.[4] The quest for Artificial Intelligence is as modern as the frontiers of computer science and as old as antiquity.[5] The concept of a "thinking machine" began as early as 2500BC when the Egyptians looked to talking statutes for mystical advice. Automata, the predecessor of today's robot, date back to ancient Egyptian figurines with movable limbs like those found in Tutankhamen's tomb.[6] It took the invention of the analytical engine of Charles Babbage in 1833 to make artificial intelligence a real possibility. Artificial Intelligence, as both a term and a science was coined 120 years later, after the operational digital computer had its debut. Suddenly, the world was introduced to a true "thinking machine" - one that knew more than its programmers.

---

[1] The term Artificial Intelligence (AI) was first coined by John McCarthy in 1956 when he held the first Academic Conference on the subject, but the journey to understand if machines can truly think is said to began much before that. See Smith, C. *et. al.* (2006) "The History of Artificial Intelligence." Retrieved from http://www.courses.cs.washington.edu/courses... on December 26, 2015 at 12.00am.

[2] Perhaps the best known Type A program is IBM's Deep Blue. In 1997, Deep Blue challenged and defeated the then world chess champion, Gary Kasparov.

[3] Tate, K. (2014) "History of Artificial Intelligence." Retrieved from http://www.livescience.com/...history-of-ai-artificial-intelligence on December 26, 2015 at 12.44am.

[4] *Ibid.*

[5] Haack, S. (nd) "A Brief History of Artificial Intelligence." Retrieved from http://www.atariarchives.org/deli/artificial_intelligence.php on December 26, 2015 at 12.59am.

[6] Tutankhamen, was an Egyptian Pharoah of 18th Dynasty, during the period of Egyptian history known as the New Kingdom. King Tut is mainly known for his intact tomb, discovered in Egypt's Valley of the Kings in 1922. Born in circa 1341BCE, King Tut was the 17th King of the 18th Egyptian Dynasty. The name Tutankhamen means "the living image of Amen." Tutankhamen changed his name to Tutankhamun, which means "the living image of Amun." Haack, S. (nd). *Ibid.*

By the end of the Dartmouth Conference,[7] "thinking machines" and *automata* were looked upon as antiquated technologies. Researchers predicted that within ten years a digital computer will be the world's chess champion and that AI would spark intellectual revolution that unveils in importance the earlier industrial revolution.[8] It is argued that it is possible that a machine can take over the routine functions of human muscles and another can take over the routine uses of human mind.[9] Scientists have long dreamed of autonomous thinking systems that are free of human interference. Despite five decades of research, the intuitive intelligence of human beings seem to be still beyond the capabilities of reasoning machines. Some people deem the invention of a "thinking machine" a dangerous endeavour that is ultimately doomed to failure, the misuse of AI have the potentials to ruin the social, economy and political well being of human beings. It is further argued that there is no ideal replacement for human beings. AI may help alleviate the difficulties faced by man but intelligent machines can never be human.[10] The rise of technology opens a world of opportunities in the realms of communication, education, and industrial science. However, it simultaneously created a new era of corruption: cybercrimes. From professional hacking and virus writing to identity theft and fraud, cyber criminals are rapidly discovering new ways to threaten the internet - so rapidly that it is hard for law enforcement agencies to keep with them.[11]

Historically, the criminal abuse of information technology and the necessarily legal response have been discussed ever since the technology was introduced.[12] Over the last five

[7] Dartmouth Summer Research Project on Artificial Intelligence, attended by John McCarthy, creator of the AI programming language URP and Director of Stanford University Artificial Intelligence Laboratory; Mervin Minsky, leading AI researcher and Professor of Science at M.I.T.; Claude Shammon, Nobel Prize – wining pioneer of information and AI theory. *Ibid.*

[8] *Ibid.*

[9] Shubhendu, S. S. and Vejay, J. (2013) "Applicability of AI in Different Fields of Life." *International Journal of Scientific Engineering and Research (IJSER).* Retrieved from www.ijser.in./archives/... on January 25, 2016 at 8.46pm

[10] *Ibid.*

[11] Tatera, K. (2015) "Using Artificial Intelligence to Take Down Cyber Criminals." Retrieved from http://thescienceexplorer.com/technology/usingartificial_intelligence on December 29, 2015 at 3.25pm

[12] Mamandi, K. and Yari, S. (2014) "A Global Perspective on Cybercrimes." *Humanities and Social Sciences Journal*. Vol. 2, No. 2, pp.33-37. Retrieved from http://article.sciencepublishinggroup.com/pdf/... on March 20, 2016.

decades, various solutions have been implemented at the national and global level. One of the reason why the topic remained challenging is the constant technical development as well as the changing methods and ways in which cybercrimes are committed.[13] Cybercrimes did not spring up as a problem overnight. In the early days of computing and network, computers were million dollar huge mainframes with limited number of users.[14] By that time, average criminal possess neither the necessary hardware nor the technical expertise to benefit from such digital opportunity. In the 1950s, students of Massachusetts Institute of Technology (MIT) established the basis for what would emerge as the hackers of culture.[15] In the 1960s, the introduction of transistor based computer systems which were smaller and less expensive than the vacuum-tube based machines led to an increase in the use of computer technology. At this stage, offences focused on physical damage to computer systems and store data.[16] In 1961, the first hackers' group came about at the MIT. The members of the group used to program for a sheer joy of it, which the original essence of the term hacking. Between the 1960s and early 1970s, hacking became associated with radical movement and took on a negative tone.[17] In the 1970s, the use of computer system and computer data increased further. The first affordable personal computer became available, the Altair 88000. From that moment on, it was possible for individual to buy their own computers and learn how to program. Altair gave birth to hacking as it is known today.[18] The 1970s were characterised by a shift by traditional property crimes against computer systems to new forms of crimes.[19] The recognised new forms of computer crimes include illegal use of computer systems and the manipulation of electronic data. The shift from manual to computer operated transaction led to another new form of computer related fraud ensuring laws of multimillion dollars and

[13] Mamandi, K. and Yari, S. (2014) *Op.cit.,* pp.33-37
[14] Hoscheidt, M. M. and Eichner, E. F. (2014) "Legal and Political Measures to Address Cybercrime." World Summit on the Information Society Forum. UFRGS Model United Nations, p.446. Retrieved from http://www.ufrgs.br.ufrgsmun/2014/files/ws12.pdf on February 16, 2016 at 11.00am
[15] *Ibid.*
[16] For example in Canada, student riot caused a fire that destroyed computer data hosted at the University.
[17] Hoscheidt, M. M. and Eichner, E. F. (2014) *Op.cit.,* p.448
[18] *Ibid.*
[19] *Ibid.*

additional challenges to law enforcement agencies.[20] In 1988, the wakeup call for security occurred. Robert Morris J., a doctoral (PhD) candidate at Cornell University, released the first internet worm over the U.S., infecting thousands of computers and shutting down a large portion of the internet.[21] From that moment on, internet users realised that someone in their midst harboured malicious intent. One of the side effects of the spread of computer systems was an increasing interest in software, resulting in the emergence of the first forms of software piracy and crimes related to patent. Viruses started to appear in the 1990s. The 1990s personal computers became popular and the number of potential targets for criminals increased. For the first time, the target included a broad range of critical infrastructure. The interconnection of the computer systems brought about new types of offences. Networks enabled offenders to enter a computer system without been present at the crime scene. In addition, the possibility of distributing software through networks enable offenders to spread malicious software and computer viruses were discovered. Countries started the process to update their legislation so as to meet the requirement of the changing criminal environment. International organisations also got involved in the process. Organisation for Economic Cooperation and Development (OECD) and the Council of Europe set a study group to analyse the phenomenon and evaluate possibilities for legal responses.[22]

The introduction of graphical interface in the 1990s that was followed by a rapid growth in the number of internet users led to new challenges. Information legally made available in one country was available globally even in countries where the publication of some information was criminalised. Another concern associated with online services is the investigation of transnational crime was the speed of information exchange. The distribution of child pornography moved from physical exchange of books and tapes to online distribution

[20] *Ibid.*
[21] *Ibid.*
[22] *Ibid.*

through websites and internet services.[23] While computer crimes were in general local crimes, the internet turned electronic crimes into transnational crimes. As a result, the global community tackled the issue through the UN General Assembly Resolution 45/121 adopted in 1990 and the manual for the prevention and control of computer related crimes issued in 1994 are just two examples of the preceding decade, new trends in cybercrimes continued to be discovered in the 21st Century.[24] In 1996, a hacker shutdown the Public Access Corporation in New York using a hack attack called "Cancelbit." Over 25,000 news group messages were destroyed and in the same year, the U.S. Department of Justice, the CIA and the Airforce were hacked.[25]

The first decade of the new millennium was dominated by highly sophisticated method of committing crimes, such as phishing and botnet attacks, and the emerging use of technology that is more difficult for law enforcement to handle and investigate, such as Voice Over IP Communication and Cloud Computing. It is not only the methods that changed, but also the impact. As offenders became able to automate attacks, the number of offences increased, countries, regional and global organisations have responded to the growing challenges and giving response to cybercrimes high priority.[26]

Thus, the effect of Information and Communication Technology (ICT) on the world poses benefits for the citizens of the global village.[27] The negative effect of ICT is its misuse for criminal activities. Cybercrimes are crimes committed or facilitated via the internet. They are criminal activities involving computers and networks. They range from fraud to unsolicited e-mails, theft of government or corporate secrets through criminal trespass into

[23] Aaushi, S. and Srinidi, R. (2012) *A – Z of Cybercrimes.* Asian School of Cyber Laws. Retrieved from http://ensaiosjuridicos.files.wordpress.com on January 28, 2016 at 3.47am
[24] *Ibid.*
[25] Hoscheidt, M. M. and Eichner, E. F. (2014) *Op.cit.*, p.450
[26] *Ibid.*, p.36
[27] The impact of computer technology on society has been profound. From simple beginnings in arithmetical calculations, computer technology has produce immense data retrieval systems; systems controlling traffic by land, sea and air; systems indispensable to functioning of industry, banking and commerce. See Smith, J.C. (2002). *Smith & Hogan Criminal Law*. 10th Edition, LexisNexis Butterworths, London, p.723

remote systems around the globe.[28] Cybercrimes are kind of crimes that happen in "cyberspace", that is, they are crimes that happen in the world of computer and internet.[29] Cybercrimes are crimes committed by means of a special knowledge or expert use of computer technology.[30] Cybercrimes became problem with the increase use of computer technology.[31] Since the first reported case of computer abuse, computers have been involved in most types of crimes such as theft, fraud, embezzlement, extortion and espionage.[32]

In Nigeria, internet usage has grown rapidly resulting in the explosion of Internet Service Providers (ISPs) and Internet Access Point.[33] This has several positive impacts on the socio-economic and educational developments in the country. However, the country's image has also suffered as a result of the criminal activities of some Nigerians that have turned the internet into a channel for the perpetration of criminal activities such as the Advance Fee Fraud (AFF).[34] It has been observed that most of the cybercrimes perpetrated in Nigeria are generally targeted at individuals and not necessarily computer systems, hence they require less technical expertise.[35] Thus, the internet criminals or persons with criminal intent have

[28] Cybercrimes National Crime Prevention Council. Retrieved from www.ncpc.org.pdf on April 20, 2016 at 4.15pm

[29] Mamandi, K. and Yari, S. (2014) 'A Global Perspective on Cybercrimes.' *Journal of Humanities and Social Science*. Retrieved from www.sciencepublishingroup.com/jhs.pdf.Vol2.No.2, pp.33-37 on April 20, 2016 at 4.21pm

[30] Safra, J. E. *et al* (1998). *The New Encyclopaedia Britannica.* Vol. 3, 19th Ed. Encyclopaedia Inc. U.S.A., p.507.

[31] *Ibid.*

[32] According to Vatsal, the first recorded cybercrime took place in 1820! It was not surprising because abacus which is thought to be the earliest form of a computer has been around since 3,500BC in India, Japan and China. The modern computer began with the analytical engine of Charles Babbage. In 1820, Joseph Marie Jacquard, a textile manufacturer in France, produced the loom, a device that allowed the repetition of series of steps in the weaving of special fabric. This resulted in the fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. Retrieved from www.cybercrimesplanetindia.net/intro.htm on August 10, 2011 at 8.30pm.

[33] The growth of the internet in Nigeria can be linked with the growth in the telecommunications sector of the country's economy. According to a report tagged: "Trends in Telecommunications Market in Nigeria", Internet users in Nigeria increased from less than half a million in 2002 to about 1.6million in 2003 to 1.8million in 2004, representing increase in penetration rates from 0.3 in 2002 to 1.3 in 2003 to 1.4 in 2004. See Ocholi, D. 'The Internet Revolution.' *Newswatch Magazine.* August 2, 2010, p.50. The Nigerian Communications Commission (NCC) stated that the number of internet users on the Global System for Mobile Telecommunications (GSM) network has increased from 76,322,802 in 2014 to 81,892,840 in January 2015. Retrieved from www.premiumtimesng.com, April 5, 2015 at 2.20pm

[34] Longe, B. O. and Chiemeke, C. S. (2008). 'Crime and Criminality in Nigeria - What Roles are Internet Access Points Playing?' *European Journal of Social Sciences*. Vol. 6, No. 4, pp.132 - 139.

[35] *Ibid.*, p.133.

been given a tool which increase their potential pool of victims and makes them all the harder to trace and apprehend.[36]

The challenge in combating cybercrimes, it is observed, relates to the fact that cybercrimes have been in existence for as long as the cyberspace exist. This, it is submitted explains the absence of preparedness on the part of the Nigerian society to combat them.[37] Many Nigerian youths have used the communication channels for crimes and they are credited to be at the forefront of sending fraudulent financial proposals to people and organisations all over the world. A 2008 Internet Crime Report placed Nigeria as number three on the list of world's top ten online crime spots. It puts the number of Nigerians especially the youths, who engage in cybercrimes at 80% of the total internet users in the country.[38] Criminals involved in advance fee fraud schemes (419) are referred to as "*Yahoo boys*" in Nigeria.[39] The criminals have succeeded in carving for Nigeria negative names and appellations among other nations. When one comes across phrases like "Nigerian Scam" the assumption that crosses the mind is that all or most scam emails originate from Nigeria. What started a few years ago as 'Nigerian cyber mail' had by 2004 acquired a sub-regional character as a 'West African mail', even as Spanish, South African, Australian, British and Canadian 'lottery letters' exploded on the internet. Thus, in no time, a multi-million dollar crime has migrated from the Nigerian geographical space to embrace a wider canvas of the whole sub-region.[40] It is with this wide spread national, regional and global implications of cybercrimes in mind that the 1st West African Cybercrimes Summit (WACCS 2010)[41] was held in Abuja with the following objectives:

---

[36] *Ibid.*
[37] *Ibid.*
[38] See *Newswatch Magazine*. August 2, 2010, p.51.
[39] Sesan, G. *et al* (2013) *Economic Cost of Cybercrime in Nigeria*, Paradigm Initiative in Nigeria. Report for Cyber Stewards Network Project of Citizen Lab, Munk School of Global Affairs, University of Toronto. Retrieved from www.pinigeria.org/download/cybercrimecost.pdf on April 28, 2016 at 11.50pm
[40] Ribadu, N. (2007) 'Cybercrimes and Commercial Fraud: A Nigerian Perspective.' A presentation at the Modern Law for Global Commerce Congress to celebrate 40th Annual Session of UNCITRAL, Vienna, July 9-12. Retrieved from www.unicitral.org/pdf/english/congress/ribadu on February 8, 2011 at 9.01pm.
[41] The 1st West African Cybercrimes Summit (WACCS 2010) was held at Transcorp Hilton Hotel, Abuja between November 30th and December 2nd, 2010. The Summit was attended by more than 450 participants from several countries namely, Togo, Guinea, Guinea Bissau, Gambia, Ghana, Sierra Leone, Senegal, Niger, Ivory

(a) to position the fight against cybercrimes as a national priority to help the economic development of the region;

(b) to provide a platform to develop capacity building with scalable and sustainable solution;

(c) to strengthen trust by developing partnerships among various stakeholders at the national and international level; government, civil society, academics, industry and international organisations: and

(d) showcase and share best practices case studies of partner organisation in combating cybercrimes.

The summit recommended the urgent adoption of legislation on cybercrimes and electronic evidence throughout the Economic Community of the West African States (ECOWAS) member states and the creation of national multi-disciplinary working groups across the sub-region with a view to addressing the multi-faceted aspects of cybercrimes at the national, regional and international levels.[42]

Cybercrime is a fast growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of internet to commit a diverse range of criminal activity that know no borders, either physical or virtual, cause serious harm and pose real threat to victims worldwide.[43] Cybercrimes are responsible for the interruption of normal computer functions and have been known to cause downfall of companies and personal entities.[44] For example, a report indicated that Nigeria is losing about $80 million (₦11.2 billion) yearly to copyright piracy. The report was the findings of a study conducted by Institute of Digital Communications (IDC), a market research and forecasting firm based in South Africa on behalf of Businesses Software Alliance of South Africa.[45] Besides, the Nigerian Ministry of Communication reported that Nigeria is losing about N78 billion to

---

Coast, Mauritania, Australia, UK, France, USA, Turkey, South Africa, UAE, Tunisia and Nigeria. Various international and regional organisations such as United Nations on Drugs and Crime (UNODC), Council of Europe (COE), Interpol, US FBI, ECOWAS. Also represented were business community, the financial sector such as the Central Bank of Nigeria (CBN), VISA, Western Union and IT industry with Microsoft and Sub-urban West Africa. See www.waccs.net. Retrieved on March 4, 2011 at 9.15pm.

[42] See the Communique of the 1st West Africa Cybercrimes Summit. Retrieved from www.waccs.net on March 4, 2011 at 9.15pm.

[43] Retrieved from http://www.interpol.int/crime_area/cybercrime/crime on December 29, 2015 at 3.15am.

[44] Mamandi, K. and Yari, S. (2014) *Op.cit.*, p.33.

[45] see Ayantokun, O. 'Fighting Cybercrimes in Nigeria.' Retrieved from http://www.tribune.com.ng on August10, 2011 at 9.32pm.

activities of cyber criminals who target financial institutions, ministries, departments and agencies.[46]

Again, the Internet Crime Complaint Center in the United States of America received and processed over 200,000 complaints in 2006. More than 86,000 of these complaints were processed and referred to various law enforcement agencies like the International Police (Interpol) and the Federal Bureau of Investigation (FBI). The total alleged dollar losses were more than $194 million.[47] Similarly, in the United States of America, Botnets[48] and other malicious codes operate to assist criminals with identity theft. The Federal Bureau of Investigation estimates that identity theft costs American businesses and consumers $50 billion a year.[49] Cybercrimes are becoming more organised and established as transnational business. High technology online skills are available for rent to variety of customers including nation states, individuals and groups that could represent terrorist groups. For example, in 2007, the North Atlantic Treaty Organization (NATO) and the United States sent computer security experts to Estonia to help that nation recover from cyber-attacks directed against government computer systems, and to analyse the methods used and determine the source of the attacks. [50] The increased use of automated attack tools by cybercriminals is said to overwhelm some current methodologies used for tracking cybercrimes.[51] Thus, the internet and critical infrastructure such as the telecommunications or the electric power grid could

[46] The claim was made by the Nigerian Minister of Communication, Mr. Adebayo Shitu at a workshop for Nigerian Universities in Abuja. The Minister urged universities to breed talents who can design software and programs to check the activities of cyber criminals. See Okeke, C. C. (2016) 'Nigeria loses N78 Billion Yearly to Cybercrimes.' *Daily Trust.* January 16, 2016 at www.dailytrust.com, at 12.17am

[47] Akonobi, J. (2008) "The Effect of Cybercrimes on National Economy." Being a Presentation at the National Conference on Cybercrimes and Cybersecurity. Nicon Luxury Hotel, Abuja, August 18-20.

[48] Botnets or "Bot Networks," are made up of vast numbers of compromised computers that have been infected by malicious code and can be remotely-controlled through commands sent via internet. Hundreds or thousands of these infected computers can operate in concert to disrupt or block internet traffic for targeted victims, harvest information, or distribute spam, viruses, or other malicious code.

[49] Wilson, C. (2008). 'Botnets, Cybercrimes, and Cyber terrorism: Vulnerabilities and Policy Issues for Congress.' Congressional Research Services (C. R. S.) Report for Congress, pp. 10-11.

[50] Nagre, D. and Warade, P. (nd) 'Cyberterrorism, Vulnerabilities and Policy Issues: Facts behind the Myth.' Retrieved from http://www.andrew.cmu.edu/user/dnagre/cyberterrorism on August15, 2011 at 11.53am.

[51] *Ibid.*

possibly attract cyber attacks to extort money or damage the economy to affect national security.[52]

It is in view of the challenges pose by cybercrimes that the Nigerian Defence Headquarters, Abuja asserted that it is putting measures aimed at tackling cybercrimes in the country.[53] However, less than three weeks after the statement issued by the Nigerian Defence Headquarters, the then Chief of Defence Staff (CDS), Air Marshal Oluseyi Petirin claimed that some unknown persons gained unlawful access to the computer systems of Defence Headquarters and that of the Nigerian Navy. The Chief of Defence Staff represented by the Chief of Research and Development,[54] informed the attendance of the World Cyber Security Conference, in Abuja that there was daily increase in high profile hacking incidences against websites of major corporations and institutions around the world including Nigeria's defence and security institutions.[55] From the foregoing, it may not be out of place if it is asserted that cybercrimes represent security threat to Nigeria as a country.

1.2 Statement of the Research Problem

It is earlier noted that the rise of technology opened a world of opportunities in the realms of communication, education and industrial science. However, it simultaneously created a new era of corruption, which is cybercrimes that ranges from professional hacking and virus writing to identity theft and fraud. It is also noted that cyber criminals are rapidly discovering new ways to threaten the internet. Intel Security for instance, estimated that

[52] A newspaper in Nigeria reported the leak on the internet of the staff records of former and current operatives of the State Security Service (SSS) including home address and names of immediate family members along with a message threatening the service operatives. The paper reported that the leaked details contain home addresses, telephone numbers, email addresses, dates of birth, bank account numbers of more than sixty serving and retired personnel including the SSS Director General, Mr. Ita Ekpenyong. However, it was not clear if the information had been hacked from the outside and obtained or taken out by the agency employee or someone with access to the materials. This incidence, one may be inclined to agree that it is a serious security breach to the spy agency and the nation as a whole, more so, that many of the personnel of the SSS have been killed by unknown gun-men in the recent past. *See Daily Trust.* August 31, 2012, pp.1-6

[53] The Chief of Communications, Defence Headquarters (DHQ), Air Vice Marshal Amao claimed that the DHQ will be organising a Cyber Stakeholders Conference between September 17 and 19, 2012 to indentify challenges associated with cyber space, cashless economy, space resource and thereafter proffer solutions to the same. The conference with the theme: "Exploiting the Cyber and Space Resources to Meet Contemporary Security Challenges" was aimed at building on the knowledge and awareness on the latest development in cybercrimes and its threats to national security with a view to developing strategies for containing them. See Bashir, M. 'Military to Combat Cybercrimes.' *Daily Trust.* Wednesday September 19, 2012, p.4

[54] Major General M. K. Amao

[55] See Bashir, M. 'Defence Headquarters Website Hacked.' *Daily Trust.* Wednesday September 19, 2012, p.4.

cybercrimes cost the global economy more than $400 billion annually, possibly even maxing out at $575 billion.[56] The estimate is more than the national income of most countries and governments. To make things more unsettling, over 390,000 malicious programs are released every day in attempts to infiltrate computer networks and steal trade secrets and personal data.[57]

It must be stated here that effective legal regimes and vibrant institutions are important in the fight against crimes generally and cybercrimes in particular. Nigeria is entering the Information and Communication Technology (ICT) age rather late in comparison to the western world. Access to internet and personal computer technologies started evolving in the late 1990's and are witnessing accelerated growth.[58] At the turn of the 21st Century, Nigerian Internet penetration level is reported to have taken a running jump. Whereas the number used to be 5% in 2002 - 2003, it stood at over 30% by the end of 2012 and the growth is poised to increase.[59] With the growth of computer technology in Nigerians' personal and business life, so also is the increase in computer based crimes originating from Nigeria committed by Nigerian citizens around the world.[60] The impact of cybercrimes on Nigeria's image, economy, security and citizenry cannot be overemphasised. The advent of mobile telephony on the Nigerian market played a major role and continued to be a key driver of cyber advancements. The rise of the internet in Nigeria has come with an unintended consequence of global notoriety as a haven of cybercrime.[61] Global anti-crime bodies such as the International Police (Interpol)[62] and Financial Action Task Force (FATF)[63] had listed

[56] Tatera, K. (2015), *Op,cit.,* p.2
[57] *Ibid.*
[58] Oyesanya, F. 'Nigerian Internet 419 on the Loose.' Retrieved from www.nigeriavillagesquare.com/ on September 29, 2010 at 8.11pm.
[59] Sesan, G. *et al* (2013) *Op.cit.,* p.1
[60] Oyesanya, F, *Op.cit.*
[61] Sesan, G. *et al* (2013), *Op.cit.,* p.1
[62] The Interpol was established on 7 September 1923 with headquarters in Vienna, Austria on the initiative of Dr. Johannes Schober, President of the Vienna Police. As at 2011 the Interpol has 673 employees with annual budget of €60 million and 190 member state countries. See http://www.interpol.int/crime-areas/cybercrimes. Accessed on August20, 2011.
[63] FATF is an independent intergovernmental body that develops and promotes policies to protect the global financial system against organised crimes. Recommendations issued by the FATF define criminal justice and regulatory measures to be taken by financial institutions to counter problems of crimes. Since its creation by the

Nigeria as one of the most crime vulnerable countries in the world.[64] Internet crimes activities from Nigeria have socio - economic and political effects on Nigeria. This fact was captured by Ribadu[65] when he noted that:

> Cybercrimes are depressing trade and investor confidence in our economy and to that extent it presents clear danger to our national security and the prosperity of our citizens. Indeed, of all the grand corruption perpetrated daily in our communities, most are of the nature of cybercrimes executed through the agencies of computer and internet fraud, mail scam, insider trading, bribery, insurance fraud, government fraud, tax evasion, financial fraud, securities fraud, credit card fraud, bankruptcy fraud, kickbacks, counterfeiting, laundering, embezzlement, as well as economic and copyright/trade secret theft...The implications for the national economy as well as for international trade are enormous. In Nigeria, between the year 2003 and 2007, we successfully disrupted and blocked transactions worth £300 million, €200 million and $500 million dollars respectively. In the same span we successfully prosecuted 97 cybercrimes specific offences... the larger and broader import is more disturbing. It is leading to erosion of confidence in genuine Nigerian commercial credibility and today many western countries with France taking the lead have moved to deny Nigerian businessmen and women who are legitimates the rewards of commerce. France today requires web camera verification for most online business transaction from Nigeria...

Nigeria has in place legal regimes and institutional measures for combating the menace of cybercrimes. Such legal and institutional regimes include the *Advance Fee Fraud and Other Fraud Related Offences Act (AFFA 2006),* the *Economic and Financial Crimes Commission Act (EFCC Act)*[66] which established the Economic and Financial Crimes Commission and the *Cybercrimes Act*, 2015. It is in this light that the instant research examines the legal regimes and institutional measures put in place in Nigeria with the view to determine the effectiveness or otherwise of the same. To achieve that, the following research questions were framed:

(i) What are the developments of the legislative measures, policy and institutional strategies adopted by the Nigerian Government in combating the scourge of cybercrimes and computer related offences?

1989 G-7 Summit, FATF has ensured that its recommendations are recognised globally as the international standard for anti-financial crimes including money laundering and terrorist financing. See Ladan, M.T. (2010) 'International Legal and Administrative Regimes for Combating Money Laundering and Terrorist Financing.' A paper presented at A-2 Day Workshop on Money Laundering Laws and Regulations. Organised by Lintol Resources Base Ltd., Lagos, March 1-2, pp.17-22.

[64] *Ibid.*

[65] Ribadu, N. (2007) *Op.cit.*

[66] Cap. E1 LFN 2004.

(ii) Are the legal and institutional measures for combating cybercrimes in Nigeria adequate and/or effective having regards to the global best practices?

1.3 Aim and Objectives of the Research

The research aimed at primarily appraising the effectiveness of the legal regimes and institutional frameworks for combating cybercrimes in Nigeria. Specifically, the objectives of this research are:

(a) to examine the nature and development of the legislative and institutional measures adopted by the Nigerian Government in combating the menace of cybercrimes and computer related offences; and

(b) to ascertain the effectiveness or otherwise of the legal and institutional measures for combating cybercrimes in Nigeria in line with the global best practices.

1.4 Justification of the Research

This research is justified in view of the difficulties associated with combating cybercrimes. Nigeria has in existence legal regimes and institutional measures for combating the menace of cybercrimes, hence, the need to examine the efficacy or otherwise of the legislative and institutional frameworks. Besides, there is the need to provide methods of reducing the incidence of cybercrimes in Nigeria. The research will no doubt be beneficial to academics, legal practitioners, judges, legislators, law enforcement agencies and students.

1.5 Scope of the Research

The scope of this research is limited to the development and review of legislative and institutional measures for combating cybercrimes in Nigeria and the analysis of best practices of selected countries on the subject matter of the research. The focus of the research is therefore on such laws as the *EFCC Act, 2004*, the *AFFA, 2006* and the *Cybercrimes Act, 2015,* being the main legislation used for combating cybercrimes in Nigeria. Recourse was made to the municipal laws of countries such as the United Kingdom, the United States of America, India and South Africa that have established some bearing in combating cybercrimes. Besides, the analysis of best practice of municipal laws of the selected countries is done with the view to appreciate the influence and development of such municipal laws on

Nigeria. The choice of the countries is deliberate because of the progress they made on the subject of cybercrimes. The research is basically anchored on criminal law aspect of cybercrimes. However, recourse was made to transnational institutional bodies such as the Interpol, owing to the transnational nature of cybercrimes.

1.6 Research Methodology

The research methodology employed in this work is essentially doctrinal. Thus, reliance was placed on library based sources of primary and secondary authorities. Primary source materials used and generated include relevant national laws and policies, case laws from both within and without Nigeria. Secondary sources materials generated include textbooks and articles in peer review journals. Field visits were carried out for the purpose of securing unreported cases as well as discussion with personnel of the following relevant national institutions such as the Economic and Financial Crimes Commission (EFCC) and the Judiciary. This was undertaken with the view to complement the doctrinal method of research highlighted above. All the materials consulted have been duly acknowledged.

1.7 Literature Review

This research attempted a review of some of the earlier works on the subject of the study with the view to identifying their relevance and possible gaps. The literatures consulted include textbooks, articles in journals, law reports, documents and commentaries made therefrom. Wang and Huang,[67] noted that as far back as the early 1990s, the internet was argued to be a unique medium showing the fastest speed of diffusion in human history. That today, there are very few people whose lives are not affected beneficially and or harmfully by the technology of the internet era. The positive side is the ability to share and exchange information instantaneously has provided benefit in the areas of education, commerce, entertainment and social interaction. On the negative side, it has created increasing opportunities for the commission of crimes - information has enabled potential offenders to

[67] Wang, S. K. and Huang, W. (2011) "Evolutional View of the Types of Identity Thefts and Online Fraud in the Era of Internet." *Internet Journal of Criminology.* Retrieved from www.internetjournalofcriminology.com on April 26, 2016 at 5.12am

commit large scale of crimes with almost no monetary cost and much lesser risk of being caught.[68] Compared with perpetrators of traditional economic crimes such as burglaries and robberies, online fraudsters are relatively free to worry from directly encountering law enforcement and witnesses.[69] The writers examined identity theft with focus on the mechanism of identifying and individual, followed by the definition and typology of the crime. They concluded that cyberspace has become attractive place where suitable targets like personal information increase in value while effective guidance typically fall behind.[70]

To Olayemi,[71] the global information infrastructure creates unlimited opportunities for commercial, social and other human activities which are however increasingly under attack by cyber criminals with increasing number of cost and sophistication at an alarming rate. Olayemi examined the sociological and technological factors that impact cybercrime and cyber security thereby articulate the relevant circumstances and threat of cybercrimes in Nigeria. He approached the issues enforcement agencies and governmental institutions and concluded that at the point of writing, that Nigeria has no existing statute that directly address cybercrimes.

According to Mamandi and Yari,[72] cybercrimes are responsible for the interruption of normal computer functions and have been known to cause the down fall of many companies and personal entities. That cybercrimes are kind of crimes that happen in "cyberspace", that is, in the world of computer and the internet. Cybercrimes have the potential for severe impact on the society because the society is becoming an information society, full of information exchange happening in cyberspace. Cybercrimes are crimes committed on the internet using the computer as either a tool or a targeted victim. Computer can be considered

[68] *Ibid.*
[69] *Ibid.*
[70] *Ibid.,* p.18
[71] Olayemi, O. J. (2014) "A Socio-Technological Analysis of Cybercrime and Cybersecurity in Nigeria." *International Journal of Sociology and Anthropology.* Vol. 6 (3), pp.116-125
[72] Mamandi, K. and Yari, S. (2014) "A Global Perspective on Cybercrimes." *Journal of Humanities and Social Sciences.* Vol. 2, No. 2, pp.33 – 37.

as tool in cybercrimes when the individual is the main target of cybercrime.[73] That cybercrimes, once the domain of disaffected genius teenagers has grown into a sophisticated threat to the open nature of the internet. Cyber criminals like their non virtual traditional criminal counterparts seek opportunity and are attracted to vacuums in law enforcement. The news media is filled with report of debilitating distribution of service attacks, defaced websites and new computer viruses warming their ways through the nations' computers. That there are many other cybercrimes that are made public due to private industries reluctance to publicise its vulnerability and government concern for security.[74]

Babaji,[75] while examining the development of cybercrimes under Nigerian law noted that cybercrimes are new in Nigeria as well as in many parts of the world, for a number of reasons such as the absence of specific legislation or statute proscribing and punishing cybercrimes. That, by its nature, cybercrimes involves the use of cyberspace, internet, computer and other related information technology devices which are not known or understood by many Nigerians. He observed that the existing penal statutes do not have direct and adequate provisions on cybercrimes, though; they may not be totally ignorant of the concept and ideas of cybercrimes. The writer attempted a definition of key concepts such as cyberspace, internet, computer crimes and cybercrimes in addition to drawing distinctions and similarities between cybercrimes and computer crimes. The work, though recent, did not take into account nor referred to decided cases by Nigerian courts.[76] This research attempted to fill the gaps in Babaji's work by making reference to judicial authorities in Nigeria and other parts of the world. The work of Babaji is nonetheless very relevant and useful in the preparation of this study as it touches on some basic points this researcher would dwell on.

[73] *Ibid.*
[74] *Ibid.,* p.34
[75] Babaji, B. "Cybercrimes under Nigerian Law" In: Chukkol, K. S. (2010). *The Law of Crimes in Nigeria*. A.B.U., Press Ltd., Zaria, pp.517 - 523.
[76] The EFCC through its Head of Advance Fee Fraud Unit, Mr. Olaolu Adegbite boasted of securing 220 convictions out of the 460 cases of cyber and computer related crimes in Lagos alone. See Olusola, O. 'Yahoo Plus: The New Face of 419.' *The News Magazine*. July 26, 2010, p.20.

Hassan *et al*,[77] identified causes of cybercrimes in Nigeria to include urbanisation, unemployment, quest for wealth, negative role models, weak implementation of cybercrimes law and inadequate equipped law enforcement agencies.[78] They noted the effect of cybercrimes to include reducing the competitive edge of organisations, time wastage and slow financial growth, deformation of image, slow production time and add to overhead cost. This study accedes completely to the positions taken by Hassan *et al* above.

Bali,[79] Ladan,[80] Ashaolu and Oduwale[81] wrote on cybercrimes and cyber jurisdiction including the taxonomies of cybercrimes. Ashaolu and Oduwale took further steps by briefly discussing specific offences and challenges to prosecuting cybercrimes in Nigeria. Ladan posited that Nigeria is fast becoming a heavy user of the internet for commerce, information and communication, and is spending on the internet. He argued that with the expansion of internet Nigeria begins to experience rising tide of cybercrimes and the global news broadcast terrifying figures and instances of e-mail scams done by Nigerians. This study draws from their work to elucidate further the subject matter of the research.

Ladan[82] examined the effectiveness of legal and enforcement framework in fighting advance fee fraud and money laundering activities. He observed that the various forms of corporate fraud especially computer fraud or electronic fraud have assumed an alarming dimension in the world of financial crime. That advances in computer technology have made it possible for criminals to direct funds electronically away from their rightful owners. Besides, electronic fraud perpetrators came from every educational, geographical, racial, religious, gender and socio-economic backgrounds and they are often trained professionals

[77] Hassan, A. B. *et al* (2012) "Cybercrime in Nigeria: Causes, Effect and the Way Out." *ARPN Journal of Science and Technology*. Vol. 2, No. 7, ISSN 2225-7217.
[78] *Ibid.*, pp.628-629
[79] Bali, O. (2002). *Information Technology and the Law: The Nigerian Perspective*. Legal Digest Publishing, Lagos, pp.8 - 100.
[80] Ladan, M.T. (2003). *Introduction to Jurisprudence: Classical and Islamic.* Faith Printers International, Zaria, pp. 15 - 16.
[81] Ashaolu, D. D. and Oduwale, O. A. (2009). *Policing Cyberspace in Nigeria: A Publication in Honour of Col. Sani Bello (Rtd)*. Life Gate Publishing Co. Ltd., Ibadan.
[82] Ladan, M. T. 'The Effectiveness of Legal and Enforcement Framework in Fighting Advance Fee Fraud and Money Laundering Activities.' A paper presented at the 3rd National Seminar on Economic Crimes, Abuja, June 27 - 29, 2004. Retrieved from www.dawodu.com/Ladan2.htm on August 15, 2011 at 11.06pm.

who are good at stealing money and assets from people. Ladan concluded that advance fee fraud and related crimes cannot be fought by legislation alone. The moral tone of the society must also be raised by all and sundry. That effort should be made to remove the socio-economic injustice and inequities in the society, provision of job opportunities and creation of right atmosphere for genuine business and investment to thrive. Ladan's work emphasised on advance fee fraud and money laundering offences only. However, this work will discuss other species of cybercrimes such as cyber stalking, cyber terrorism, hacking, malicious codes, and child pornography among other offences. Nonetheless, the writer's work is relevant and shall be relied on by this researcher in the course of writing this dissertation.

Tokura,[83] discussed issues of definitional problems of computer crime, world situational and vulnerability of countries, jurisdictional issues, and computer related crimes and challenges of enforcement of law. The emphasis in Tokura's work is on commercial law aspects of cybercrimes instead of public law which is the domain of criminal law. That perhaps explained why he did not discuss specific cybercrime offences but focused on providing proposed lists of computer crimes by Organisation for Economic Co-operation and Development (OECD) and Council of Europe (COE) in chapter two of his work. At no point in the entire work did the writer made reference to the *Advance Fee Fraud Act* which is an important legislation in cyber related crime in Nigeria. At the same time, the writer did not cite a single decision on cybercrimes by Nigerian courts. The present study will address the problems identified in Tokura's work above. This is rather necessary because Tokura's work is the only Post Graduate study conducted in the area of this research known to this researcher.

The authors of *Smith and Hogan* on *Criminal Law*[84] examined the *actus reus* and *mensrea* of the offences of unauthorised access to computer material, unauthorised access

[83] Tokura, S. S. (2008). *The Legal Regime of Cyber Security and Crime: Challenges of Enforcement in Nigeria*. LL.M Thesis (Unpublished), Faculty of Law, A.B.U., Zaria.
[84] Smith, J. C. (2002). *Smith and Hogan Criminal Law*. 10th Edition Butterworths LexisNexis, London, pp.725-732.

with intent to commit or facilitate further offences and unauthorised modification of computer material under the *Computer Misuse Act*, 1990 of United Kingdom (U.K.). The discussion by Smith, though borders on the offences under the *Computer Misuse Act* of U.K., a foreign legislation will serve as a guide to the writing of this dissertation.

Brill, Baldwin and Munro,[85] in three volume books made a collection of essays and articles on Computer crimes and Encryption Technology, Infrastructure Protection and Management Solutions, Cybercrimes and Security in the United States, Transnational Responses, U.S. Federal and State Legislation, U.S. Federal and State Judicial Decisions and Cybercrimes and Security in Europe amongst others. Although the works do not include cybercrimes experience in Nigeria, they are nonetheless relevant and shall be relied on in the writing of this dissertation.

Ladan,[86] reviewed the Cyberlaw and Policy on Information and Communications Technology (ICT) in Nigeria and ECOWAS. In four chapters, he discussed the concept of cyberlaw, cybercrime, cyber security, information and communications technology and cyber jurisdiction. He further examined the legal and policy responses to ICT, cybercrime in Nigeria and ECOWAS and international and regional initiatives on cybercrimes, cyber security and ICT and by way of conclusion noted the need to develop safeguard mechanisms to counter cybercrime trends as cybercrime goes mobile, social networks and the need to cope with investigation and prosecution challenge in terms of cooperation with service providers or private sector in area of investigation and liability issues.[87] Ladan's work is relevant and pertinent to this research as it touches on cybercrimes, which is the basic theme of this study. However, the book is wider in terms of scope as it discussed both the civil and criminal aspect of cyber law and extends to ECOWAS jurisdiction. This study on the other hand is limited to cybercrimes experience in Nigeria..

[85] Brill, E. A. Baldwin, F. N. and Munro, R. J. (2001). *Cybercrimes and Security*. Oceana Publications Inc., U.S.A., Vols.1, 2 and 3.
[86] Ladan, M.T. (2015). *Cyber Law and Policy on Information and Communications Technology in Nigeria and ECOWAS.* A.B.U. Press Ltd., Zaria.
[87] *Ibid.*, p.487.

Osinbajo,[88] Babaji[89] and Tar[90] examined the problems of proof of computer and other electronically generated evidence in local and international financial transactions, the legal basis for the admissibility of electronic evidence under Nigerian law and computer and electronically generated evidence respectively. Although, the works of the authors were in respect of electronically generated evidence in both civil and criminal proceedings, the emphasis in this study shall be with respect to cyber and computer related crimes.

Mbanaso,[91] Udotai,[92] and Akinsuyi,[93] attempted a discourse on the concepts of internet, cyber space, cyber security, threat landscape, developing cyber security strategy, legal requirements and challenges for cyber security, technical threats and vulnerabilities, computer crime convention, data protection directive, information security laws, crime in interconnected world, legislation and institutional framework challenges. The posited that the increasing dependence on the internet and ICT have impacted on individuals, organisations and governments. It is a defining feature of a modern interconnected and knowledge-based society and economy. The internet has become an open space for the 'good', 'bad' and 'ugly', creating a new virtual world (known as cyberspace - a global domain within the information environment consisting of the interdependent networks of information technology infrastructure) that has dismantled national boundaries and controls. Thus, every traditional illegal activity or crime has its equivalent in the cyberspace. Likewise, every traditional hostile activity is prevalent in the cyberspace. It is argued that there is the need to recognise the real and significant risks posed by inadequate by cyber security and the need to

[88] Osinbajo, Y. (2001). *Cases and Materials on Nigerian Law of Evidence*. Macmillan Publishers, Lagos, pp.270-296; see also Osinbajo, Y. Electronically Generated Evidence. In: Babalola, A. *Law and Practice of Evidence in Nigeria.* Sibon Books Limited, Ibadan, pp 243-273

[89] Babaji, B. (2009). Admissibility of Documentary and Electronic Evidence under Nigerian Law. Ph.D Dissertation (unpublished), Faculty of Law, A.B.U., Zaria, pp.387-476.

[90] Tar, S. (2006) *Law of Evidence in Nigeria: Substantive and Procedural*. Pearl Publishers, Portharcourt, pp. 754-476.

[91] Mbanaso, U. (2011). 'Technical Perspectives on Cyber Security.' Proceedings at Stakeholders' Workshop on Cyber Security Legislation, held on October, 20, at International Conference Centre, Abuja.

[92] Udotai, B. (2011). 'A Legal Overview of the Draft Legislation on Cyber Security.' Proceedings at Stakeholders' Workshop on Cyber Security Legislation, held on October, 20, at International Conference Centre, Abuja.

[93] Akinsuyi, F. F. (2011). 'Cybercrime Legislative Framework.' Proceedings at Stakeholders' Workshop on Cyber Security Legislation, held on October, 20, at International Conference Centre, Abuja.

take full control of a nation's cyberspace for the purpose of protecting and ensuring its continuity because an attack on a nation's cyberspace could significantly disrupt the functioning of government and businesses alike and produce cascading effects far beyond the targeted sector and physical location of the incident. What is needed therefore, is substantive and procedural provisions as well as prosecutorial authority with adequate enforcement powers. The works of the authors are relevant to this research as they relate to the subject of the study, that is cybercrimes.

Oluwo,[94] highlighted the general weakness or inertia of African states in curbing the menace of cybercrimes and particularly draw attention to the inherent limitation and failure in current domestic legal responses to cybercrime. He concluded by making a case for a definition for the notion of sovereignty and its implications for the recurring decimal of cybercrime against African economies and societies. That the unprecedented opportunities the internet provided to criminals to perpetrate their acts revealed that purely domestic solutions are proven inadequate because 'cyberspace' has no geographical boarders and moreso, computer system can be stealthily compromised from any location in the world. Thus, developing a universal model for tackling cybercrimes is especially challenging giving the transnational nature of the ICT. The work is relevant to this study in the areas of regional initiative that would streamline and synergise effort of African state in responding to the phenomenon of cybercrimes.

Akintola *et al*,[95] attempted a contextualisation of the concept of cybercrimes and e-commerce in Nigeria, legal and regulatory framework of e-commerce in Nigeria, jurisdictional choice of law and evidential issues, while Wada and Odulaja,[96] asses cybercrime and its impact on the banking institutions in Nigeria, bearing in mind the policy

[94] Oluwo, D. (2009). 'Cybercrimes and Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa.' *Journal of Information, Law and Technology (JILT).* Retrieved from http://go.warwick.ac.uk/jilt/2009_1oluwo on July 25, 2015 at 10.32am.
[95] Akintola, K. G. *et al* (2011). 'Appraising Nigeria Readiness for E-Commerce Towards Achieving Vision 20: 2020.' Retrieved from www.arpapres.com.../IJRRAS on July 27, 2015 at 10.37am.
[96] Wada, F. and Odulaja, G. O. (2012). 'Assessing Cybercrimes and its Impact on E-Banking in Nigeria Using Social Theories.' *African Journal of Computing and ICT.* Vol. 5, No. 1, pp.69-82. Retrieved from www.ajocict.net/uploads/wada_Odulaja... on July 27, 2015 at 10.40am.

framework and success of the institutional counter measures in combating cybercrimes. The writers situated their discourse on e-banking crimes, effects of cybercrime on banking and cybercrime policy in Nigeria. The emphasis in the works is on e-commerce and cybercrimes which is not the focus of this research. However, reliance shall be made to the issues of cybercrimes, jurisdictional and evidential issues in this study.

Longe *et al*,[97] and Hassan *et al*,[98] examined the concepts of internet crimes, cybercrime and criminality in Nigeria, nature of cybercrimes in Nigeria, types of cybercrimes, causes of cybercrimes in Nigeria, effects of computer crime and combating cybercrimes in Nigeria. They noted that Nigeria's image has suffered as a result of the nefarious activities some Nigerians who have turned the internet into cheap channel for perpetration of criminal activities, ranging from phishing, online trickery and advance fee fraud popularly known as '419 spam'. That despite the laudable contributions of Internet Service Providers (ISPs) as facilitators of internet usage in Nigeria, the ISPs seemingly remain oblivious of the damaging implications resulting from the use of their infrastructures for online criminal activities. The level of security provided against the crime by ISPs are relatively low resulting in a positive relationship between the level of internet crime and the attitude of ISPs to protecting their networks. Hassan *et al* on their part identified some of the causes of cybercrimes to include urbanisation, unemployment and weak implementation of cybercrime laws. The effect of which include reducing the competitive edge of organisations, waste of production time and damage to the image of the country. Thus, with Nigeria venturing into cashless society, there is a need for cybercrimes menace to be minimized by taking reasonable steps to protect information technology infrastructures like networks and computer systems.

[97] Longe, O. B. *et al* (2009). 'Internet Service Providers and Cybercrime in Nigeria-Balancing Services and ICT Development.' *Journal of Information, Law and Technology (JILT).* Vol. 7, No. 3. Retrieved from www.jiti.net on July 25, 2015 at 11.07am.

[98] Hassan, A. N. *et al* (2012). 'Cybercrime in Nigeria: Causes, Effects and the Way Out.' *ARPN Journal of Science and Technology*. Vol. 12, No. 7. Retrieved from www.ejournalofscience.org on July 25, 2015 at 10.46am

Morano,[99] examined laws that have developed in response to new digital technology were inadequate. He therefore recommended the promulgation of laws relating to the internet specifically same being crucial to the growth of online services and necessarily prerequisite to global information infrastructure.

Writing on economic cost of cybercrimes in Nigeria, Sesan *et al*,[100] observed that cybercrimes are by no means peculiar to Nigeria, nonetheless, they have become persistent source of national chagrin within the comity of nations. Global popular culture continued to associate Nigeria with oil and princes who promised riches via e-mail. That combating the spectre of cybercrimes and the attendant reputational deficit that it occasions has been high on national agenda over the past decades.[101] In a survey conducted between February 15 and March 8, 2013, both online and offline from four locations across Nigeria namely, Abuja (Capital city), Abeokuta (Southwest Nigeria), Minna (Northern Nigeria) and Uyo (South-south Nigeria) with a total 2,980 respondents participating in the survey, 41 per cent of the respondents indicated that they had been victims of cybercrimes at one time or the other, while 59 per cent indicated that they had yet to fall victim.[102] With respect to monetary losses, the sum of N2,146,666,345,014.75 was estimated to be lost to cybercrimes in Nigeria.[103] It is estimated that 1.6 billion people are on the internet, approximately 24 per cent of the world's population provides an unprecedented pool of offenders and victims.[104] Evidence from victimization survey pointed out that about 5 per cent of Americans aged 16 and above were victims of successful and attempted identity theft and the direct financial damage to the victims were as high as $16 billion.[105]

[99] Morano, M. F. (1996). 'Legislating in the Face of New Technology: Copyright Laws for Digital Age.' *Fordham International Law Journal*. Vol. 20, Issue 4, Article 9. Retrieved from http://ir.lawnet.fordham.edu/ilj on July 26, 2015 at 11.11am.
[100] Sesan, G. *et al* (2013) *Op.cit.*
[101] *Ibid.*
[102] *Ibid.*
[103] *Ibid.*, p.11
[104] See Internet World's Stats, Internet Usage Statistics: The Internet Big Picture-World Internet Users and Population Stats (2009). Retrieved from internetworldstats.com/stats.htm on December 26, 2015 at 2.05pm
[105] Wang, S. Y. and Huang, W. (2011) *Op.cit.*, p.2

To Fafinski *et al*,[106] policing practices are often shepherd by incident report and evidence of patterns of crime. This makes the collection and analysis of crime statistics of great value. Cybercrime is no exception. Statistics are been collected on cybercrimes by police and private bodies around the world.[107] However, the distributed nature of the internet makes it challenging to examine the specific geography of cybercrime. As with other crimes, there can be disincentives to report cybercrimes, such as fear that report could undermine public confidence in a business enterprise, but also incentives to over-report, such as to grab headlines. They noted that there is a difficulty in trying to draw any complete distinction between online and offline world.[108] However, legal perceptions would need to be evolved as the cyberspace environment developed and expanded, and that a new conceptualisation of cyber law would be required. By extension, this would also necessitate a redefinition of cybercrimes as a subject of cyber law.[109] The internet has transformed traditional crime on a global scale. The European Convention on Cybercrimes for example, provides a framework for international cooperation in this field, creating a quasi-federated response. The Convention contains a provision on a specific type of trans border access to stored computer data.[110] Notwithstanding the contributions made by the aforementioned writers, this Thesis improved on the existing literature and provided a more up to date analysis and conclusions.

1.8 Organisational Layout

This work comprises five chapters. Chapter one dealt with general introduction and highlighted preliminary matters such as the background and statement of the research problem, aims and objectives of the study, justification, scope of the study, research methodology, literature review and organizational layout.

[106] Fafinski, S. *et al* (2010) "Mapping and Measuring Cybercrime." Retrieved from www.oii.ox.ac.uk/publications /FD18.pdf on October 17, 2016 at 4.30am
[107] *Ibid.,* p.2
[108] *Ibid.*
[109] *Ibid*.
[110] *Ibid.*

Chapter two focused on conceptual clarification of terms, such as artificial intelligence, cyberspace, crime, cybercrimes, criminal responsibility in cybercrimes, motivations for cybercrimes, distinction between cybercrimes and other forms traditional crimes, types/taxonomies of cybercrimes, cyber jurisdiction and the relationship between cybercrimes, economy and national security.

Chapter three examined the legal framework for combating cybercrimes in Nigeria. The examination here was limited to developments of cybercrimes legislation in Nigeria as well as the *Advance Fee Fraud Act 2006, Economic and Financial Crimes Commission Act 2004* and the recently enacted *Cybercrimes Act, 2015.* An examination was also made on the developments of global best practices in some selected municipal jurisdictions such as United Kingdom, United States of America, India and South Africa because of the progress made by the countries in cybercrimes legislation and their geographical spread.

Chapter four is on the role of the institutional framework in the fight against cybercrimes in Nigeria and some selected international institutional agencies such as the Interpol and FATF. The chapter discussed the problems and challenges in the areas of cyber jurisdiction, investigation and issues of evidence.

Chapter five concluded the work with summary, findings, recommendations and conclusions.

CHAPTER TWO

CONCEPTUAL CLARIFICATION/DEFINITIONS OF KEY TERMS

2.1 Introduction

The attempt in this chapter will be to provide conceptual clarification/definitions of key terms with respect to the subject of the study. This is pertinent in view of the fact that it is a relatively emerging area of study. The chapter therefore starts with clarification/definitions the concepts of artificial intelligence, cyberspace, crime, cybercrime, criminal responsibility in cybercrime, classifications/taxonomies of cybercrimes, cyber jurisdiction as well as the relationship between cybercrimes, economy and national security. A basic understanding of these concepts and the salient issues which they raised, are relevant to the overall objectives of this study.

2.2 The Concept of Artificial Intelligence (AI)

Artificial Intelligence (AI) also called machine intelligence, emerged as a research discipline at the Summer Research Project of Darmouth College in July, 1956. John McCarthy who coined the term defined it as "the science and engineering of making intelligent machines."[111] Although, it has earlier been argued that the quest for AI is as modern as the frontiers of computer science and as old as antiquity.[112] The concept of a "thinking machine" is said to begin as early as 2500BC when the Egyptian looked to talking statutes for mystical advice.[113] The universally accepted definition of AI is that "AI is the study of how to make computers do things which, at the moment people do better."[114] The central goals of AI research include reasoning, knowledge, planning, learning, natural language processing (communication), perception and the ability to move and manipulate

[111] Rajaraman, V. (2014) "John McCathy - Father of Artificial Intelligence" in *General Article Resonance.* March, 2014, p.17.
[112] Haack, S. (nd) *Op.cit.*, p.1
[113] *Ibid.*
[114] Rajaraman, V. (2014) *Op.cit.*

objects.[115] An AI system must be capable of doing three things, that is, store knowledge, apply the stored knowledge to solve problems and to acquire new knowledge through experience. AI has three key components – representation, reasoning and learning. Typical AI methods mainly focus on individual human behaviour and inference procedures. On the other hand, Distributed AI (DAI) mainly focuses on social behaviour.[116]

The view has been that the solutions to ever increasing spate of cybercrimes may be too advance for human but doable for something created by humans: Artificial Intelligence.[117] The rate at which digital crime occurs leaves little hope for human intervention to prevail without human error. As such, AI has a better chance at detecting and analyzing appropriate defences against cybercrimes because it too is a product of technology. In a recent study about application of AI techniques to combat cybercrimes, experts in computer engineering and cyber defence concluded that AI can detect and respond to attacks in a timely and efficient manner and most importantly, that AI can prioritize and prevent secondary attacks.[118]

It is argued that with the expansion of the internet, access to knowledge and tools for committing cybercrimes has spread. To combat these dynamically evolving attacks, conventional methods simply don't cut anymore, AI equipped cybercrimes fighters with innovation and unanticipated defence techniques.[119] AI is already being used by IBM's computer "Watson" to take down cybercriminals in some capacities. Through Artificial Neural Network (ANN)[120] applications - predictions, classifications or control in a complex computer environment is now possible.[121] Again, with the use of Intelligent Agent (IA) applications,[122] computers can cooperate and share data and plan or implement appropriate

[115] *Ibid.*
[116] *Ibid.*
[117] Tatera, K. (2015), *Op.cit.,* p.3
[118] *Ibid.*
[119] *Ibid.*
[120] ANN is a computational mechanism that mimics the functionality of neural networks existing in biological nervous system.
[121] Tatera, K. (2015), *Op.cit.*
[122] Intelligent Agents are autonomous computer - generated forces that communicate with each other.

responses in case of unexpected events.[123] IA technology is collaborative by nature and able to adapt to the environment in which it is deployed, making it a powerful weapon against cybercrime. Other methods used in cyber security research and defence are Artificial Immune System (AIS) applications, Genetic Algorithms (GA) and various hybrid applications. Each AI method applies unique characteristic of AI to combat cybercrimes, but these approaches require a lot of future research and testing. The best method of defence may be a combination of these approaches by implementing a number of extraordinary AI capabilities systematically. Nigeria being technologically backward, is yet to attain this feat.

2.3 The Concept of Cyberspace

The term 'cyberspace' has been defined as "a computer network consisting of a worldwide network of computer networks that use Internet Transmission Control Protocol and Internet Protocol (TCP/IP) networks to facilitate data transmission and exchange."[124] It may be understood as the electronic medium of computer network in which online communication takes place. Historically, the word 'cyberspace' was reported to have been coined by a science fiction novelist and author William Gibson in his 1982 story "Burning Chrome" and was popularized by his 1984 novel "Necromancer."[125] The portion of which is usually cited as follows:

> "Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators in every nation, by a graphic representation of data abstracted from the banks of every computer in the human system… unthinkable complexity. Lines of light ranged in the nonspace of mind, clusters and constellations of data…"[126]

By the 1990s, the term "Cyberspace" became a *defacto* name for internet and later the worldwide web particularly among the academic circles. It is, to borrow from the words of John Ferry Bantow "the present day nexus of computers and telecommunications

[123] Tatera, K. (2015), *Op.cit.*
[124] Retrieved from http://www.audioenglish.net. Accessed on March 24, 2012 at 4.15am
[125] Retrieved from www.en.wikipedia.org/.wiki/cyberspace. Accessed on March 24, 2012 at 4.08am
[126] *Ibid*.

networks."[127] In current usage, the term cyberspace stands for the global network of interdependent information technology, infrastructures, telecommunication networks and computer processing system. And as a social experience, individuals can interact, exchange ideas, share information, provide social support, conduct business, direct action, engage in political discussion and so on using global network. The term became a conventional means to describe anything associated with internet and the diverse internet culture. Thus, the core characteristic of cyberspace is that it offers an environment that consists of many participants with the ability to affect and influence each other.[128] Writing on cyberspace, Lawrence[129] noted that:

> Cyberspace is not a place. It is many places. The character of these many places is not identical. They instead differ in ways that are fundamental. These differences come in part from differences in the people who populate these places. Cyberspace has changed in part because the people using it have changed, and in part because the capacities provided by the space have changed… At the start of the internet, communication was through text, media such as USENET Newsgroup, internet Relay chart and e-mail all confined exchange to text to words on a screen, typed by a person…

The above statement by Lawrence underscores the transformation of cyberspace to an ultimate transnational communications network, offering unrivalled capability to access data and computer systems on a global level. Nonetheless, cyberspace provides a unique source of vulnerability for the nation state, whether from political dissent, economic liberalism or cyber terrorism. Cyberspace can be used to undermine state control and circumvent state laws.[130] Thus, Walden[131] noted that;

> Cyberspace spawns cybercrimes. Since crime tends to follow opportunity and the internet provides many new opportunities, then new crimes will certainly emerge. Cybercriminals will be driven by a range of motivation, from intellectual joy riding to political protest. Post September 11th, cybercrimes has become one element of developed nation's fascination with terrorism. Attention has focused

[127] *Ibid.*
[128] *Ibid*
[129] Lawrence, L. (1999). *Code and other Laws of Cyperspace.* Basic Books, NewYork, U.S.A., pp. 63-89
[130] It has been reported that Cyberspace played a critical role in the Egyptian protests that led to the toppling of Mubarak's 30 years rule in Egypt. See 'Internet Role in Egypt's Protest.' *Daily Trust.* February 14, 2011, p. 44.
[131] Walden, I. '*Crime and Security in Cyber space.'* Retrieved from http://www.lawnet. Ik/docs/articles/cv47.htm on April 15, 2012 at 4.51pm

> on the possibilities for 'cyber terrorism'; cybercrimes with a premeditated political motivation as well as for 'cyber war'; state based activity, with the image of a future electronic 'pearlharbour' haunting policy makers.

In determining what constitutes cybercrimes it may be beneficial to outline what constitutes cyberspace. The U.S. National Security Presidential Directive 54/Homeland Security Presidential Directive 23,[132] defines cyberspace as "the interdependent network of information technology infrastructures, and includes the internet, telecommunication networks, computer systems and embedded processors and controllers on critical industries."[133] Put differently, cyberspace is the "virtual environment of information and interactions between people."[134]

Cyberspace is not a fixed predetermined reality operating according to principles and dynamics that cannot be controlled or altered by man. The cyber world is a contracted world, a fabrication because it is constant. Cyberspace is mutable; much of it can be modified and transformed. Criminal actors do not exist in cyberspace rather they exist in the physical world and their actions traverse the real world as well as the cyberspace, impacting victims in the real world.[135] Here, criminals may rely upon cyberspace as a market place to have carryout malicious activities, but they and their victims remain in the physical world.[136]

It has been observed that individual interest for use of available technology, national interest to secure its community from inner and outer threat, sovereign privilege of non interference in any extra-territorial authority, trade and developmental trust are consideration in the area of cyberspace.[137] With the speed of cyber activity and how volume of data used, the protection of cyberspace cannot be handled by any physical device or by human intervention alone. There is the need for considerable automation to detect threats and to

[132] National Security Presidential Directive - 54/Homeland Security Presidential Directive - 23.
[133] *Ibid.,* p.6
[134] *Ibid.*
[135] Finklea, K. and Theoary, C. A. (2015) *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement.* Congressional Research Service (CRS) Report Prepared for Members and Committee of U.S. Congress.
[136] *Ibid.,* p.6
[137] *Ibid.,* p.36

make intelligent real time decision. Cyberspace security management has already become an important component of national security management, military related scientific security management and intelligence management all over the world.[138] Future intrusion threatening national security may not necessarily come from land, air or maritime waters but happen in cyberspace. Intelligence operations and covert actions will increasingly become cyber bound.[139]

The Nigeria's National Cybersecurity Policy defined the concept of cyberspace as:

> An interdependent network of critical and non-critical national information infrastructure, convergence of interconnected information and communication resources through the use of information and communication technologies. It encompasses all forms of digital engagements, interactions, socializations and transnational activities, contacts, contacts and resources deployed through interconnected networks. Cyberspace is recognized as the domain for non-critical and critical national functions such as economic development, trade and commerce, social interactions, communications, medical and health, government operations, national security and defence.[140]

The term cyberspace is simply understood in this context to mean the network of networks that constitute internet and the communication and the content services made available over it. So there has been the growth in the criminality associated with this environment. The internet is built on a modern computer technology with tens of thousands of mutual cooperation on the basis of the network and the network load based on a combination of information collection. It is not only a physical cable connection with a variety of computer networks, it is currently the most influential computer network. Thus, the operation, sustaining and survival of critical national function is anchored on a safe and secured national critical information infrastructure, robust policies and processes with skilled manpower to manage such critical infrastructure.[141]

[138] Mamandi, K. and Yari, S (2014), *Op.cit.,* p.35
[139] *Ibid.*
[140] Para. 2.1-2.1.2 of the Nigeria's National Cybersecurity Policy. December, 2014.
[141] See the Doctrine on Cyberspace Critical Assets and Infrastructure of Nigeria's Cybersecurity Policy, 2014.

2.4 The Concept of Crime

Crime is said to be universal and inevitable in any human society because some violation of code of conducts proscribed by the members of a society are bound to occur.[142] Since the scriptural revelations on Cain and Abel (Arabic: *Qabil* and *Habil*),[143] believed to be the first major crime committed in the history of mankind, crimes and criminality have become inherent and integral aspects of human society.[144] The inevitability and universality of crime has been described by sociologists, such as Emile Durkheim, who argued that to some extent crime helps in promoting social solidarity among people constituting the society. In Durkheim's words:

> "…There is no society that is not confronted with the problem of criminality, its forms changes; the act thus characterized is not the same everywhere; but everywhere and always, there have been men who have behaved in such a way as to draw upon themselves penal repressions…"[145]

Thus, even a society composed of persons possessing good or kind qualities would in the views of Durkheim, not be free from violations of the norms of that society with the result that faults which appear permissible to the layman will create there the same scandal that the ordinary offences does in ordinary consciousness.[146] The views of Durkheim above were shared by Paranjape[147] when he stated thus:

> …It is a myth to think of a crimeless society. Infact, there can be no society without the problem of crime and criminals. The concept of crime is essentially covered with social order…Although most

[142] Qadri, S.M.A. (2009). *Criminology and Penology.* 6th ed. Eastern Book Company, Lucknow, India, p. 1

[143] Cain and Abel are believed to have been the first two sons of Adam and Eve. Cain was the elder son and Abel the younger. Both were asked to offer individual sacrifice to God. God accepted Abel's sacrifice because of Abel's righteousness and Cain out of jealousy, slew Abel. See *Genesis* 4:1-8; *Qur'an* 5:27-37.

[144] It may be argued that the first violation of a human code of conduct as revealed by the scriptures was by Adam and Eve when they ate from the forbidden tree of the knowledge of good and evil and were sent forth from the garden of Eden to till the ground from where he was taken. See *Genesis* 2:16-17 and *Genesis* 3:1-24. The distinction here is that Adam violated the command of his creator not to eat of the forbidden tree thereby committed a sin, Cain's iniquity was against a fellow human being.

[145] Qadri, S.M.A. *Op.cit.*, p.1.

[146] *Ibid*.

[147] Paranjape, N.V. (2010). *Criminology and Penology*. 14th ed. Central Law Publications, Allahabad, India,p.1

> people believe in 'live and let-live' principle. Yet there are few who for some reason or the other, deviate from this behavioural pattern and associate themselves with anti-social elements. This obviously imposes an obligation on the state to maintain normalcy in society. This virtuous task of protecting the law abiding citizens and punishing the law breakers rests with the state which performs it through the instrumentality of law…

There have been problems with the conceptualization of the term "crime." This difficulty, according to Chukkol[148] and Ladan,[149] "stems largely from the complexity of the concept and the elusive imprecision of the word crime." Commenting on the difficulties encounter in defining crime, Smith and Hogan[150] stated thus:

> …It is now rather unfashionable to begin law books with definitions. One reason for this is the difficulty frequently encountered in defining the subject matter of a particular branch of the law; and nowhere has this been more greatly felt than in the criminal law. But a book about crimes which does not tell the reader what a crime is allows him to proceed with his own preconceived notions in the matter.

The above views notwithstanding, attempts have been made in providing theories, perspectives and definitions of crime.[151] The *Criminal Code Act*,[152] particularly in section 2 thereof defined the word 'offence' (or crime) as 'an act or omission which renders the person doing the act or making the omission liable to punishment under this Code or under any Act or Laws…' In section 28 of the *Penal Code*,[153] the word offence was defined to include 'an offence under any law for the time being in force.' It is clear that the principal criminal legislation in Nigeria defined the word 'offence' and not 'crime' *per se*. However, for the

[148] Babaji, B. 'Cybercrimes under Nigerian Law' In: Chukkol, K. S. (2010). *The Law of Crimes in Nigeria*. A.B.U., Press Ltd., Zaria, p.1
[149] Ladan, M.T. (1998). *Crime Prevention and Control and Human Rights in Nigeria*. Justice Watch, Abuja, p.1
[150] Smith, J. C. (2002). *Smith and Hogan Criminal Law*. 10th Edition Butterworths LexisNexis, London, p. 15.
[151] Some of the theories include Physiological and Psychological Theories of Crime; The Functionalist Perspectives of Crime; and the Marxian Perspectives of Crime. See Haralambo, M. and Heald, R.M. (1983). *Sociology: Themes and Perspectives.* University Tutorial Press Ltd, Britain, p. 408-440; see also Dambazzau, (1994). A.B. *Law and Criminality in Nigeria: An Analytical Discourse*. University Press Plc, Ibadan, pp. 45–46
[152] Cap. C 38 Laws of the Federation of Nigeria (LFN), 2004
[153] Cap. P 3 LFN, 2004.

purpose of this work, the words "crime" and "offence" have the same meaning assigned to them because they mean one and the same thing.[154]

From the above definitions, it may be safe to say that crime is that act or omission which the state has prohibited or commanded. As such if a particular act or omission has not been criminalised as crime by the code or any criminal statute, such an act or omission cannot be regarded as an offence in the eye of the law. Thus, inspite of the legal definitions above, three approaches have been identified as explaining what conduct is generally proscribed and regarded as criminal. The three approaches are; the moralists, the utilitarian and the positivists.[155] According to the moralists, crimes are essentially sins or immoral acts. Though, there are some kind of relation between crime and sin to the extent that most various crimes such as murder, rape and theft are also sins,[156] the two radically differ in their content scope and consequences. Whereas the concept of sin emanates from religion or a violation of rules of religion or morality for which punishment is given by God, crime is a legal proposition. It involves the breach of law and the punishment meted out by the state. In sin, there is no direct injury or harm and the remedy is penance, but crime necessarily involves some direct injury and a person who commits a crime is subjected to a term of sentence by the court.[157] Chukkol,[158] rightly identified two problems associated with the moralists conception of crime. He observed that morals are mostly subjective value judgment from time to time; and talking about morality, whose morality? What are the yardsticks that can be used to gauge what is morally right and morally wrong? Chukkol queried.

The utilitarian, on their part, see crime on the ground of what is injurious to the society. That the function of criminal law should be restricted to the prevention of harm and

[154] Note however that learned author Aguda was quoted as holding the view that the word 'crime' and 'offence' in the Criminal Code were not meant to be synonymous, otherwise, that the phrase 'criminal offence' would make no sense if they were. See Ladan, M.T. (1998) *Op.cit.,* p.15
[155] See Chukkol, K.S. (2010) *Op.cit.,* pp.3-9
[156] For one to concede to the saying that absolute divorce of law from morality would be of fatal consequences. See Chukkol, K.S. *Ibid.,* p.4
[157] See generally Paranjape, N.V. (2010) *Op.cit.,* p.9 on the distinction between crime and sin.
[158] Chukkol, K.S. (2010) *Op.cit.,* pp.5-6

the penal law and not to be invoked to enforce a moral principle.[159] It is with the utilitarian view in mind that most European countries have decriminalized offences that do not have direct harm to others or society. Such offences otherwise called victimless crime include drunkenness, homosexuality, begging, etc. It may be stated that the legality or illegality depend mostly upon the morality and economic interests of the society. The positivists argue that crime is whatever act or omission the rulers of the day proscribed by penal consequences. Chukkol[160] submitted that each of the three views highlighted above has some truth and that crime is actually a combination of the three. He noted that:

> …a state has an unfettered discretion to create offences but it behoves the ruling classes to seriously think about enforcement. An act made criminal… which the ordinary members of society cannot justify from moral standpoint cannot command respect or acceptance and will be difficult to enforce… though crime and morality have had overlapping jurisdictions over the years, their areas do not necessarily always overlap… though most crimes are *mala inse* (i.e. what is sinful or moral) the new offences created daily by statutes are clearly *mala prohibita* and may have little or no relationship with sin. It is therefore reasonable to conclude that both the criminal law and morality do help to fashion a society to the achievement of peace and justice but the former can exist without the latter and *vice-versa*.

The above submission by the Chukkol no doubt summed up the relationship between crime and morality. It is pertinent at this juncture to examine the concept of criminal responsibility.

2.5 The Concept and Nature of Cybercrimes

Defining the concept of cybercrimes is not an easy task. Cybercrimes are broad construct for many emerging sorts of abuse and crimes enabled by Information and Communication Technologies (ICT).[161] Cybercrimes embrace harmful behaviour that takes place via cyberspace and that transcend geographical jurisdiction, confusing tradition law enforcement investigation methods.[162] The primary problem for analysis of cybercrimes is the

[159] *Ibid.*, p.6
[160] *Ibid.*, p.8
[161] Hoscheidt, M. M. and Eichner, E. F. (2014) *Op.cit.*, p.446
[162] *Ibid.*

lack of consistent and statutory definition for the activities that may constitute cybercrimes. According to Smith *et al,*[163] "defining cybercrime raises conceptual complexities. Varied definitions do exist. In addition to the difficult of definition, it is also called by variety of terms such as computer crime, computer related crime, digital crime, IT crime, internet crime, virtual crime, e-crime, etc. Cybercrimes can include a variety of criminal offences and activities."[164]

As experiences and technology have developed so have the definition of computer crimes or cybercrimes. Historically, a search for a definition must emphasize the knowledge or the use of computer technology.[165] In the first presentation on computer crime,[166] computer related crime was defined in the broader meaning as: "any illegal act for which knowledge of computer is essential for its successful prosecution."

The 10th United Nations (UN) Congress on the Prevention of Crime and Treatment of Offenders,[167] defined cybercrimes into two categories as:

(i) In a narrow sense, as any illegal behaviour directed by means of electronic operation that target the security of computer systems and data processed by them; and

(ii) In a broader sense, as any illegal behaviour committed by means of or its relation to a computer system or network including such crimes as illegal possessions and offering or distributing information by means of a computer system or network.

In a study on the international legal aspects of computer crime, computer crime was defined as: "encompasses any illegal act for which knowledge of computer technology is essential for its perpetration."[168]

The Council of Europe Recommendations of 1987 adopted a functional approach, and computer related crime was described as "the offences enumerated and defined in the

[163] See Olayemi, O. J. (2014) "A Socio-Technological Analysis of Cybercrime and Cyber Security in Nigeria:." *International Journal of Sociology and Anthropology.* Vol. 6 (3), pp.116-125. Retrieved from www.academic journal.org/ijsa on October 17, 2016.
[164] *Ibid.,* p.117
[165] Schjolberg, S. 'The History of Global Harmonization on Cybercrimes legislation: The Road to Geneva?' Retrieved from http://www.cybercrimeslaw-net/documents/cybercrimes-history.pdf on January 27, 2012
[166] Computer Crime: Criminal Justice Resource Manual (1973). See Schjolberg, S., (1986). Computers and Penal Legislation: A Study of the Legal Politics of a new Technology. Complex 3/86, Universite teforlaget, p.3
[167] Vienna, April, 2000.
[168] *Ibid*.

proposed guidelines or recommendation for national legislators."[169] In the Council of Europe Recommendations of 1995 on Criminal Procedural Law, the term "offences connected with Information Technology" IT offences or IT crimes are described as "encompassing any criminal offence, in the investigation of which investigating authorities must obtain access to information being processed or transmitted in computer systems, or electronic data processing systems.[170]

The Organization for European Cooperation and Development (OECD) recommendations of 1986 included a working definition as a basis for the study, that: "Computer related crime is considered as any illegal, unethical or unauthorized behaviour relating to automatic processing and the transmission of data." According to Tokura,[171] the OECD definition is vague because of the inclusion of the word "unethical" which could also mean the same as "conduct" which covers both acts and omission in cases in which a man is able to show that his conduct, whether in the form of action or inaction was involuntary, he must not be held liable for any harmful result produced by it.

In the proposal for an International Convention on Cybercrimes and Terrorism by the Stanford University, Cybercrimes was defined as: "conduct with respect to cyber systems that is classified as an offence punishable by this convention." A cyber system according to the proposal is "any computer and network of computers used to relay, transmit, co-ordinate, or control communications or data or programs."

The proposal for a European Union Council Framework Decision on Attacks Against Information Systems of April 19, 2002, the European Commission includes a functional definition of cybercrimes as "including attacks against information systems as defined in this

[169] Recommendation No. R (89)9, adopted by the Committee of Ministers of the Council of Europe on September 13, 1989 and Report by the European Committee on Crime Problems: Computer-relatred crime. See http://cm.cre.int/ta/rec/1989/89rg.htm

[170] Recommendation No. R (95)13, approved by the European Committee on Crime Problems (CDPC) at its 44th Plenary Session, May 29-June 2, 1995: Concerning problems of criminal procedural law connected with information technology. See http://cm/coe/int/ta/rec/1995/95r/13.htm

[171] Tokura, S.S. (2008) *Op.cit.*, pp.17-18.

framework decision."[172] The Council of Europe Convention on Cybercrimes of 2001,[173] defines cybercrimes as:

(i) offences against the confidentiality, integrity and availability of computer data and systems;

(ii) computer related offences;

(iii) content related offences;

(iv) offences related to infringements of copyrights and related rights.

According to schjolberg,[174] content related offences such as copyright infringement, racism, xenophobia and child pornography may not be understood as cybercrimes since copyright infringements, for example, are essentially based upon civil agreements and contract. The copyright infringements will often be enforced through civil remedies. Schjolberg's view may be relevant in his home country because in Nigeria, the *Copyright Act* provides for offences of infringement of copyrights,[175] infringement of performer's rights,[176] and infringement of folklore,[177] among other offences, which may be enforceable through criminal prosecution.[178] Child pornography has always been criminal offence. Today, offences such as identity theft, spam and phishing must be included as forming part of cybercrimes.

Ashaolu and Oduwale[179] observed that "there is no comprehensive and tenable legislative material on cybercrimes under the Nigerian law which would have probably defined the phenomenon of cybercrimes." This view was shared and acknowledged by Babaji[180] who stated thus:

> "Cybercrime is new for a number of reasons, such as absence of specific legislation or statute proscribing and punishing

[172] Retrieved from http://europa.en.int on January 27, 2012 at 9.14pm
[173] Retrieved from http://conventions/coe.int/treaty/en/treaties/honl/185.htm on January 27, 2012 at 9.03pm
[174] Schjolberg, S. *Op.cit.*
[175] Section 15 of the *Nigeria Copyright Act*. Cap. C28 LFN 2004.
[176] *Ibid.*, Section 30
[177] *Ibid.*, Section 33
[178] *Ibid.*, sections 20 and 24 which provide for criminal liability.
[179] Ashaolu, D.D. and Oduwale, O. A. (2009) *Op.cit.* p.12
[180] Babaji, B. 'Cybercrimes under Nigerian Law.' In: Chukkol, K. S. (2010) *Op.cit.*, p.518

> cybercrimes… our existing penal statutes do not have direct and adequate provisions on cybercrimes even though, they may not be totally ignorant of cybercrimes…"

The best we have had in Nigeria are "open-blanket" description of duties of law enforcement agencies to include concepts which may be linked to or referred to as cybercrimes.[181] The *Nigerian Cybercrimes, Act 2015* which would have afforded the opportunity of a definition in Nigerian context did not define the term cybercrime.

As it is only the *Telecommunications and Postal Offences Act*[182] attempts a definition of electronic crimes as:

> "any person who… engages in computer fraud or does anything relating to fake payment, whether or not the payment is credited to the account of an operator or the account of the subscriber, is guilty of an offence."

The above definition, it is observed, did not incorporate other forms of cybercrimes like hacking, dissemination of viruses and other malicious codes.[183] Halder and Jaishanker,[184] defined cybercrimes as offences that are committed against individuals or groups of individuals with criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss to the victim or indirectly, using modern telecommunication networks such as internet and mobile phones.

The term 'cybercrimes', to borrow from Paranjape,[185] can be defined as 'any criminal activity that uses a computer either as an instrumentality, targets or means of perpetrating further crime. It is any criminal act, the execution of which computers, computer networks and electronic super highway are involved.[186] Cybercrimes include credit card fraud, pornography, software piracy, theft of computer processor or central processing unit (CPU),

[181] Section 6(b) of the *EFCC Act,* 2004 which made reference to advance fee fraud, computer credit card fraud, etc. as part of the EFCC's jurisdiction.
[182] Cap. T4 LFN. 2004; Note that the AFFA, 2006 provides for electronic telecommunication offences, etc, under sections 12-13.
[183] Ashaolu, D.D. and Oduwale, O.A. (2009) *Op.cit.,* p.13.
[184] Halder, D. and Jaishanker, K. (nd) "Cybercrime and Victimisation of Women: Laws, Rights and Regulations." Quoted in Somaiya, J. *et al* (2014) "A Survey of Web Based Cybercrimes and Prevention Techniques." *International Journal of Computer Applications.* Vol. 105.
[185] Paranjape, N.V. (2009) *Op.cit.,* p.133.
[186] Ashaolu, D.D. and Oduwale, O.A. (2009) *Op.cit.,* p.14.

theft of handsets, mobile or cellular phones, hacking and distribution of viruses and worms, forgery, electronic money laundering, tax evasion, electronic vandalism, terrorism, extortion telemarketing fraud, illegal interception of telecommunication, hate crime, espionage, identity theft, etc.[187] It can be deduced from the aforestated list, though, not exhaustive, that cybercrimes include traditional crimes conducted through the internet.

Cybercrimes are used as umbrella terms to refer to criminal activities that include offences against computer data and systems; computer related offences etc. Since there is no single body that controls the internet, it is no government, cyber criminals perpetrate their criminal activities unnoticed due to the anonymous nature of their conducts, cyber criminals need not be present physically with their victims to commit crimes as these crimes can be sceneless and faceless, thus, cybercrimes are silent in nature, global in characteristics, create high impact and are easy to perpetrate.[188] Thus, cybercrimes are terms used broadly to describe criminal activities in computers or where computer networks are tools, targets or place of criminal activities and include everything from electronic cracking to denial service attacks. They are also used to include traditional crimes in which computers and networks are used to enable elicit activities.

2.5.1 The Concept and Nature of Criminal Responsibility in Cybercrimes

Criminal responsibility is always a function of what the actor believes regarding the nature and consequences of his conduct (and the various probabilities thereof) and what the actor's reasons are for acting as he does in the light of those beliefs.[189] Responsibility, therefore means, legal liability for one's act or omission. Liability applies to that in which the accused may be responsible for his or her act which constitutes a crime thus making him or her subject to conviction and punishment.

---

[187] See Ladan, M.T. (2004) *Op.cit.*, pp.15-16; Chukkol, K.S. (2010) *Op.cit.*, pp.517-518; Ashaolu and Oduwale (2009) *Op.cit.*, p. 14; Paranjape, N.V. (2009) *Op.cit.*, p. 133

[188] Agbonika, J. A. A. *et al* (2016) "Economic and Financial Crimes: Cybercrime, Money Laundering and Financial Terrorism in Nigeria." Paper presented by Faculty of Law, Kogi State University, Anyigba at the 49th Annual Conference of the Nigerian Law Teachers' Conference, Nasarawa State University Keffi.

[189] Alexander, L. and Ferzan, K.K. (2009). *Crime and Culpability: A Theory of Criminal Law*. Cambridge University Press, Cambridge, p.41

The attempt here is a brief discussion on the concept and basic elements of criminal responsibility. The reason is to determine how these principles can be adopted to our study on the concept of cybercrimes.[190] "As a general rule" Ocheme[191] noted, "criminal liability would attach to a man who violates the criminal law. However, the rule is not absolute and is subject to a number of limitations which are succinctly expressed in the Latin maxim *actus non facit reum, nisi mensit rea,* meaning an act itself does not make a man guilty unless his intentions were so." Thus, the intent and the act must both concur to constitute the crime.

Ashaolu and Oduwale,[192] writing on the culpability of cyber criminals noted that:

> The word "*actus*" connotes a deed, a physical result of human conduct. The *actus reus* includes all the elements of the crime excepts the accused person's mental state…it is not majorly an act but consist also in a state of affairs not including an act at all… it sometimes includes the consequences of the acts and the circumstances which constitute the affairs in so far as they are relevant. Where a state of mind is required as part of the essential elements of an offence, like consent in rape, such a state of mind becomes part of the *actus reus* of the crime…

Thus, while the component of *actus reus* is easy to identify, it is not always easy to prove. The commission of the offence in question may not be in doubt, the problem is the proof of its commission because most of the steps are electronic in nature.[193] The requirement of deceit in most cases of fraud may constitute part of the *actus reus* of the offence. For example, the offence of obtaining property by false pretence under section 1 of the *Advance Fee Fraud and Other Fraud Related Offences Act*,(*AFFA*)[194] is to the effect that:

---

[190] It is important to note that many scholars have written in detail on the concept of criminal responsibility or liability. See for example, Smith, J. C. (2002) *Op.cit.,* Caps 4-6; William, G. (1983). *Textbook of Criminal Law*. 2nd ed. Stevens and Sons, London, Caps 3-7; Okwonkwo and Naish. (1999) *Op.cit.,* Caps. 3 and 4; Chukkol, K.S. (2010) *Op.cit.,* pp.37-50; Aguda, A. and Okagbue, I. (1990) *Op.cit.,* n.98, Caps. 2-6; Ocheme, P.A. (2006). *The Nigerian Criminal Law*. Liberty Publications Ltd, Kaduna, Cap. 4; Jefferson, M. *Op.cit.,* Cap. 2.

[191] Ocheme, P.A. (2006) *Op.cit.,* p.23; see the English case of *Fowler vs. Pagett* (1798) 7 T.R. 509, where in a case for the interpretation of a statute which made it an act of bankruptcy for a man to depart his dwelling home whereby his creditors may be defeated or delayed. Lord Kenyon C.J. stated that 'it is a principle of natural justice and of our law that *actus non facit reum, nisi mensit rea*.'

[192] Ashaolu, D.D. and Oduwale, O.A. (2009) (2009) *Op.cit.,* pp.14-15.

[193] For example, in the offence of cyberfraud, it may suffice if a person sends unsolicited mail to an intended victim or where he/she fills out an online order form or eventually claims the proceed of his/her scheme. Every time such a person uses the internet to prosecute his criminal act, the computer performs certain functions which can be said to constitute "*actureus*".

[194] Act No. 14, 2006.

> "…any person who by false pretence and with intent to defraud… induces any other person…to deliver to any person, any property, whether or not the property is obtained or its delivery is induced through the medium of a contract induced by false pretence, commits an offence under this Act."

Therefore, failure of the prosecution to prove inducement or actual deceit of the victim may be fatal to the case of the prosecution.[195] For other crimes such as hacking and unauthorized access where the crime is facilitated by software and other sophisticated tools, the *actus reus* may be as remote as the mere purchase of the software or such tool by the intending criminal intended for the purpose of the unauthorized access.[196]

With respect to *mensrea* or the state of the mind of the accused person in cybercrimes, perhaps, it is more difficult element to prove in the establishment of cyber offences. The reason being that cyber criminals often employ methods identical to legitimate business concerns in order to gain the confidence of the victim. The influence and impact of electronics in the perpetration of the offences also make it more difficult since the criminals need not be seen to commit the act and thus difficult to ascertain his remote intention.[197]

In determining the *mensrea* of cybercrimes, recourse has to be made to the laws creating cyber offences. Using cyber fraud for example, section 1 of the *Advance Fee Fraud Act* provides that;

(1) …any person who by any false pretence and with intent to defraud;

(a) Obtains from any other person in Nigeria or in any other country, for himself or any other person, or

(b) Induces any other person in Nigeria or in any other country, to deliver to any person, any property, whether or not the property is obtained or its delivery is induced through the medium of a contract induced by false pretences, commits an offence under this Act.

[195] See *Ijuaka vs. C.O.P* (1976) NSCC 285, where the Supreme Court of Nigeria held discharging the accused person on the ground that there was no evidence at all that it was the appellant's ability to print genuine 50k notes that induced the complainants to part with their money. Rather, it was the request for money to buy liquid that made them part with their money. The appellant in this case deposited a machine, allegedly capable of printing 50k notes with the two complainants after receiving money from them. The appellant requested for more money from each of the complainants to purchase chemicals and paper for printing the 50k notes. The complainants resisted and demand their monies to be refunded by the appellant which he refused and the complainants reported the matter to the police.

[196] See Ashaolu, and Oduwale (2009) *Op.cit.*, p.6

[197] *Ibid.*, p.18

(2) A person who by false pretence and with intent to defraud, induces any person in Nigeria or in any other country to confer a benefit on him or on any other person by doing or permitting a thing to be done on the understanding that the benefit has been or will be paid for commits an offence under this Act.

From the foregoing, it can be said that the *mensrea* in cyber offences is generally "intention." Thus, a charge under section 1 of *AFFA* that could not prove beyond reasonable doubt the accused's intention to commit the offence is bound to fail without more.

2.5.2 Motivations for Cybercrimes

Motivations for cybercrimes focus largely around personal profit or financial gain. For example, use of malware to gain access to bank account details or a form of protest and/or criminal damage such as hacking and website defacement.[198] Motivations can largely be inferred by examining the function of the programs or tools that are used. Other motivations may for example be for satisfying intellectual curiosity or challenge,[199] general maliciousness, revenge, establishing respect and power amongst online communities or simply boredom.[200] A motivation involve in cybercrimes depend on criminal intent and need. The following are common motives behind cybercrimes:

(a) Monetary Profit

Like many traditional crimes, cybercrimes are motivated by the desire for financial gain. Hackers are no longer enthusiastic cyber geeky profiled teenagers but persons with real bad intentions having monetary interest and selfish motives.[201]

(b) Political Motives

Internet is used by extremists and radical groups for propaganda to attack the website and networks of their opposite group. Today, attacks possess a greater damage potential.

[198] McGuire, M, Dowling, S. (2013) "Cybercrimes: A Review of the Evidence." *Research Report 75*. Retrieved from https://www.gov.uk/...pdf on February 8, 2015 at 9.02am

[199] Albert Gonzalez, for example, was said to be motivated by ego, challenge and greed and was fond of the national attention his computer intrusion and data theft drew. See Weil, N. (nd) "Gonzalez sentenced for Multi-million Dollar Credit Card Scam." Retrieved from https://www.pcworld.com... On February 8, 2016 at 8.35pm.

[200] *Ibid.*, p.6

[201] McAfee Report (2013) "The Economic Impact of Cybercrimes and Cyber Espionage." Center for Strategic and International Studies, p.9.

Various claims from hacker group regarding hacking into Pentagon network to steal military software followed by threats to sell it to terrorists if their demands are not met.[202]

(c) Sexual Impulses

Sexual deviant behaviour is illegal and is considered harmful. People view porn sites to fulfill their immoral desires and needs.

(d) Entertainment

Many cybercrimes are done for fun and enjoyment unlike other cybercrimes, in which internet is means to an end. For cyber criminals such as hackers, fun is both means and an end. The early hackers were basically programmers who programmed on machines for the sheer joy of it. This curiosity could be interpreted as the essence of hacking in its original sense. Some got involved into their acts in an attempt to gain personal fame. Movies such as War Games and Hackers motivated few others as they saw the character of a hacker as a brilliant guy that break the law for noble purposes.[203]

(e) Emotional Motivators

Cyber criminals use anger as motivation as spurned lovers, fired employees, business associates or someone who feels cheated.[204]

It has been posited that the distinction between cybercrimes and other malicious acts and the virtual realm is the actor's motivation.[205] Cyber criminals exhibit a wide range of self interest, deriving profit, notoriety and/or gratification from activities such as hacking, cyber stalking and online pornography.[206] Without knowing the criminal intent or motivation, however, some activities of cyber criminals and other malicious actors may appear on the surface to be similar causing confusion as to whether a particular action should be categorise

[202] Aseef, N. (2005) "Cyber Criminal Activity and Analysis." White Paper Fall. Retrieved from http://www.virus. Itn.com…xml, p.8.
[203] *Ibid.*
[204] *Ibid.*
[205] Finklea, K. and Theohary, C. A. (2015), *Op.cit.*, p.6.
[206] *Ibid.*

as cybercrime or not.[207] Terms such as cyber attack, cyber espionage and cyber war are often loosely applied and they may obscure the motives of the actors involved. Criminal attribution is a key delineating factor between cybercrimes and other cyber threats. When investigating a given threat, law enforcement is challenged with tracing the action to its source and determining whether the actor is a criminal or whether the actor may be a terrorist or state actor posing a potentially greater national security threat.[208]

2..5.3 Classifications/Taxonomies of Cybercrimes

This part of the research will explain the classifications/taxonomies of cybercrimes.[209] Discussions on cybercrimes taxonomies give rise to two schools of thoughts. First, that cybercrimes could be boldly categorised in some way. For example, traditional crime that affect technology such as stealing a computer; traditional crime that mediate through technology such as 419 fraud or distribution of obscene content; and exclusively technological crime such as distributed denial of service attack. It is described as: virtual crime, hybrid crime and augmented traditional crime.[210] Cybercrimes may be classified as cybercrimes against person, property and state or society. These classifications are by no means exhaustive because as at 2012, 74 species of cybercrimes have been identified and more are being discovered.[211]

(a) Cybercrimes Against Person

These are cybercrimes committed by direct physical harm or force been applied to the person or victim of the crime. They include:

i. Harassment via Emails

---

[207] *Ibid.*
[208] *Ibid.*
[209] See generally on Classification of Cybercrimes: Pati, P. (nd) 'Cybercrimes.' Retrieved from www.naavi.org on November 20, 2009, Paranjape, N.V. (2009) *Op.cit.,* pp.136-141; www.hitechcj.com/computer/cyber _crime.html; Jeyabalan, R. 'Types of Cybercrimes.' Retrieved from http://cybercelimumbai.com/files on November 20, 2009.
[210] Fafinsky, S. *et al* (2010) "Mapping and Measuring Cybercrime." Retrieved from www.oii.ox.ac.uk/ publications/fd18.pdf October 17, 2016 at 4.30am.
[211] Aaushi, S. and Srinidi, R. (2012), *Op.cit.,* pp.11-259

This is where the mail is used to annoy or worry somebody by putting pressure on them saying unpleasant things to them. Patithasarathi Pati[212] captured the situation when he gave example of a lady who constantly receives email from her former boy friend threatening sometimes emotionally blackmailing her. In another development connected with the use of cyber space in Nigeria, one Miss Cynthia Osokogu, a Postgraduate student of Nasarawa State University and an only child of a retired Major General Frank Osokogu was killed by two fraudsters she met and befriended on facebook. The suspects-Nwabuzo Okumo and Ezekiel Odera were said to have lured her to a Lagos hotel where she was drugged, chained and raped before being beaten to death.[213] Cyber harassment, as such encompasses obscenities and derogatory comments directed towards specific individuals focusing for example on race, gender, religion, nationality, sexual orientation etc.[214]

ii. Cyber Stalking

A form of harassment that makes use of modern technology like cell phones, fax machines and other devices to pursue their victims. The criminal may send repeated, threatening or harassing messages at regular or random intervals. Due to the anonymity of the internet, the perpetrator's identity can be completely concealed. In cyber stalking, persistent messages are sent to unwilling recipient thus causing them annoyance, worry and mental torture.[215] It involves following a person's movements across the internet by posting threatening messages on the bulletin boards frequented by the victim, entering the chat-room frequented by the victim or constantly bombarding the victim with emails.[216] Cyber stalking usually occurs with women or children who are stalked by men or adult pedophiles.[217] A cyber stalker generally collects personal information about the victim's name, age, family background, telephone or mobile numbers, work place etc. He collects the information from the internet resources or profiles the victim may have filled-in while opening email or internet

[212] Pati, P. (nd) *Op.cit.*, p.6
[213] See Adibe, J. 'The Cynthia Osokogu's Case.' *Daily Trust.* August 30, 2012, p.56
[214] Pati, P. (nd) *Op.cit.*, p.6
[215] Paranjape, N.V. (2010) *Op.cit.*, p.136
[216] Pati, P. (nd) *Op.cit.*, p.6
[217] Paranjape, N.V. (2010) *Op.cit.*, p.136

relay chat account.[218] Internet Relay Chat (IRC) servers have chat rooms in which people from anywhere in the world can come together and chat with one another. Criminals use it for discussing their exploits or sharing techniques while pedophiles use chat rooms to lure small children. A cyber stalker does not have to leave his home to harass his targets and has no fear of physical avenge since he cannot be physically touched in cyber space. In South Carolina, U.S.A., a woman has been stalked for several years via e-mail by unknown person who threatened her life; threatened to rape her daughter and posted her home address on e-mail, making it openly available to anyone with access to internet.[219]

iii. Dissemination of Obscene Materials/Indecent Exposure

The internet is used to disseminate materials that could be offensive. It may include the hosting of website containing prohibited materials or use of computers for producing obscene materials which may harm, deprave or corrupt the minds of the people. In Mumbai, India, a Swiss couple would gather children and then force them to appear for obscene photographs. They will then upload these photographs to websites specially designed for paedophiles. The Mumbai police arrested the couple.[220]

iv. Cyber Defamation

This is not different from conventional defamation except that it involves the use of cyber space medium. Any derogatory statement which is intended to injure a person's reputation or lower the person in the estimation of the right thinking members of society generally or to cause him to be shunned, avoided or exposed him to hatred, contempt or ridicule. Here, the criminal sends emails containing defamatory matters to all concerned of the victim or post defamatory matters on a website. A disgruntled employee may do this against his employer, ex-boy friend against girl, divorced husband against wife, etc.[221] In India, for example, a disgruntled step father with intent of breaking up the marriage of his

[218] *Ibid.*
[219] Aaushi, S. and Srinidi, R. (2012), *Op.cit.*
[220] *Ibid.*
[221] Pati, P. (nd) *Op.cit.*, p.6

step daughter because he did not want to lose control of her property, which he was the guardian till she got married, sent malicious e-mails containing derogatory things about the step daughter to his would be in-laws.[222]

v. Cyber Fraud

Cyber fraud is the fallacious misrepresentation of fact conveyed with an intention of inducing another to do or refrain from doing something that will lead to some major loss.[223] They are largely motivated by economic reasons. It may assume different forms, such as credit card fraud, that is, unauthorized use of a credit/debit card or card numbers to fraudulently obtain money or property.[224] Credit/debit card numbers can be stole from unsecured websites or obtained in an identity theft scheme. Identity theft occurs when someone appropriates another's personal information without their knowledge to commit the theft or fraud. Identity theft is a vehicle for perpetrating other types of fraud schemes.[225] Here, the victims are led to believe they are divulging sensitive personal information to a legitimate business, sometimes as a response to an email solicitation to update billing or membership information or as an application to a fraudulent internet job posting.[226]

A website offered to sell Alphonso mangoes at through away price. Distrusting such transaction, very few people responded to or supply the website with their credit card numbers. These people were actually sent the Alphonso mangoes. The word about this website spread. Thousands of the people from all over responded and ordered mangoes by providing their credit card numbers. The owners of what was later proven to be a bogus

---

[222] See Aaushi, S. and Srinidhi, R. (2012) *Op.cit.*, p.3

[223] Retrieved from http://www.spamlaws.com/types_of_cybercrimes.html on November 15, 2010 at 4.32am.

[224] For example, customers of one of Nigeria's top banks were reported to have lost over N60,000,000 in a new Automated Teller Machine (ATM) fraud. Most of the affected customers received withdrawal alerts on their mobile phones without conducting any transaction. A customer of the bank who lost N200,000 in the scam said he was in his office one evening when he received an alert from the bank that N200,000 had been withdrawn from his account. He went to the bank to enquire but the bank manager told him to write a complaint which he did, but since then there has been no response. See Muhammad, H. 'Bank Customers Lose over N60,000,000 in ATM scam.' *Daily Trust*. Monday, June 15, 2009, p.47.

[225] Dr. Douglas Rusell, a reknowned ATM expert, cautioned that cyber fraudsters are continuously investing in new technologies and means to compromise security of ATM machines to defraud banks and customers of their monies. The criminal use sophisticated devices such as spy cameras, phishing through the internet, false key pad on the machines board, card trapping to defraud ATM card users. See *Daily Trust.* Thursday, July 29, 2010, p.17.

[226] Retrieved from http://www.hitechcj.comcomputercrime/cyber_crime.html on November 15, 2010 at 4.32am

website then fled taking the numerous credit card numbers and proceeded to spend huge amounts of money much to the chagrin of the card owners.[227]

vi. Phishing/Spoofing and Pharming

Phishing and spoofing are somewhat synonymous in that they refer to forged or faked electronic documents. Phishing is the pursuit of person financial information with the intent to commit fraud by relying upon the recipient's ability to distinguish bogus emails, messages, websites and other online contents, from legitimate ones. They are designed to appear with legitimacy. Phishers can use a combination of tricks involving websites, emails, and malicious software to deceive potential victims for the purpose of stealing their personal identity information and financial account credentials.[228] Spoofing generally refers to the dissemination of email which is forged to appear as though it was sent by someone other than the actual sender. Phishing, often utilized in conjunction with spoofed email is the creation of website to make that site appear as the legitimate business website. Once the fraudulent e-mail has been launched, the spoofed websites attempt to dupe the unsuspecting victims into divulging sensitive information such as passwords, credit card numbers and bank account information. In an American case, a teenager made millions of dollars by spreading false information about certain companies whose shares he had short sold. This information was spread by spending spoofed e-mails, purportedly from news agencies like Reuters, to share brokers and investors who were informed that the companies were doing very badly. Even after the truth came out the value of the shares did not go back to their earlier levels and thousands of investors lost a lot of money.[229] Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. A typical phishing attach begins when phishers send out massive amount of email (spam) or messages with bait, which is intended to trigger the target victims intuitive interest, usually the unsolicited emails, ask recipient to log out the provided URL and confirm their

[227] Aaushi, S. and Srinidhi, R. (2012) *Op.cit.*, p.84
[228] Wang, S. and Huang, W. (2011) *Op.*cit., p.9
[229] Aaushi, S. and Srinidhi, R. (2012) *Op.cit.*

personal information details, particularly their password of access. The fraudulent emails are designed to look like they are from large and well known financial institutions such as Bank of America, City Group or PayPal.[230]

Social engineering schemes use 'spoofed' emails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers,[231] hijacking brand names of banks, e-retailers and credit card companies.[232] Technical subterfuge schemes plant crime ware onto personal computers (PC) to steal credentials directly, often using Trojan key logger spy ware. Pharming crime ware misdirects users to fraudulent sites or proxy server.[233]

(b) Cybercrimes Against Property

This is where the computer or system is specifically targeted. The examples include:

i. Computer Vandalism

Computer vandalism occurs when an intruder removes valuable information from the computer system. The intruder prevents the legitimate user from having access to that information. This includes deliberately destroying or damaging a computer or system. That is, doing physical harm or damage to the computer of any person.[234]

ii. Unauthorized Access/Control over Computer System

This is commonly referred to as hacking. Hacking is used to describe cybercrimes such as illegal access, defacing, hijacking, bombing denial of service attack, eaves dropping and so on. Some internet users think hacking is harmless fun but it can be a

---

[230] *Ibid.*
[231] *Ibid.*
[232] A cousin of this researcher, Mohammad Salisu Mayyaki (Zoogy) received an email on Thursday, August 5, 2010 at 7:09pm from "Interswitch Verve ©" <Jason@takumtw.local) requesting him to confirm his information to secure his Interswitch Verve Card from fraud, having as they claimed to have temporarily prevented him access to his account. That he should apply for the upgrade of his ATM Interswitch Verve Card by going to 'their' website: www.radiospacedigital.com/portal/interswetch_service_upgrade_2010.html. The message specifically directed him to enter his card number printed on the card issued by bank and 3-digit number printed at the back of the card. My cousin who incidentally happened to be one of my research assistants in this study did not respond to the demand in the email and nothing affected the use of his bank account. This example typically represented how unsuspecting victims are lured into fraudulent transactions leading to loss of their hard earned savings.
[233] Retrieved from www.hitechcj.com/computer_crime/cyber_crime.html on November 15, 2010 at 4.35am
[234] Pati, P. (nd) *Op.cit.*, p.7

serious invasion of privacy and a significant threat to e-commerce. Hacking is the act of gaining unauthorized access to a computer system or network and in some cases making unauthorized use of this access.[235] Hacking was perceived as a creative activity that helped overcome the limitations of computer about a half century ago when such machines were not common, but the image of hacking changed, largely influenced by the media, to a threatening force. Hacking is attractive for the reason that offenders do not have to physically appear at the crime scene to "rob" or steal from institutions.[236] Hacking is also the act by which other forms of cybercrimes (e.g. fraud, terrorism, etc.) are committed. Hacking in simple terms means illegal intrusion into a computer system without the permission of the computer owner/user. It is the "unlawful access to a computer system... which may include breaking the password of protected website or circumventing password of a computer system"[237] In 1990, hackers broke into and defaced several website including the U.S. Department of Justice, U.S. Airforce, Central Intelligence Agency (CIA), National Aeronautics and Space Administration (NASA) and others. In 1991, when security breach occurred at the research facility of major U.S. automobile manufacturer, the company lost up to $500 million worth of designs for future cars and suffered in the market place because its design fell into the hands of the competitors. In 1995, U.S. Defence Department computers sustained 250 thousand attacks by hackers.[238]

iii. Internet Time Theft/Identity Theft

This is done by gaining access to login ID and the password. The internet hours were used up by any other person.[239] In identity theft, an individual obtains a piece of personal

[235] A French computer hacker was arrested for breaking into President Obama's twitter account. The hacker was tracked down in a trans-Atlantic police operation co-ordinated by the FBI. Agents spent six months on his trail after he managed to gain access to Mr. Obama's twitter account. A micro blogging site, which the President frequently uses to communicate with voters. See *Daily Trust.* Friday, March 26, 2010, p.47.
[236] Wang, S. and Huang, W. (2011) *Op.cit.*, p.9
[237] Ladan, M. T. (2015) *Op.cit.*, pp.38-39
[238] Types and Incidence of Cybercrimes in Nigeria. Retrieved from http://martinslibrary.blogspot.com.ng on December 29, 2015 at 11.10am
[239] Ladan, M. T. (2015) *Op.cit.*

identifying information belonging to another individual and uses that information without the owner's knowledge or approval.[240] For example, a person who knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet any unlawful activity that constitute a violation of a law, can be said to commit an identity theft.

iv. Virus/Worm Transmission

A computer virus is a man made program or piece of code that is loaded onto one's computer without the victim's knowledge and runs against the victim's wishes. Viruses can replicate themselves over and over again and are relatively easy to produce. Viruses can be transmitted as attachment to an e-mail note or in a downloaded file or be present on a diskette or CD.[241] Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They make functional copies of themselves and do this repeatedly till they eat up all available space on a computer's memory.[242] As such virus, worm, Trojan horse,[243] time/logic bombs,[244] are malicious software that destroy information and data in a computer system. Unauthorised installed spyware can either keep a log of the victim's keystrokes (e.g. user names, passwords, security information) or actively seek out key financial information kept on the storage devices. The stolen information is then electronically sent to or retrieved by the offender.[245] Viruses can cause

[240] Wang, S. and Huang, W. (2011), *Op.cit.*, p.4
[241] Aaushi, S. and Srinidhi, R. (2012) *Op.cit.*, p.229
[242] Wang, S. and Huang, W. (2011), *Op.cit.*,p.4
[243] Trojan horse is an unauthorized program which gains control over a computer by representing itself as an authorized program. It is commonly installed through email. Trojan horse is said to be installed in the computer of a lady film director in the United States while chatting. The cyber criminal through the web cam installed in the computer obtained her nude photographs and harassed her. See Pati, P. (nd), *Ibid.*
[244] Logic bombs are programs that are created to do something only when a certain event occurs. They lie dormant in the system and become active only on a particular date. They are event dependent programs.
[245] Wang, S. and Huang, W. (2011), *Op.cit.*, p.11

different damages such as an annoying message appearing on a computer screen, reduce memory or disk space, modify existing data or erase hardware.

In 1999, the Melissa virus was so powerful that it forced Microsoft and a number of large companies to completely turn off their e-mail systems until the virus could be entertained.[246] Melissa virus was released by a man called David Smith, using a stolen American Online Account to post a message promising access to pornographic websites. The virus spread through e-mail messages, replicating and sending itself through computer networks. From 1996 to 2000, many high profile websites such e-bay, UNICEF, The New York Times, Yahoo, Amazon and Microsoft were victims of hackers. Likewise, in 2000, a Philippine programming student released the "I Love You" worm causing significant damage to computers running Microsoft Windows.[247] The Love bug virus filled e-mail gateways as it multiplied exponentially across the internet. The worm appeared as an attachment to an e-mail message that once appeared, used to delete a variety of multimedia files on the victim's computer, and afterwards, would send a copy of itself to every address in the address book. One e-mail message quickly became hundred messages which exploded into thousands of messages, dogging the internet. It took only six hours for the virus to spread worldwide, costing losses of billions of dollars.[248]

v. Intellectual Property Crimes/Distributions of Pirated Software

Computer technology makes it easy to copy creative products such as music or films and the internet provides a free and anonymous means of transmitting or exchanging these pirated materials around the world. Here, the internet is used to copy digital documents without authorisation or when a person tries to make money by registering, selling or using internet domain names that belongs to trademarks.[249] Intellectual property

[246] Aaushi, S. and Srinidhi, R. (2012) *Op.cit.*, p.229
[247] Hoscheidt, M. M. and Eichner, E. F. (2014) *Op.cit.*, pp.450-451
[248] *Ibid.*
[249] *Ibid.*

consists of rights which may be violated by committing software piracy, copyright infringement, trade mark violations. Computer pirates steals valuable intellectual property when they copy software music, graphic/pictures, books, movies, etc. which are available in the internet.[250]

(c) Cybercrimes Against Organization or Society

Here, the society of organisation is targeted. For example:

i. Trafficking

This takes different forms. It may be trafficking in drugs, weapons or human beings. For example, drug traffickers use the internet as a medium for trading their illegal substances by sending out encrypted email and other internet technology. Some drugs, arms or human traffickers arrange their illegal deals at cyber cafes, using courier websites for the delivery of illegal packages.[251]

ii. Cyber Terrorism

Cyber terrorism is "the premeditated use of descriptive activities or threat thereof, in cyberspace with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives."[252] A 'cyber terrorist' is a person who uses computer system to put the public or section of the public in fear; affect adversely the harmony between different religious, racial, language, regional groups, castes, communities, coerce or over awe the government; or endanger the sovereignty and integrity of the nation.[253]

The term "cyberterrorism" was said to have been coined in the 1980s by Barry Collin, a research fellow at the Institute for Security and Intelligence in California, to refer to

[250] See Paranjape, N.V. (2010) Op.*cit.*, p.139; Pati, P. (nd) *Op.cit.*, p.7
[251] See http://www.spamlaws.com/typesofcybercrimes.html
[252] See Paranjape, N.V. (2010) Op.*cit.*, p.137; Pati, P. (nd) *Op.cit.*, p.8
[253] *Ibid.*

"the convergence of cyberspace and terrorism."[254] Cyber terrorism is the premeditated politically motivated attack against information, computer systems, computer programs and data which result in violence against non combatant targets by subnational groups or clandestine agents.[255] Perhaps, the closest examples of real life incidences of cyberterrorism were the 1998 e-mail bombing by the Internet Black Tigers against the Sri Lanken embassies,[256] and in 2002, numerous Indian websites were defaced with messages relating to the Kashmir issue pasted on their home pages. The Pakistani hackers' group led by Doctor Nenkar was believed to be behind the attack.[257] However, some possible scenarios have been described by scholars. In one, a cyber terrorist attacks the next generation of air traffic control systems. Two large civilian aircrafts collide. In another, a cyber terrorist disrupts banks, internal financial transactions and stock exchanges. Economic systems grind to a halt, the public loses confidence and destabilization is achieved. In a third, a cyber terrorist hack into the processing control system of a cereal manufactures and changes the levels of iron supplement. Nations of children gets sick and die.[258] Thus, it has been observed that electronic and electro-magnetic attacks that lead to death, body injury explosions, plane crashes, water contamination, severe economic loss or serious attacks against critical infrastructures may be carried out by cyber terrorists.[259] The intention of cyber terrorists attack could range from economic disruption through interruption of financial networks, systems or in support of physical attacks to cause further confusion and possible delays in proper response or to drive home a political point or enforce a demand for political ends.[260]

[254] Denning, D. E. 'Internet and International Systems: Information Technology and American Foreign Policy Decision Making Workshop': In Brill, A. E., *et al.* (2010) *Op.cit.,* p.23
[255] Politt, M. M. 'Cyberterrorism Fact or Fancy?' Proceedings of the 20th National Information Systems Security Conference. October 1997, pp.285-286
[256] See Denning, D. E. *Op.cit.*, p.23.
[257] See Ashaolu and Oduwale (2009), *Op.cit.*, p.105
[258] Denning, D. E. *Op.cit.*, p.167
[259] See Ashaolu and Oduwale (2009), *Op.cit.*, p.105
[260] *Ibid.*

In 2012, Aljazeera news reported a huge cyber attack on Spamhaus, a Swiss-British anti spam watchdog responsible for keeping advertisements for counterfeit Viagra and bogus weight loss pills out of the world in boxes. The attack that sent ripples of disruption across the web was described as the largest in the history. Spamhaus had been buffeted by the Denial of Service attack in March, 2012 by groups angry at being blacklisted by the Swiss-British group. Denial of Service attack overwhelms a server with traffic, like hundreds of letters being jammed through a mail slot at the same time. Cyber security experts measure those attacks in bits of data per second. Recent cyber attacks, like the one that caused persistent outages at United States Banking site in late 2011 have tended to peak at 100 billion bits per second. But the assault on Spamhause clocks 300 billion bits per second, according to San Francisco - based Cloudflare Inc. which Spamhause has enlisted to help it weather the attack.[261]

In November, 2010, a group calling itself the Indian Cyber Army hacked the websites belonging to the Pakistan Army, Ministry of Foreign Affairs, Ministry of Education, Pakistan Computer Bureau, Council of Islamic Ideology, etc. The attack was done as a revenge for the Mumbai terrorist attack.[262]

iii. Denial of Service Attack

This is an act by the criminal, who floods the band width of the victim's network or fills the victim's email box with spam mail depriving him/her of the services he/she is entitled to access or provide. Spam or unsolicited bulk email is used for committing crimes. It is unsolicited because the recipients have not opted to receive the email. Spam acts as the vehicle for accessing computers and servers without authorization and transmitting viruses and Botnets. The subject masterminding this spam often provide

[261] It was not clear who exactly was behind the attack. However, they were described as disgruntled Russian Internet Service Providers who had found themselves on Spamhause blacklists. The attacks perpetrators had taken advantaged of weaknesses in the internet's infrastructure to trick thousands of servers into routing a torrent of junk traffic to Spamhause every second. The attack sent ripples of disruptions across the internet as servers moved mountains of junk traffic back and forth across the web causing major slowness in the internet activities.

[262] Aaushi, S. and Srinidhi, R. (2012) *Op.cit.*, p.50

hosting services and sell proxy information, credit card information and email list illegally.[263]

iv. Cyber Pornography

It is the use of web for sexual abuse. It is trend among the youth. Internet is used as an avenue for luring paedophiles and for distributing child pornography. Mobile phones and internet facilities are now used by prostitutes to advertise their bodies for internet users. This eventually live their clients to schedule a physical meeting where they carry out their trade. Pornography on the internet may take various forms. It may include hosting websites containing some obscene or prohibited material or use of computers for producing obscene materials. Such materials tend to pervert the thinking of adolescents and corrupt their mind sets.[264] Pornography encourages customers to access their website. Anybody including children can log on to the internet and access websites with pornographic contents with a click of a mouse.

A case in India, perhaps illustrates this phenomenon. A student of the Airforce Balbharati School, Delhi, was teased by all his classmates for having pockmarked face. Tired of the jokes, he decided to get back at his tormentors. He scanned photographs of his classmates and teachers, morphed them nude photographs and put them up on a website that he uploaded onto a free web hosting service. It was only the father of one of the class girls featured on the website objected and lodged a complaint with the police that any action was taken.[265]

v. Fraud, Money Laundering and Tax Evasion

Computers have made fraud and tax evasion more efficient. Money laundering is a kind of cybercrimes in which money is illegally downloaded in transit. There is a phenomenal increase in the incidence of this cyber offence.[266]

---

[263] Retrieved from http://www.hitechcj.com/computercrime/cyber_crime.html on November 15, 2010 at 4.37am
[264] Paranjape, N.V. (2010) Op.*cit.*, p.138
[265] Aaushi, S. and Srinidhi, R. (2012) *Op.cit.*
[266] *Ibid.*, p.139

vi. Net Extortion

Copying a company's confidential data in order to extort the company for huge amount of money.[267]

vii. Salami Attack

This kind of cybercrimes is prevalent in the financial institutions or for the purpose of committing financial crimes.[268] In Salami attack, the criminal makes such program that deducts small amount of money per month from the accounts of all the customer of the bank and deposit the same in his account. The criminal makes insignificant changes in such a manner that such changes would go unnoticed. No account holder will approach the bank for such small amount but the criminal gains huge amount of money.

A closer look at the above classifications of cybercrimes revealed that the classifications are not watertight. For example, the offence of unauthorized access or control over a computer system otherwise known as hacking can be committed against person, individual property, an organization or even the society as a whole.

2.5.4 Distinctions between Cybercrimes and Other Traditional Forms of Crimes

Traditional crimes are violation of the legal codes that are punishable by the state. Central to this is the premise that crimes occur within the boundaries of some physical reference points, that is, a location that constitutes a specific jurisdiction. For example, when conventional case of fraud rears, one of the important consideration is where the actual offence took place so that question of the appropriate jurisdiction for prosecution can be addressed. Officials need to know where the victim and offender came into contact with one another in the perpetration of the offence so that investigative and prosecutorial authority can be determined.[269] However, this component is compounded when cybercrimes are committed

[267] *Ibid.*
[268] Pati, P. (nd) *Op.cit.*, p.4
[269] Finnie, T. *et al* (2010) "The Future Challenges of Cybercrimes." *Proceedings of the Future Working Group.* Vol. 5, p.6.

because the location is no longer a static concept. With the advent of cyberspace, jurisdiction has become much more problematic, transcending local, state and national boundaries.[270]

Equally compounding is the scope of cybercrimes. There are vast range of illegal behaviour that could be identified as cybercrimes. There seem to be degree of ambiguity about what is been discussed when the subject of cybercrime broached. Fraud, technology theft, child pornography and stalking all fall within the realm of cyber criminality. Even within the computer community, there are disagreement about which kinds of behaviour should be classified as criminal. Argument has been that, certain forms of hacking, where a computer is breeched should not be thought of as a criminal act. Advocates of this position maintained that the motivation for this action is often not malicious and may prove beneficial in terms of identifying security shortcomings. It is where sabotage or financial gain is involved that punishment should follow.[271]

The law enforcement community will disagree with this position, pointing out that the so called harmless act of hacking collectively cost billions of dollars in damages.[272] It is difficult to measure the extent of cybercrimes. This is due to the fact that when cybercrime is recorded by authorities it is not necessarily recorded as computer related offence. Rather, it is recorded as cases of fraud, pornography or other conventional crime. Thus, available data on cybercrimes are found in survey which can only give an estimate of the scope of cybercrimes. The lack of substantial data on computer related crimes may be another argument against classifying cybercrimes as unique forms of criminality. Yet it may be a reason for more clearly defining and thus being able to measure cybercrimes.[273]

In 2007, the European Commission issued a communication towards a general policy in the fight against cybercrimes, noting that there was not even an agreed definition of

[270] *Ibid.*
[271] Gordon, S. and Ford, R. (2006) "On the Definition and Classification of Cybercrimes." *Journal of Computer Virology.* Vol. 2, pp.17-20
[272] Susemani, M. A. (1999) "The Critical Challenges from International Hitech and Computer Related Crime at the Millennium." *Duke Journal of Comparative and International Law*. Vol. 9, pp.451-469.
[273] *Ibid.*

cybercrime.[274] The European Commission proposed a three-fold definition: Traditional forms of crime such as fraud or forgery committed through electronic communication, networks and information system; the publication of illegal content over electronic media, for example, child sexual abuse material or incitement to racial hatred and a crime unique to electronic networks, for example, attacks against information systems, denial of service or hacking.[275]

Cyber criminals are different from their gun-toting counterparts in the sense that cyber criminals are rarely in close physical contact with an often not in geographical proximity to their targets. Their distance and anonymity hardly diminish the incident of their crimes nor the damages they can inflict. Cyber criminals are usually located internationally, which makes finding and extraditing them difficult. Again, cyber criminals are directed and targeted toward a specific person or persons or entity. Cyber attacks are multifaceted in terms of their tools, types and outcomes can lead to a cybercrime that is actually a combination of crimes. Cybercrimes are more prevalent more damaging and more sophisticated than ever before.[276]

Cybercrime is an intended act involving the use of computers or other technologies and the criminal activity must take place in a virtual setting such as the internet. Cybercrime share three elements: (i) tools and techniques to perpetrate a crime; (ii) approach or methodology for executing the criminal plan; and (iii) crime itself, that is, the end result of those plans and activities (a cybercrime is the ultimate objective of the criminal's activities).[277]

One of the main differences between traditional crimes and cybercrimes is that software applications, ICT devices, operating systems and malware design complexities are expanding potential effect in terms of scale of denial, disruption, destruction or theft of data and associated financial cost of restoring information systems integrity.[278] Cybercrimes can

[274] European Commission (2007) "Towards a General Policy on the Fight against Cybercrimes." COM (2007) 267 Final. Retrieved from http://eu.lex.europa.eu/... On December 26, 2015 at 2.15pm
[275] *Ibid.*
[276] Singleton, T. (2013) AICPA. The Top 5 Cybercrimes. Retrieved from https://www.aicpa.org/...pdf on December 27, 2015 at 11.10am
[277] *Ibid.,* p.3
[278] Hoscheidt, M. M. and Eichner, E. F. (2014) *Op.cit.,* pp.452-453

be more harmful than traditional crimes, since cyber offenders can deploy multiple attacks at anytime, from anywhere, partly or completely anonymously, against information system. A developed cyber attack can cover its own traces. Cybercrimes can also damage critical infrastructure and other hardware structures.[279]

When referring to cybercrime incidents, terms such as cyber attack and cyber war are often loosely applied and they may obscure the motives of the actors involved. Also, the term cyber espionage or exploitation and cyber attacks are often used interchangeably though they may refer to distinct set of activities that are governed by different laws, regulations or strategies. However, there are areas where these activities overlap causing confusion over the applicable governing structure. It is posited that the over use of the term cyber war or information warfare when referring to cybercrime may sensationalise certain cybercrimes that are threat to public security but not reasonably threat to national security.

2.6 The Concept of Cyber Jurisdiction

The issue of jurisdiction in cyberspace has become a popular topic in law reviews and journals.[280] Jurisdiction is the scope of authority to enforce laws or pronounce legal arguments.[281] Jurisdiction encompasses several concepts, such as jurisdiction to prescribe, jurisdiction to adjudicate and jurisdiction to enforce. Jurisdiction to prescribe is said to be a sovereign entity's authority "to make its laws applicable to the activities, relations or status of persons, or the interest of persons in things… by legislation, executive act or orders, administrative rule or by determination of a court."[282] Jurisdiction to adjudicate is a sovereign entity's authority "to subject persons or entities to the process of its courts or administrative

[279] *Ibid.*

[280] See for example, American Bar Association Section Report: Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet, 55 BUS. Law 1801 (2000); Burns, J.S. and Bales, R.A. 'Personal Jurisdiction and the Web.' 53 ME.L REV 29 (2001); Crave, W., 'Legislative Updates: The World Wide Jurisdiction: An Analysis of Over-Inclusive Internet Jurisdictional Law and Attempt by Congress to fix it. J. ART & ENT. L 267 (2001).

[281] Shinder, D.L. (2002). 'Science of Cybercrimes: Jurisdictional Issues and other Special Problem in Enforcing and prosecuting.' Paper presented at Dallasion Conference on Cyber terrorism, p.5.

[282] S. 401 (a) of *Restatement (Third) of Foreign Relations Law of the United States*. Quoted in Brenner, S.W. and Koops, B. (2004) "Approaches to Cybercrimes Jurisdiction". In *Journal of High Technology Law.* Vol. 4. No.1, (2004) Retrieved from http://www.law.suffolk.edu/highlights/stuorgs/jhtt/docs/pdf/JHT4Brenner-koops-article.pdf on April 13, 2012 at 9.05pm

tribunals for the purpose of determining whether law has been violated.[283] Jurisdiction to enforce is a sovereign entity's authority to compel or induce compliance or to punish non-compliance with its laws or regulations, whether through the courts or by use of executive, administrative, police or other non-judicial action.[284]

Traditionally, all three types of jurisdiction have been based mainly upon the concept of territory. A state had jurisdiction to prescribe for conduct within its territory. The transnational nature of most cybercrimes can give rise to complex jurisdictional issues, involving persons and systems located in different countries. Even where the perpetrators and the victims are located in the same jurisdiction, relevant evidence may reside on a server located in another jurisdiction such as a 'Hotmail' account.[285] The transnational nature of cybercrimes encompasses both the commission of offences and the obtaining and collection of evidence used in the prosecution of such offences.[286] As with many aspects of cyberspace, traditional concepts and principles are sometime challenged by the nature of the technologies involved. The general principle of international criminal law is that a crime is committed within a state's territory may be tried there.[287] The concept of jurisdiction followed from the basic principle that a sovereign entity has a lawful authority to exert control within its territory generally to the exclusion of other states, authority to govern in that territory, and authority to apply law there.[288]

Brenner and Koops (2004) submitted that the 20th and 21st centuries increased use of telecommunications technology undermined certain assumptions that gave rise to the

[283] S. 401 (b), *Ibid.*
[284] S. 401 (c), *Ibid*.
[285] See Walden, I. 'Crime and Security in Cyberspace.' Retrieved from www.lawnet.ik/docs/articles/cv47.htm on April 15, 2012 at 8.02pm
[286] *Ibid.*
[287] *Ibid*.
[288] See Brenner, S.W. and Koops, B. (2004) *Op.cit,* p. 6; In *American Banana Co. vs. United Fruit Co*. (1909) 213 U.S. 347 at 356, the United States Supreme Court held that 'the character of an act as lawful or unlawful must be determined wholly by the law of the country where the act is done.' It thus follows generally that no nation could apply its criminal laws to conduct occurring within the physical territory of another nation. This position is emphasized by Article 4 of the *United Nations Convention Against Transnational Organized Crime* 2000, which provides for protection of sovereignty. It is to the effect that a state party shall not undertake in the territory of another the exercise of jurisdiction and performance of functions reserved exclusively for the authorities of that other state by its domestic law.

traditional model of jurisdiction. It is now easier for someone to commit a criminal act in one country and quickly flee the country, thereby frustrating its ability to apply its criminal laws to the perpetrator.[289] It has also become possible to commit a criminal act against a victim physically situated within the territory of nation B without the perpetrator's ever leaving his own country. This was demonstrated by the saga of the "Love Bug" virus.[290] Jurisdiction is no longer predicated solely upon one's having been physically present within a nation at the time the offence was committed. Under modern conception of jurisdiction, a nation has jurisdiction to prescribe law with regard to any of the following:

(a) Conduct that wholly or substantially takes place within its territory;

(b) Conduct outside its jurisdiction that has or is intended to have substantial effect within its territory;

(c) The status of persons, or interest in things, present within its territory;

(d) The activities, interests, status or relation of its nationals outside as well as within its territory;

(e) Conduct outside its territory by persons not its nationals that is directed against the security of the state or against a limited class of other state interest.[291]

---

[289] *Ibid.*

[290] In May. 2000, the "Love Bug" virus appeared on the internet and spread around the world in two hours. It is estimated to have affected over 45 million users in over 20 countries and to have caused between two and ten Billion Dollars damages. Virus experts traced the "Love Bug" virus to Philippines, where agents from the Federal Bureau of Investigation (FBI) and the Philippines Bureau of Investigation traced it to one Onel de Guzman, a Philippines citizen. The agents investigation was hampered by the fact that virus dissemination was not an offence in the Philippines at that time. The agents had difficulty obtaining warrant to search de Guzman's apartment for evidence pertaining the creation and dissemination of the virus. And when eventually they arrested de Guzman, they faced the problem of prosecuting de Guzman because virus dissemination was not a crime in Philippines. The authorities in Philippines charged de Guzman with fraud and credit card theft on the premise that the virus was meant to harvest user passwords that would be used to obtain internet service and other things of value-but the charges were dismissed as legally insufficient. Ultimately, It was determined that Philippines could not prosecute de Guzman, and because he could not be prosecuted there he could not be extradited for prosecution in the United States or any of the countries in which the "Love Bug" inflicted damage. And base on the national sovereignty concern, extradition treaties require "double criminality", that is, the conduct at issue have been a crime in both countries for extradition to be permissible. See details on the "Love Bug" in Brenner and Koops (2004) *Op.cit.,* pp.6-7.

[291] See for example S.403 (1) of *Restatement (Third) of Foreign Relations Law of the United States* (1987); See also, S.4 of the *Penal Code* and S. 12A of the *Criminal Code* which provide that a state will have jurisdiction to try an offence where the initial element of the offence is committed within the state even if subsequent acts that complete the offence occur elsewhere. The Nigerian *Locus* cases on criminal jurisdiction include *Patrick Jacob Osoba vs. The Queen* (1961) 1 N.L.R., 1; *Sunday Okoro vs. A.G. Western Nigeria* (1966) N.M.L.R 13 and *Patrick Njovens & 3 Ors vs. The State* (1973) N.S.C.C. 257. In *Osoba vs. The Queen* (Supra), the Nigerian Court assumed jurisdiction over a fraudulent Merchant Bank Manager who released the sum of £35, 000.00 to his own use. The Supreme Court of Nigeria overruled the arguments of F.R.A. William (S.A.N), counsel to the Appellant and held that since the initial element of the offence occurred in Nigeria, the Nigerian Courts rightly assumed jurisdiction in the matter. It is therefore clear from the aforestated cases that criminal jurisdiction in Nigeria is essentially territorial in nature.

Even under this expanded view of jurisdiction, a nation cannot exercise jurisdiction to prescribe law with respect to a person or activity having connection with another state when the exercise of such jurisdiction is unreasonable.[292] And whether the exercise of jurisdiction to prescribe is unreasonable is determined by courts considering various factors such as the link of the activity to the territory of the regulating state, that is, the extent to which the activity takes place within the territory or has substantial direct and foreseeable effect upon the territory, the connections such as the nationality, evidence or economic activity between the regulating state and the person principally responsible for the activity to be regulated or between the state and those whom the regulation is designed to protect.[293]

Reasonableness is also required for jurisdiction to adjudicate. Nations have authority to exercise adjudicative authority through their courts if the relationship between the nation and the person or thing that is the object of the adjudicative effort is such as to make the exercise of jurisdiction reasonable. Such an exercise of jurisdiction will generally be deemed to be "reasonable" if any of the following factors exist:

(a) The person or thing is present in the territory of the state, other than transitorily;

(b) The person, if a natural person is domiciled, resident or a national of that state;

(c) The person, if juridical or a corporation, is organized pursuant to the law of that state;

(d) A ship, vehicle or aircraft is registered under the laws of the state;

(e) The person, whether natural or juridical, has consented to the exercise of jurisdiction;

(f) The person, whether natural or juridical, carries on business in the state.

(g) The person, whether natural or juridical, had carried on outside the state an activity having a substantial, direct and foreseeable effect within the state;

(h) The thing, the subject of adjudication is owned, possessed or used in the state…in respect of a claim reasonably connected with that thing.[294]

[292] See for example S. 402 of *Restatement (Third) of Foreign Relations Law of the United States* (1987).
[293] See Brenner, S.W. and Koops, B. (2004) *Op.cit.*, p.9
[294] See for example S. 421 (2) *Restatement (Third) of Foreign Relations Law of the United Stated* (1987).

Again, a nation will have jurisdiction to employ judicial or non-judicial measures to compel or induce compliance or punish non-compliance with its laws if it has the jurisdiction to prescribe under the standards given above.

Brenner and Koops (2004),[295] examined the factors or principles the courts take into consideration in determining whether or not to assume jurisdiction in cybercrimes. They are:

(A) Territorial Claims

(i) Location of the Acts

The Europe Convention on Cybercrimes[296] uses one of the territorial claims, that is, location of the acts, as the main constituting factor of jurisdiction. Article 22 (1) (a) of the Europe Convention on Cybercrimes provides: "Each state party shall… establish jurisdiction over any offence established in accordance with Article 2 through 11 of this Convention, when the offence is committed…in its territory."

It is however, not easy to determine whether or not an offence has been committed in a nation's territory when the commission of the offence involved the use of cyberspace. This was demonstrated in two cases. Firstly, a French court assumed jurisdiction over Yahoo, an American online company and ordered it to remove web pages showing Nazi memorabilia, material that is illegal to view in France but legal in other places.[297] In another case, a British court held a British subject liable for posting photographs on an American web server considered obscene in Britain but not in the United States.[298] National and state laws take various approaches to defining when an offence is committed within a particular country. In the United Sates, for example, the *West Virginia Computer Crimes and Abuse Act* provides that:

> Any person who violates any provision of this code and, in doing so, accesses, permits access to, causes access to, attempts to access a computer, computer network, computer data, computer resources,

[295] Brenner, S.W. and Koops (2004) *Op.cit.*, pp.10-29
[296] *Europe's Convention on Cybercrimes* of November 2001
[297] See *Licra v. Yahoo (2000)*, see also "Yahoo ordered to Bar French from Nazi Websites." Retrieved from www.zdnet.co.uk/story/o,1269./html on March 10, 2012 at 10.31pm
[298] See R v. Waddon (1999), see also Nuttal, C. 'Police Hail Net Porn Ruling!' BBC News at www.bbcnews.co.uk/hi/english/sci/tech/news. Accessed on March 10, 2012 at 10.06pm

> computer software or computer program which is located, in whole or in part, within this state, or passes through this state in transit, shall be subject to criminal prosecution and punishment in this state and to the civil jurisdiction of the courts of this state.[299]

Thus, a court in West Virginia will assume jurisdiction if the access or attempt to access a computer or a computer network, data, resources or software is located in part or in whole within the state or passes through the state in transit.

(ii) Location of Computers

In Singapore, the courts claim jurisdiction over cybercrimes if "for the offence in question…the computer, program or data was in Singapore at the material time."[300] Thus, in Singapore, one of the bases of jurisdiction is the location of computer as at when the offence is being committed.

(iii) Location of Persons

The location of persons, that is, the victims or perpetrators of the offence sometimes constitute factor for jurisdiction. This is easier to determine with physical crimes because the crimes occur in the same place as that of the victim or the perpetrator. However, with content related crimes such as virtual child pornography, that is, child pornography that has been created electronically without real children having been abused. This has been criminalized in the Cybercrimes Convention.[301] Who then is the victim of such offence? It is certainly not the children who have been abused in the making of the pornography. Should this means also that country A that has criminalized virtual child pornography can claim jurisdiction over child pornography produced and located in country B, with the argument that it fueled the list of pedophiles who abused children in country A? the answer to this question depend on whether or not scientific evidence establishes that virtual child pornography causes

[299] Section 61-3c-20 of *West Virginia Code* (2004)
[300] See Article 11(3) *Singapore Computer Misuse Act*.
[301] For example, Article 9 of the *Europe's Convention on Cybercrimes* which provides for "realistic images representing a minor engaged in sexually explicit conduct."

pedophiles to act on their unlawful fantasies about children.[302] If country A can show that the virtual child pornography produced in country B was a causal factor in crimes committed against its citizens and within its territory that makes a much stronger case for allowing country A to claim jurisdiction against the individuals in country B who are responsible for the virtual child pornography.

With respect to the perpetrators of the offence in child pornography cases, countries such as Singapore and Netherland claim jurisdiction over foreigners who have committed the crime abroad if they reside in the country, even if the person starts to reside in the country after the crime was committed.[303] Singapore, for example, claims jurisdiction in cybercrimes if for the offence in question, the accused was in Singapore at the material time, that is, in Singapore when the offence was committed.

(iv) Location of Effect

Jurisdiction may be assumed in respect of an offence committed outside the territory of the state but that had a harmful effect within the territory of that country. In *State of Michigan vs. Dudley*,[304] the court in the United States held that it can prosecute someone who while physically located within the state or outside the state, commits a criminal offence that produces substantial and detrimental effects within the state.

(v) Location of Anything

Article 11 of the *Singapore Computer Misuse Act* has wide reaching jurisdiction. It provides that the provision of the Act shall have effect in relation to any person whatever his nationality or citizenship, outside as well as within Singapore. And where an offence is committed by any person in any place outside Singapore, he may be dealt with as if the offence has been committed within Singapore. The provision of the Act shall apply if for the

[302] Those who support banning virtual child pornography argue that it incites sexual abuse of children; those who oppose such a ban argue that it provides "substitute satisfaction" and reduces offence. See *R vs. Sharpe* (2001) Can. Sup. Ct LEXIS.8
[303] See Brenner and Koops (2004) *Op.cit.*, p.19
[304] (2003) 354 SC 514

offence in question, the accused was in Singapore at the material time or the computer, program or data was in Singapore at the material time.

(B) Personality Claims

(i) Nationality of the Perpetrator

After territoriality, the nationality of the perpetrator is the second major constituting factor of jurisdiction in cybercrimes. The European Cybercrimes Convention for example requires parties to establish jurisdiction when the offence is committed by one of its nationals, if the offence is punishable under criminal law where it is committed or if the offence is committed outside the territorial jurisdiction of any state.[305] Germany and Belgium are reported to have general criminal jurisdiction over a crime committed abroad by their nationals if the act is punishable where it was committed or is not subject to criminal jurisdiction where it was committed.[306] Belgium even allows for the prosecution of foreigners who have aided and abetted a crime committed by a Belgian national outside Belgium.[307]

(ii) Nationality of the Victim

Besides, the nationality of the perpetrator, the nationality of the victim may also be constituting factor. In the United States, the Federal Cybercrimes provision confers jurisdiction to prosecute when the conduct at issue impacts upon the United States itself.[308] It makes it a federal offence for anyone to intentionally, without authorization, to access any non-public computer of a department or agency of the United States. Also, it is a federal crime to knowingly and with intent to defraud, traffic in any password that can be used to access a computer for the government of the United States.[309] In cybercrimes, nationality of the victim may create a few interesting results, such that countries might claim jurisdiction over content related offences with the argument that one of their citizens is a member of the

[305] Article 22 (1) (d) *Europe's Convention on Cybercrimes*, 2001
[306] Section 6 of the *German Criminal Code*, 1998.
[307] Article 7 of the *Belgium Code of Criminal Procedure (CCP) Act, 1993* as amended in 1999.
[308] See for example S. 1030 of the *Computer Fraud and Abuse Act* (18 U.S. Code)
[309] See for example S. 1030 (a), (b) (3) *Ibid.*

class that the offence targets, with viruses, countries could perhaps claim jurisdiction if the computer of one of their nationals residing abroad has been infected.

(C) Other Claims

(i) Protection

The protective principle,[310] allows a country to exercise jurisdiction when an act that occurs outside of its borders threatens its security or basic functions. Examples of such acts include counterfeiting and espionage. The United States has come to rely on the principle more widely as illustrated by its approach to exercising jurisdiction in computer- crime cases. The United States of America *Patriot Act,* enacted in October, 2001 specifically confers extraterritorial jurisdiction in cybercrimes cases. It allows the United States government to exercise jurisdiction over criminal activity impacting upon a protected computer which is defined as a computer that is used in interstate or foreign commerce or communication including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.[311] The United States can now join in international hacker investigations involving investigators and victims in more than one country. The law creates the option, where appropriate of prosecuting such criminals in the United States.

(ii) Universality

For a number of crimes, countries may claim universal jurisdiction. That is, a claim of jurisdiction regardless of the location of the act, the nationality of the perpetrator or victim or any protected interest of a country. For example, Belgium and Germany do claim jurisdiction for a particular cybercrimes; child pornography. In these countries, the dissemination of child pornography can be prosecuted with universal jurisdiction.[312]

[310] Protective principle under International Law allows a sovereign state to assert jurisdiction over a person whose conduct outside its boundaries threatens the state security or interferes with the operation of its government. See *US v. Zehe, 601 F.*
[311] See for example S. 1030 (2) (e) *Ibid.*
[312] See Brenner and Koops (2004) *Op.cit.,* p.28

As noted above, nations have used various theories, essentially territoriality, nationality, protection and universality to justify the exercise of jurisdiction to proscribe and adjudicate the application of prescriptive law in particular types of a criminal activity. While it may be reasonable for a nation to exercise jurisdiction to proscribe criminal conduct – including cybercrimes that takes place wholly or substantially within its territorial boundaries. This being consistent with the premise that nations have jurisdiction to proscribe conduct that is likely to threaten their ability to maintain internal order. The difficulty with cybercrimes is that the sequence of conduct involved in the mission of an offence and its consequences may not occur within the territory of a nation within which the perpetrator is situate at the time he or she consummated the criminal act.[313] However, in *Hartford Fire Insurance Co. vs. California*,[314] the United States Supreme Court was faced with an argument that the U.S. anti-trust laws could not be applied to conduct which occurred in Britain and which was perfectly consistent with British law and policy. The Supreme Court rejected this contention and found quite rightly, that the fact that conduct is lawful in the state in which it took place will not of itself, bar application of the U.S. anti-trust laws, even where a foreign state has a strong policy to permit or encourage such conduct. Likewise, in *United States vs. Kaczowski*,[315] it was held that the fact that bets were accepted in a country where gambling was legal did not preclude indictment for conspiracy to violate and violation of *Wire Act* where gambling was illegal in New York where the bets were placed. Kaczowski was one of the two defendants charged with aiding and abetting and conspiring to conduct, finance and own an illegal gambling business which used facilities in interstate and foreign commerce to distribute the proceeds of unlawful bookmaking between New York and West Indies and Central America to place bets on sporting events.

[313] *Ibid*., p.31
[314] (1993) 509 U.S. 704
[315] (2000) 114 F. Supp. 2d 143

With the aforestated judicial authorities, the law is therefore settled that the fact that a conduct is lawful in the state in which it took place, it will not bar its proscription and penalty in another state where it impacted if the law in that other state proscribed it.

2.7 The Concepts of Cyber Law and Cyber Security

Cyber Law has been defined as "the area of law that deals with the internet's relationship to technological and electronic elements including computers, software, hardware and information system.[316] It is also known as internet law, information technology law, etc."[317] Cyber law are needed for, among other reasons, that "the borders of cyberspace do not map into the borders of real space, which poses a fundamental problem for courts whose jurisdiction is based on geography."[318] Cyberspace is open to participation by all regardless of age, race and geographical location leading to traffic in volumes or billions of information/data in seconds. Cyber law therefore includes all legal standards that seek to combat all forms of cybercrimes and enhance cyber security for the benefit of all stakeholders that necessarily depend on the ICT regime and the cyber environment for prosperity.[319]

Cybersecurity on the other hand, is the coordinated actions pertaining to the prevention, detection, response and recovery from incidence on the part of government authorities, the private sectors and citizens.[320] Cybersecurity strives to ensure the attainment and maintenance of the security, properties of a national cyberspace against security risk. It is a global concern and can only be addressed through the coherent strategy taken into account the role of different stakeholders and existing initiatives.[321]

Cybersecurity objectives comprise; confidentiality, that is, access to a particular segment of the cyberspace and its resources in restricted only to duly authorized entities; availability, that is, availability of cyberspace to its legitimate users; and integrity, that is, cyberspace resources should always be in the form presented by the original entity devoid of

[316] Ladan, M. T. (2015), *Op.cit.*, p.104.
[317] *Ibid.*
[318] *Ibid.*, p.106.
[319] *Ibid.*, p.107.
[320] Mbanaso, U. (2011) *Op.cit.*, p.8.
[321] *Ibid.*, p.9.

tampering, modifications and ensuring non-repudiation.[322] Thus, cybersecurity is the collection of tools, policies, securities, concepts, security safeguards, guidelines, risk management approaches, actions, trainings, best practices, assurance and technologies that can be used to protect the cyber environment and organizations and users' assets. Organization and users' assets include connected computing devices, personnel, infrastructures, applications, services, telecommunication systems and the totality of transmitted and/or stored information in the cyber environment.[323] Thus, cybersecurity encompasses all the necessary elements required to defend and respond to cyber threats in cyberspace, for example, technology, tools, policies, legislation, security concepts, security safeguards, guidelines, risk management approaches, among others.[324]

2.8 Relationship between Cybercrimes, Economy and National Security

Perhaps, a reproduction of the content of the Federal Bureau of Investigation's (FBI) Report to Chairman White House Committee on Cyber Security would capture the discourse under this heading. The FBI's Report[325] states that it is difficult to overstate the potential impact cyber threats pose to national economy, national security and critical infrastructure upon which countries rely. That the number of sophistication of cyber attacks has increased over the years and is expected to continue to grow. The threat has reached the point that given enough time, motivation and funding, a determined adversary will be able to penetrate any system that is accessible directly from the internet.[326] It is therefore difficult to state with

[322] *Ibid.*, p.10.
[323] International Communication Unions (ITU), (2012). Understanding Cybercrime Phenomenon: 'Challenge and Legal Response.' Quoted in Ladan, M.T. (2015) *Op.cit.*, p.81
[324] *Ibid.*, pp.81-82.
[325] See Snow, G.M. (2011) 'Cyber Security: Responding to the Threat of Cyber Criminals.' FBI Report to Chairman, White House Committee on Cyber security. Washington DC, April 2011. Retrieved from http://www.fbi.gov/news/cybersecurity on June 15, 2012
[326] In March, 2012, Chennai –based Copyright labs, an Indian anti-piracy firm won a court order that made Indian ISPs and phone firms stop their customers reaching websites that were illegally sharing copies of certain Bollywood films. The ruling led to a series of cyber attacks by the Hacker group Anonymous, which targeted a number of Indian websites, including those for government departments and India's Supreme Court. Anonymous said the attacks were carried out in retaliation against blocks imposed on video and file-sharing sites. The internet hacking group then staged numerous protests against "Internet Censorship" in India. See 'India unblocks file-sharing sites. Retrieved from www.bbcnews.co.uk on June 15, 2012

confidence that critical infrastructure – the backbone of a country's economic prosperity, national security and public health – will remain unscathed and always be available when needed.[327] The most significant cyber threats to a nation are those with high intent and capability to inflict damage or death, to illicitly acquire assets, or to illegally obtain sensitive or classified military intelligence or economic information. The United States FBI[328] identified the following as affecting the economy and security of countries including the United States.

2.8.1 Cyber threats Against the Private Sector

Cyber criminal threats results in significant economic loses. But the threat against financial institutions is only part of the problem. Of serious concern are threats to critical infrastructures, the theft of intellectual property and supply chain issues.

2.8.2 Cyber Threats to Critical Infrastructure

Critical infrastructure faces growing cyber threat due to advancement in the availability and sophistication of malicious software tool and the fact that new technologies raise new security issues. The increasing automation of critical infrastructures provides more cyber access points for adversaries to exploit. Industrial control system which operates the physical processes of pipelines, railways and other critical infrastructures are at risk of cyber exploitation.[329] The proliferation of malicious techniques could degrade, disrupt, or destroy critical infrastructure.

2.8.3 Intellectual Property theft and Supply Chain Risks

Intellectual property rights violations including theft of trade secrets, digital privacy and trafficking counterfeit goods also represent high cyber criminal threats resulting in losses

[327] The recent security breach by unauthorized intruders into the parent company of National Association of Securities Dealers Automated Quotations (NASDAQ), (a computerized system for trading in securities) is an example of the kind of breaches directed against important financial infrastructure and illustrates the difficulty of determining clear attribution.

[328] See Snow, G.M. (2011) *Op.cit.*

[329] This situation was illustrated in the 2007 Hollywood movie titled "Die hard 4" starred by Bruce Willis as John Melane. The main plot finds Melane fighting a gang of cyber terrorists who hacked into computers and took control of the transportation grids, stock market, power grid and the natural gas supply, while nationally broadcasting messages threatening the United States. The movie captured how critical infrastructures could be hijacked by cyber terrorists causing substantial loss to a country's economy and security.

of billions of dollars in profits annually. These threats also pose significant risk to public health and safety via counterfeit pharmaceuticals, electrical components, aircraft and automobile parts.

Cybercrimes that manipulate the supply chain could pose a threat to national security interests and consumers. Poorly manufactured computer chips infringe on intellectual property rights and could fail at critical times, posing serious health and safety threat to citizens. Malware could be embedded on the chips to infiltrate information from computers and result in the theft of Personally Identifiable Information (PII) that could then be used in future cybercrimes. The use of counterfeits network components can lead to exploitation of cyber infrastructure vulnerabilities and even network failure.

2.8.4 Botnets

Cyber criminals use botnets to perform or assist in certain types of attacks, including distributed denial of service, spamming, sniffing and key logging. Botnets are key automation used to speed the infection of vulnerable systems. Botnets are frequently used for distributed denial of service attack. An attacker can control a large number of compromised host from a remote host station, exploiting their bandwidth and sending connection request to the target host.[330] Botnets are networks of compromised computers controlled remotely by an attacker. Criminals used botnets to facilitate online schemes that steal funds or data to anonymizes online activities and to deny access by others to online resources. Botnets run by criminals and adverse nations could be used by cyber terrorists or nation states to steal sensitive data, raise funds, limit attribution of cyber attacks, or disrupt access to critical national infrastructure. For example, thousands of computers in Iran belonging to government agencies and private companies had been infected with a highly sophisticated virus, dubbed flame,[331] in the latest cyber strike against the Islamic Republic.[332] Iran is said to have been

[330] Esquibel, E. J. *et al* (2005) "Cyber Criminal Activity: Methods and Motivations." Paper Presented for Cyber Security and Homeland Security. University of Washington, CSEP 590TU.

[331] A flame is one of the most sophisticated pieces of malicious software ever discovered. It is used to spy, that is, for reconnaissance. The software tool is believed to be very complete in its ability to steal data. It is able to turn on a computer's microphone to record audio. It can also capture and record internet messaging

three-time the target of very sophisticated computer programme since 2010. The viruses in the previous attacks include Stuxnet, Dugu and Wiper. These viruses are said to have disabled centrifuges for enriching uranium, stolen data in nuclear facilities and erased computers at the oil ministry.[333] Botnets that specialize in data infiltration such as flame are able to capture the contents of encrypted web pages and modify them in real time. When properly configured criminals can ask additional questions at login or modify the data displayed on the screen to conceal ongoing criminal activity.

2.8.5 The "Not for Profit" Cybercriminals

Hacktivist groups[334] such as "Anonymous"[335] undertake protest and commit computer crimes as a collective unit. The online collective known as "Anonymous" is decentralized group operating in cyberspace. The group operates with two broad tenets: (i) Personal anonymity and (ii) The free flow of information.[336] Anonymous is loosely formed organization to the extent that it cannot be easily categorized. For example, membership may be fluid and members may have different interests and motivations for participation and may

---

conversations. Flame can spread wirelessly to nearby device that are blue-tooth enabled. Unlike stuxnet which is used to cause physical damage or interruption of Iran's nuclear facilities, flame is used to gather information by copying key board strokes and the voices of people nearby while remaining hidden in the machine for a long time. Flame, Stuxnet, Dugu and Wiper are reported to have been commissioned by the US and Israel against Islamic Republic of Iran. See Ladeinde, F., 'Formidable Cyber war Against Iran.' *Daily Trust.* June 4, 2012, p. 36.

[332] *Ibid.*

[333] *Ibid.*

[334] A Hacktivist is a hacker who utilizes technology to announce a social, ideological, religious or political message. A Hacktivist uses the same tools or techniques as a hacker, but does so in order to disrupt services and bring attention a political or social cause. Hacktivisms are motivated by revenge, politics, ideology, protest and desire to humiliate victims. See Aaushi, S. and Srinidi, R. (2012), *Op.cit.,* p.131

[335] Anonymous is a loosely associated hacktivist group. It originated in 2003 as members of certain internet subcultures whose actual identities are not known. The group oppose internet censorship and hacked various government and major security corporation websites in protests. Their members can be distinguished in public by the wearing of Guy Fawkes Masks. Some refer to anonymous as a group of online activists, others see the collective as a group of criminal actors and others have likened it to online insurgence. See www.abcnews.go.com. Retrieved on June 10, 2012 at 8.09pm

[336] Finklea, K. and Theoary, C. A. (2015) *Op.cit.,* p.13

use different forms of tactics, both legal and illegal.[337] Anonymous came into the spotlight in 2008 with its first united act to protest the church of scientology which reportedly attempted to pressure internet websites to remove a licked video of actor Tom Cruise endorsing scientology. In response, anonymous members made a Distributed Denial of Service attacks against the Church.[338] Anonymous utilize the internet to communicate, advertise and co-ordinate their actions. Anonymous has initiated multiple criminal Distributed Denial of Service (DDOS) attacks against the Recording Industry Association of America, the Church of Scientology and various businesses in support of wikileaks.[339] Anonymous hacked into websites of a United States firm with United States government contract and reportedly stole about 72,000 e-mails from the company and posted them online. This attack was in response to the claim that a researcher at the company had identified key members of Anonymous group.

In Nigeria, the Anonymous group has in solidarity with Occupy Nigeria group joined forces with the `Naija Cyber Hacktivists of Nigeria' threatened a relentless and devastating attack on the web assets of the Nigerian government. This was in protest to the removal of fuel subsidy that the majority of Nigerians depend upon for their existence, causing the price of fuel and transportation to skyrocket and therefore causing extreme hardship for the majority of Nigerians. On January 13, 2012, the Nigerian Economic and Financial Crimes Commission (EFCC) website was hacked, with a false report of the arrest of people involved in the oil sector subsidy fraud replacing the normal EFCC web page.[340]

---

[337] *Ibid.*
[338] *Ibid.*
[339] Wikileaks is an Australian made international organization launched in 2006 that publishes private, secret and anonymous submissions and leaks of sensitive materials from governments and other high-profile organizations. The recent release of thousands of sensitive diplomatic cables, secret US military logs detailing its operations in Iraq and Afghanistan pitched the U.S Government and its allies against wikileaks front man, Julian Assange. Former US Vice-Presidential candidate Sarah Palin for example calls for Mr. Assange to be pursued with the same urgency Americans pursue *Alqaeda* and *Taliban* leaders. In December, 2010, Sweden issued European arrest warrant for Mr. Assange on sexual assault allegations and he was arrested in London facing extradition trials. Retrieved from http://www.bbcnews.co.uk/.../technology on June 10, 2012 at 8.21pm
[340] See 'Subsidy Protest: EFCC Site hacked with false arrests of Oil Mogols' P. M. News Nigeria. January 13, 2012.

Also, during the 2011 Egyptian revolution, Egyptian government websites along with the website of the ruling National Democratic Party were reportedly hacked into and taken off line by Anonymous group. The sites remained offline until President Hosni Mubarak stepped down.[341]

2.8.6 Cyber Warfare

Cyber warfare is becoming a typical example for interstate conflict. Cyber space is understood as the "fifth battle space" alongside the more traditional arenas of land, sea, air and space. By this view, cyber warfare holds out the possibility of achieving political and strategic goals without the need for armed conflict by making it possible to attack a machinery of state, financial institutions, the national energy and transport infrastructure and public morale.[342] Economic cyber war for example might be understood to be a protracted campaign of espionage, corporate insurgency or intellectual property theft rather than an all out war against the economy of an adversary country.[343]

In retaliation for the removal of a World War II era statue of Soviet soldier, pro-Russian hackers launched a month long campaign that has become known as the first war in cyberspace. Using techniques known as DDOS attack on hitherto unprecedented scale, the attackers managed to effectively shutdown vital parts of Estonia's digital infrastructure.[344] An estimated one million remote controlled computers from around the world were used to bombard the websites of the President, Prime Minister, other government agencies, Estonia's biggest bank and several national newspapers. The attacks were so massive that the North Atlantic Treaty Organisation (NATO) rushed a cyber warfare team of international security experts to assist the Estonian government. The attack was described as a national security situation.[345]

---

[341] Somaiya, R. 'Hackers shut Down Egyptian Government Site.' *The New York Times.* February 3, 2011.
[342] Cornish, P. (2011) 'The Vulnerabilities of Developed States to Economic Cyber warfare: Working Paper Produced by Chatham House, (2001), p. 6. Retrieved from www.chatahamhouse.org.uk on June 10, 2012
[343] *Ibid.*, p. 10
[344] Bachmann, M. and Corzine, J. (nd) "Insights into the Hacking Underground: The Exigency of Cybercrime Research and Intervention." Quoted in Finnie, T. *et al* (2010), *Op.cit.*, p.35
[345] *Ibid.*

2.8.7 Financial Estimates of Damages

Estimating the cost for all types of cybercrimes is challenging. In UK for example, the first main attempt to do so was conducted by Detca which estimated costs of £27 billion.[346] This estimate was questioned by the Home Affairs Select Committee Report on e-crime due to lack of transparent data upon which the estimate were based. The UK Cyber Security Strategy recognised the challenges in this area and noted that "a truly robust estimate will probably never be established, but it is clear the cost are high and rising."

Cyber criminals use their accesses to obtain Personally Identifiable Information (PII) which includes online banking brokerage account credentials and credit card numbers of individuals and businesses that can be used for financial gain. The potential economic consequences are severe. Often businesses are unable to recoup their losses, and it may be impossible to estimate their damage. Many companies prefer not to disclose that their systems have been compromised so they absorb the loss, making it impossible to accurately calculate damages. As a result of the inability to define and calculate losses, the best one can offer are estimates. Virtual environments have become fertile territory for cybercrime, with the number of crimes escalating each year along with the severity of losses. In 2011, online revenue losses resulting from fraudulent transactions were estimated to be $3.4 billion up from $2.7 billion in 2010.[347] Federal Reserve statistics place credit card fraud cost to United States businesses at $52.6 billion annually.[348]

Growth in cybercrimes and their attendant cost are documented in a 2012 Ponemon Institute study. In the study, 56 large US businesses surveyed reported an average annual cost of $8.9 million for cybercrimes, with cost reaching $46 million for one company. Companies participating in the study suffered an average of 102 successful attacks per week, up from 72 in 2011. The report concluded that cybercrimes appeared to be worsening and that 51% of the

[346] McGuire, M. and Dowling, S. (2013) *Op.cit.*, p.27
[347] Singleton, T. *et al* (2013) The Top 5 Cybercrimes. American Institute of CPAS (AICPA), Dirham. AICPA Cybersource Corporation is worldwide e-commerce payment management company. It publishes annual statistics based online fraud reports at cybersource.com.
[348] Fox News "Master Card warns of possible security breach, Visa also reported affected" March 30, 2012. Retrieved from Foxnews.com on April 26, 2016 at 5.06am

Chief Executive Officers reported that their companies had been attacked either daily or hourly.[349]

In 2012, the cost estimation of loss occasioned by cybercrime to Nigeria, was put at N2,146,666,345.14.[350] While about N6.2 billion was reported to have been lost by Nigeria to cybercrimes in 2014.[351] In Nigeria, between the year 2003 and 2007, EFCC successfully disrupted and blocked transactions worth £300 million, €200 million and $500 million dollars respectively. In the same span EFCC successfully prosecuted 97 cybercrimes specific offences.[352] The above mentioned are estimates of the financial implications of cybercrimes. One cannot be specific because most victims of cybercrimes hardly report their losses to the authorities or law enforcement agencies.

2.9 Concluding Remarks

From the foregoing, Artificial Intelligence also called machine intelligence is said to begin long before the modern day computers, traced to early Egyptians civilisation anchored on talking statutes for mystical advice. Today the concept of Artificial Intelligence is used in employing machines to combat cybercrimes through applications such as artificial neural networks, intelligent agents, artificial immune system and other hybrid applications. On the concept of cyberspace, it is seen that cyberspace spawns cybercrime because the internet has provided opportunities for new crimes to emerge. It is further noted that criminal actors do not exist in cyberspace, rather they exist in the physical world and their actions traversed the real world as well as the cyberspace, impacting victims in the real world. It is further seen that criminals rely on cyberspace as a market place to carry out their malicious activities. The concept of crime on the other hand has been conceived as an act or omission which the state

[349] Ponemon Institute conducts independent research on Cybercrime and Information Security Policy. Its annual cost of cybercrimes study was published in August 2011 at ponemon.org. See Ponemon Institute 2012 cost of cybercrime study, October 8, 2012. Retrieved from ponemon.org on April 26, 2016 at 5.10am.
[350] See Sesan, G. *et al* (2012) Economic Cost of Cybercrime in Nigeria. Paradigm the Initiative Nigeria. Retrieved from www.pinigeria.org on May 6, 2016 at 2.55am.
[351] See Shazali, I. (2014) "Nigeria Lost N6.2 Billion to Cybercrime." Retrieved from www.vanguardngr.com on October 20, 2015 at 2.14am.
[352] See Ribadu, N. (2007) *Op.cit.*

has prohibited or commanded. Thus, if any act or omission has not been criminalised by the code or any criminal statute, such an act cannot be regarded as an offence. Thus, responsibility in crime is a function of what the actor believes regarding the nature and consequences of his or her conduct and what reasons are for acting as he or she does in the right of the beliefs. To constitute a crime, therefore a guilty mind must coincide with the prohibited act. In cybercrimes the *actus reus* is easy to identify but not easy to prove because the commission of the offence may not be in doubt, but the problem is the proof of the same because most steps are electronic in nature. Cybercrimes are kind of crimes that happen in "cyberspace" that is, in the world of computer and the internet. These kinds of crimes have the serious potentials for severe impact on peoples' lives and society, because society is becoming an information society, full of information exchange happening in cyberspace.[353] With respect to the *mensrea* or the state of the mind of the accused person in cybercrimes, it is more difficult to prove in the establishment of cyber offences. This is because cyber criminals often employ methods identical to legitimate business concerns in order to gain the confidence of their victims. On motivations for cybercrimes, it is noted that cyber criminals engaged on their crimes for varying reasons or motivations which include getting thrilled for doing illegal activities and hoping not to get caught; seeking publicity; revenge; or because they know how and can, either being smart or getting the instructions and tools from their friends. Motivations for cybercrimes may be for monetary profit, political motives, sexual impulses, entertainment and/or emotional motivation. We have also seen that the impact of electronics in the perpetration of offences also make it more difficult since the criminal need not be seen to commit the act and thus difficult to ascertain his intention. Cybercrimes are unlike their traditional counter parts in the sense that they are facilitated by information technology and can be more harmful than traditional crimes.[354]

[353] *Ibid.*

[354] Analyzing the role of organized criminal group in cyberspace, Grasbosky and Choo distinguished three categories of organized crime group that commit ICT related crimes. Firstly, there are traditional organized criminal groups such as Asian Triad and Japanese Yakuza (operating mainly in China and Japan respectively) that make use of ICT to enhance their terrestrial criminal activities through adopting computer software piracy,

It is also observed that the issue of cyber jurisdiction presents complex challenges to countries and law enforcement institutions established to prevent the commission of crimes generally and cybercrimes in particular. We have seen that even where the perpetrators and the victims are located in the same jurisdiction, relevant evidence may reside on a server located in another jurisdiction. The transnational nature of cybercrimes encompasses both the commission of offences and the obtaining of evidence used in the prosecution of such offences. The general principle of international criminal law is that a crime committed within a country's territory may be tried there. It therefore follows that a sovereign entity has authority to exact control within its territory to the exclusion of other states. It is further seen from the judicial authorities examined above that the fact that a conduct is lawful in the state in which it took place, it will not stop its proscription and penalty in another state where it impacted if the law in that other state proscribed it.

Cybercrimes have negatively impacted on the national economy, security and critical infrastructures upon which countries rely. The threats are real and have reached the point that given enough time and motivation, a determined adversary will be able to penetrate any system from the internet. It is difficult if not impossible to state with confidence that critical infrastructure which is the backbone of a country's economic prosperity, security and public health will always be available when needed. It is therefore pertinent to strengthen national initiatives by updating existing legislation to recognise the existence, threats and transnational nature of cybercrimes and to strive for harmonisation of global legal regimes for combating cybercrimes. There is also the need to improve security awareness by providing adequate resources to secure transactions and equip system operators through training and re-training with the view to stem the increasing tide of global cybercrimes.

---

credit card forgery and fraud; secondly, organized cyber criminal groups which operates solely online. They possess technical expertise to offer terrorist groups in terms of communications and intelligence; and thirdly, organized groups of ideologically and/or politically motivated individuals including state sponsored actors who make use of ICT to carry out their criminal conducts such as Tamil Tigers and Imam Samudra. See Hoscheidt, M. M. and Eichner, E. F. (2014) *Op.cit.*, p.458.

CHAPTER THREE

AN APPRAISAL OF THE LEGAL FRAMEWORK FOR COMBATING CYBERCRIMES IN NIGERIA

3.1 Introduction

The central assumption in this research is that cybercrimes are prevalent in modern societies as a result of the proliferations of information and communication technology as a basic unit of business and communication. The incidence of cybercrimes differ in extent and types from one jurisdiction to another, this, it is submitted accounted for the divergence in the level of development of the legal frameworks for combating its menace in various jurisdiction. The Nigerian government has over the years enacted laws aimed at combating crimes generally, inclusive of cybercrimes. This chapter therefore sets out to primarily appraise the Nigerian legislation enacted with the view to combating cybercrimes. This is necessary in view of the fact that weak legislation has been identified as one of the factors hindering successful prosecution of crimes in Nigeria.[355]

3.2 Existing Legislation on Cybercrimes in Nigeria

3.2.1 The Economic and Financial Crimes Commission (EFCC)[356] Act, 2004

In response to the changes and devastating effects of economic and financial crimes, the Federal Government of Nigeria promulgated the *Economic and Financial Crimes Commission Act*. The *EFCC (Establishment) Act,* 2004 was assented in June, 2003. The Act repealed the *EFCC Act* No. 5 of 2002 and establishes a Commission for economic and financial crimes.[357] The Commission has the power to investigate all economic and financial crimes.[358] sections 14 to 18 provides for the offences under the *EFCC Act*. These include offences relating to financial malpractices, terrorism, false information, retention of proceeds

[355] Akinseye-Goerge, Y. (2000). *Legal System, Corruption and Good Governance in Nigeria.* New Century Law Publishing, Lagos, pp.39-40
[356] Section 44 of the *EFCC Act* 2003.
[357] See Ladan, M. T. (2004) *Op.cit.*; Chawki, M. (2009) *Op.cit.*, p.9
[358] A further discussion of the powers and functions of the EFCC will be made under chapter 4 of this research.

of a criminal conduct and offences in relation to economic and financial crimes and penalties.

The *EFCC Act* defines economic and financial crimes under section 46 as:

> The non-violent criminal and illicit activity committed with the objectives of earning wealth illegally either as individually or in a group or organized manner thereby violating existing legislation governing the economic activities of government and its administration and includes any form of fraud, narcotic trafficking, money laundering, embezzlement, bribery, looting and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking and child labour, illegal oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and privacy, open market abuse, dumping of toxic wastes and prohibited goods, etc.

Chawki,[359] noted that the above definition of economic and financial crimes does not directly refer to internet scam. However, it could be argued that a direct reference to email frauds in the Act is superfluous and unnecessary because the EFCC is already charged with the administering the *Advance Fee Fraud and Other Related Offences Act* which directly governs the advance fee fraud in cyberspace. This view was shared by Ashaolu and Oduwale,[360] who submitted that by section 6 of the *EFCC Act*, the Commission shall be responsible for investigation of all financial crimes including advance fee fraud, money laundering, fraudulent encashment, computer credit crime amongst others. That the special powers of the Commission as provided by section 7 of the Act include power to act as co-ordinating agency for the enforcement of the *Advance Fee Fraud and Other Fraud Related Offences Act* and any other law or regulation relating to economic and financial crimes including the *Criminal Code* and the *Penal Code*. Thus, by a synergy of the provisions, the EFCC has the needed sufficient legislative backing to prosecute cybercrimes in Nigeria even though nothing in the Act expressly gives them an inherent cyber jurisdiction.

On their part, Ehimen and Bola observed that the definition of the economic and financial crimes as provided in the Act is all embracing because, the activities of the *"Yahoo boys*" are sabotage to the economy of the country. To that extent, the EFCC can deal with it,

[359] Chawki, M. (2009) *Op.cit.*, p.9
[360] Ashaolu and Oduwale (2009) *Op.cit.*, p.140

particularly under section 18 of the Act which provides for the offences in relation to economic crimes. Besides, the jurisdiction of the Commission covers a wide range of criminal activities including fraud. The aforestated views might be partly correct. However, the absence of specific legislation on cybercrimes no doubt hinders successful prosecution of the offences under our existing laws.

Section 15 of the *EFCC Act* provides for the offences in relation to terrorism. In particular, subsection 2 of section 15 provides that:

> "Any person who commits or attempts to commit a terrorist act or participates in or facilitates the Commission of a terrorist act commits an offence under this Act and is liable on conviction to imprisonment for life."

It is the view of this researcher that section 15 of the *EFCC Act* has been given further impetus with the enactment by the National Assembly of the *Terrorism (Prevention) (Amendment) Act*, 2013. The *Anti-Terrorism Act* amended the *Terrorism (Prevention) Act*, 2011,[361] which came into force on 3rd June, 2011. It prohibits all acts of terrorism, terrorist financing and other ancillary offences.[362] Before now, Nigeria has ratified the *United Nations Convention for the Suppression of the Financing of Terrorism*, 1999 on 28th April, 2003 and seven (7) out of the thirteen (13) *United Nations Terrorism Conventions*.[363] Perhaps, the offence of cyberterrorism though not specifically stated in section 15 of the *EFCC* and the *Anti-Terrorism Acts*, might be prosecuted thereunder. Section 30 of the *Anti-Terrorism Act* empowers the Office of the National Security Adviser (ONSA) to act as the coordinating body for all security and enforcement agencies under the Act while the office of the Attorney General of the Federation (AGF), to prosecute the offences under the Act.

[361] Act No. 10, 2011
[362] See for example sections 2-14 of the *Terrorism (Prevention) (Amendment) Act*, 2013.
[363] See Ladan, M.T. (2010). 'International Legal and Administrative Regimes for Combating Money Laundering and Terrorist Financing.' A paper presented at A 2 Day Workshop on Money Laundering Law and Regulations. Organised by Lintol Resources Base Ltd., Lagos, March 1-2, p.25; Ladan, M.T. (2013). 'Recent Trends in Regulating Money Laundering and Terrorism Financing in the Banking, Insurance and Capital Market Sectors of the Financial Economy of Nigeria: Role of the Financial Regulators.' *A.B.U. Journal of Commercial Law (A.B.U.J.C.L.)*, Vol. 6, No. 1.

It is further observed that the cyberspace is constantly under assault by cyber spies, thieves, saboteurs and thrill seekers who break into computer systems to steal personal data, trade secrets, vandalize sites, disrupt services, sabotage data and system, launch computer viruses, conduct fraudulent transactions and harass individuals, industries and companies.[364] The cost implications will include loss of sales during disruption, staff time, network delays, increase in insurance cost due to litigation, loss of intellectual property, loss of critical information and communication during emergency, loss of confidence and credibility in the financial system, global loss of image, etc. Nigeria, being one of the top oil producing country in the world is a potential target of cyber terrorist soon as it fully entered the ICT world. With Nigeria's little knowledge in IT security, an attack on the information infrastructure will paralyze, if not totally collapse the telecommunication system and possibly the entire economy.[365] The views expressed above are duly shared and held in this research.

3.2.2 The *Advance Fee Fraud and Other Fraud Related Offences Act,* 2006

The Government of Nigeria has in response to the menace of advance fee fraud[366] and related activities enacted the *Advance Fee Fraud and Other Fraud Related Act (AFFA) 2006*.[367] The Act repealed the *Advance Fee Fraud and Other Fraud Related Offences Act* No. 13 of 1995 and the *Advance Fee Fraud and Other Fraud Related Offences (Amendment) Act*, 2005.[368] The Act was intended to remedy the inadequacies and shortcomings of the provisions of the existing penal legislation on fraud and related crimes. Though, the *AFFA*

[364] *Ibid.*; In June 2013, the US Secretary of State, Hillary Rodham Clinton said that Google's allegations of Chinese hacking its email system are 'very serious' and will be investigated by the FBI. The Obama administration was disturbed by the charges which the internet giant says include breaches of email accounts belonging to senior US officials. The Chinese government rejected the claim, calling it "unacceptable" for Google to blame China for trying to steal the email account passwords of top US government officials, Chinese activists and Journalist. See *Voice of America* (*VOA) News.* June 2, 2003.
[365] *Ibid.*
[366] Advance Fee Frauds (also known as "419" after the section of the Nigerian Criminal Code) are unsolicited confidential business proposals or scheme from someone purporting to be a Nigerian civil servant or official of Nigerian Government Ministries, existing companies, or Nigerian Government contract. The proposals contain official looking stationary with appropriate Government seal, stamps and signatures. The Advance Fee Fraud criminals include university educated professionals who are the best in the world for non-violent crimes. AFF business proposals and schemes are said to have emerged in the mid 1980s following the collapse of the world oil prices which is Nigeria's main foreign exchange earner. See The Nigerian Advance Fee Fraud.U.S. Department of State Bureau of International Narcotics and Law Enforcement Affairs Publication 10465. Retrieved from www.travel.state.gov on May 15, 2013 at 8.46pm
[367] ACT No. 14 2006
[368] Section 21 of the Act.

2006 did not define the term Advance Fee Fraud, however, it gives descriptions of the acts that constitute the crime of obtaining money by false pretences.[369] Akanbi *et al*[370] defines Advance Fee Fraud as the non-violent economic and financial crime encompassing various forms of fraudulent acquisition of wealth and other forms of obtaining financial advantages through deceit.[371]

The *Advance Fee Fraud Act 2006* provides for the offences of obtaining property by false pretences;[372] other related offences;[373] use of premises;[374] fraudulent invitation;[375] receipt of fraudulent document by victim to constitute attempt;[376] possession of fraudulent documents;[377] laundering of funds obtained through unlawful activity;[378] conspiracy, aiding, etc,[379] alternative offences,[380] offences by bodies corporate,[381] electronic telecommunication offences.[382]

Learned scholars Ladan,[383] and Akanbi *et al*[384] have considerably examined the inadequacies of the provisions of the *Advance Fee Fraud Act*s in Nigeria. Perhaps an examination of some of the specific provisions of the Act that received judicial pronouncement is pertinent here because it is under this Act that EFCC is trying hard to combat cybercrimes in forms of advance fee fraud in Nigeria.

(a) Obtaining Property by False Pretence, etc.

Section 1 of the Act provides for the offence of obtaining property by false pretence as follows:

---

[369] Section 1, 2 and 7 of the *AFFA 2006*.
[370] Akanbi, M. M. *et. al.* (2013) *Op.cit.,* p.103
[371] *Ibid.*, p.104
[372] Section 1, *Ibid.*
[373] Section 2, *Ibid.*
[374] Section 3, *Ibid.*
[375] Section 4, *Ibid.*
[376] Section 5, *Ibid.*
[377] Section 6, *Ibid.*
[378] Section 7, *Ibid.*
[379] Section 8, *Ibid.*
[380] Section 9, *Ibid.*
[381] Section 10, *Ibid.*
[382] Section 12, *Ibid.*
[383] Ladan, M.T. (2010) *Op.cit.*
[384] Akanbi, M. M. *et. al.* (2013) *Op.cit.,* pp.101-126

1.(a) Notwithstanding anything contained in any other enactment or law, any person who by any false pretence, and with intent to defraud, obtain, from any other person, in Nigeria or in any other country, for himself or any other person, or

(b) induces any other person, in Nigeria or in any other country, to deliver to any person, any property, whether or not the property is obtained or its delivery is induced through the medium of a contract induced by the false pretence, commits an offence under this Act.

Also subsection (2) and (3) of section 1 provide that:

2. A person who by false pretence, and with intent to defraud, induces any other person, in Nigerian or in any other country, to confer a benefit on him or on any other person by doing or permitting a thing to be done on the understanding that the benefit has been or will be paid for commits an offence under this Act.

3. A person who commits an offence under subsection (1) or (2) of this section is liable on conviction to imprisonment for a term of not more than 20 years and not less than 7 years without the option of fine.

It can be deduced from the provisions of section 1 of the *AFFA* that the Act recognised the extra-territorial effect of the offence as it prescribe for acts or omissions committed within or outside Nigeria as falling within the territorial jurisdiction of the Nigerian courts. In *FRN* vs. *Prince Rapheal Akpiaifo,*[385] the accused counsel *vide* a motion on notice dated 30th June, 2011 prayed the trial court to strike out the charge against the accused person for want of jurisdiction on the ground that the alleged offence, that is, the hacking of the money of the nominal complainant amounting to $600,000 (Six hundred thousand Dollars) through email was done in China and not Nigeria. The accused further argued that the trial court did not possess the requisite jurisdiction to try the case against the accused person.

[385] Unreported suit No. K/EFCC/03/2011. Ruling delivered on 30th May, 2012 by His Lordship Hon. Justice A. M. Bayero, High Court No. 17, Kano.

The prosecution counsel's response was that since the initial element of the offence, that is, the act of sending the email took place in Kano State, the High Court of Kano State has the requisite jurisdiction to try the offence in view of the provisions of section 1 of the *Advance Fee Fraud Act 2006*. Sadly and quite unfortunately, the trial court did not make any pronouncement on the submission of both counsel, but proceeded to strike out the motion for non compliance with the provisions of *Kano State Practice Direction, Part B, Rule 1* which provides that: "where by the High Court Rule or any other rules of procedure, any application is authorised to be made to a Judge for the issuance of a writ of summons in the undefended list or for seeking other reliefs by way of motions or originating summons which may be supported by affidavit, every such application shall be accompanied by a written address in support of the relief sought." That the motion dated 30th June, 2011 was not accompanied by such written address. It is amazing that the Honourable Court, invited to make a judicial pronouncement on a novel issue of law affecting the *AFFA 2006* will take an easy way out of the predicament. Besides, the provisions of the *Kano State Practice Direction 2010* are only applicable to civil proceedings before the court and not criminal proceedings which are regulated by the *Criminal Procedure Code* of Kano State.

It was the view of Akanbi[386] *et al*, and this researcher conceded to the same that a significant improvement in the provisions of *Advance Fee Fraud and Other Related Offences Act 2006* in response to the new wave of economic and financial crimes in Nigeria is that section 1 *AFFA 2006* removes the circumscribed scope of the subject matter of the offence of obtaining financial advantage by deception which is restricted to "anything capable of being stolen" to "any property" of whatever nature as the subject matter of the offence. As such, information belonging to another person in the forms of digital data, Personal Identification Number (PIN) and the like can now be regarded as capable of being stolen and possibly for the purpose of committing further economic crimes such as identity theft, fraud, credit card fraud and so on.

[386] Akanbi, M. M. *et. al.* (2013) *Op.cit.,* p.112

It is important to note that false pretence is still confined to matter of past or present. A false pretence as to a future act is excluded.[387] This is one of the weaknesses identified in the provisions of sections 418 and 419 of the *Criminal Code*.[388] There are instances of future representation, which deserve punishment because there was an intention to fulfil the promise which is only part of the fraudulent scheme. Therefore if a person deceitfully undertakes to do what he never intends to do, this should be within the offence. Most internet frauds are based on future promise upon which the victims rely to part with their hard earned properties.[389]

In *Odiawa vs. FRN*,[390] the accused person was arraigned before High Court, Lagos State, Ikeja Division on information containing allegations of conspiracy to obtain by false pretence, obtaining by false pretence, forgery, uttering and possession of documents containing false pretences. The accused Harisson Odiawa (Alias Abu Belgore), Dr. Tunde Oni, Desmond Okoro, Mr. Sawyer and Others at large with intent to defraud obtained the sum of 655,000 U.S. Dollars from Mr. George Robert Blick, an American citizen resident in Virginia U.S.A. The evidence of the prosecution witnesses were that Mr. George Robert Blick, who used to be the Chief Executive Officer of Enterprise Integration Incorporated, a company he co-founded with two other persons, received an email in his computer at Enterprise Integration from the accused persons in Nigeria seeking a foreign contractor to facilitate the transfer of 20.5 million U.S. Dollars to a company in the United States. Mr. Robert not only parted with his personal savings but dipped his hands into the accounts of the company he co-founded with two other persons. He was arrested by the FBI, tried, convicted and sentenced by a U.S. Grand Jury to 30 months imprisonment for offences of wire fraud and conspiracy to defraud the Nigerian Government of 20.5 million U.S. Dollars.

[387] Section 20 of the *AFFA 2006*
[388] See Akanbi, M. M. *et. al.* (2013) *Op.cit.*, p.112-113
[389] *Ibid.*, p.113
[390] (2010) ECLR 19

Convicting the accused person (Harrison Odiawa) to a total of 130 years imprisonment and ordering a restitution of 10,000 pound sterling to be paid to Mr. Robert Blick, Hon. Justice Oyewole stated that:

> … it is unfortunate that the accused early in life choose to embark on the fast track of financial crime. Cognisance must be taken of the victim who not only lost all he had but is presently serving prison terms in his native U.S.A. The incalculable damage this has done to the image of this country cannot be estimated. For his genre of crime, the court considers that justice is not only served by terms of imprisonment but by restitution to the victim as well…

The court took a harden stance on the accused in this case no doubt, but why the pity on the victim (Mr Robert Blick) who apparently was lured into the fraudulent transaction by greed and criminal intent?

(b) Use of Premises

Section 3 of the Act makes it an offence for a person who being the occupier or is concerned in the management of any premises to cause or knowingly permit the premises to be used for any purpose which constitutes an offence under the Act. The offence is punishable with imprisonment for a term not more than 15 years and not less than 5 years without the option of a fine. In *FRN vs. Imoh Idiong*,[391] by the charge dated 9th July, 2008 the accused was alleged to have knowingly and wilfully permits the premises of which he is the manager, that is, Stallionet Cyber Café situate at No. 59, Etta Agor Road, Calabar to be used in sending scam emails among other charges thereby committing an offence punishable under section 3 of the *AFFA 2006*. The Defence Counsel through its witnesses testified on the measures taken by the accused person to prevent the commission of cybercrimes in its premises including the installation of Closed-Circuit Television (CCTV) device at the said café. The court held discharging and acquitting the accused person that:

> ...It does not matter at least for the purpose of section 3 of the Act whether the accused is a manager or supervisor of the premises used for the purpose which constitute an offence under the Act. In all cases the manager or supervisor of such premises is concerned in the management of such premises. To be culpable however, there must be

[391] Unreported Suit No. FHC/KD/107C/2008. Judgment delivered on November 15, 2011

> credible evidence showing that the recipient or person concerned in the management of such premises, cause or knowingly permits the premises to be used for any purpose which constitutes an offence under the Act. Is there any evidence before the court showing that the accused person had a fore knowledge of the existence of the documents in Exhibit D? Had the documents in question been substantiated and conclusively been found to be meant for the commission of an offence under the Act? The answer to these fundamental questions is definitively in the negative…

On the offence of use of premises under section 3 of the Act, Akanbi *et al* submitted and this researcher quite agreed with them that the use of physical premises is becoming less relevant in the commission of economic crimes in the digital age because the internet has provided an alternative virtual premises to which fraudsters are retreating.[392] Now an individual fraudster can use his handset to do anything online regarding Advance Fee Fraud without going to any internet cafe.

(c) Fraudulent Invitation

Section 4 of the Act deals with the offence of fraudulent invitation. It provides that "A person who by false pretence and with intent to defraud any other person, invites or otherwise induces that person or any other person to visit Nigeria for any purpose connected with the commission of an offence under the Act is guilty of an offence and is liable on conviction to imprisonment for a term not more than 20 years and not less than 7 years without the option of fine."

Fraudulent invitation is one of the methods used by fraudsters and cyber criminals to bring their victims into Nigeria. In 1995, the U.S. Embassy reported that one James Breaux, an American businessman was shot and killed in Surulere, Lagos. Indications were strong that Mr. Breaux was lured into Nigeria by fraudsters. His U.S. passport indicated that he was admitted to Nigeria without a visa or entry stamp by immigration officials.[393] The case of Miss Cynthia Osokogu, a Postgraduate student of Nasarawa State University who was lured to a hotel in Lagos where she was drugged, chained, raped and killed by fraudsters she met

[392] Akanbi, M. M. *et. al.* (2013) *Op.cit.*, p.121
[393] The Publication of United States Bureau of International Narcotics and Law Enforcement Affairs. Retrieved from www.travel.state.gov on September 12, 2013.

on facebook may fit into this example.[394] Fraudsters often send unsolicited emails to victims inviting them to participate in fraudulent transactions. Sometimes, the victims have full knowledge of the illegality of the said transactions. It has been suggested and we conceded that the Act be amended to incorporate punishment for criminally minded victims of the crime such as obtainable in the U.S.A.[395] In *Odiawa vs. FRN (supra)*, for example, the victim of the crime Mr. Robert Blick was sentenced by a United States Grand Jury to 30 months imprisonment for offences of wire fraud and conspiracy to defraud the Nigerian Government of 20.5 million U.S. Dollars. But the trial court in Nigeria took a pity on him and ordered a restitution of £10,000 (ten thousand Pound Sterling) in his favour.

(d) Receipt of Fraudulent Document by Victim to Constitute Attempt

Section 5 of the Act provides that where a false pretence which constitutes an offence under the Act is contained in a document, it shall be sufficient on a charge of an attempt to commit an offence under the Act to prove that the document was received by the person to whom the false pretence was directed. Again, section 5(2) of the Act provides that notwithstanding anything to the contrary in any other law, every act or thing done by a person to facilitate the commission by him of an offence under the Act shall constitute an attempt to commit the offence. On this, it has been submitted that the effect is to oust the test of attempt under sections 4 and 97 of the Penal Code.[396]

In *FRN vs. Imonina Kingsley*,[397] the accused stood trial on a four count charge of attempting to obtain by false pretence by sending scam mails from his mail box to unsuspecting victims punishable under section 1(3) of the *AFFA 2006*. After the close of the prosecution case, the defence made a no case submission on the ground that by the evidence so far led by the prosecution, no reasonable tribunal would convict the accused person on it. The evidence of the sole prosecution witness an operative of the EFCC was that, as part of his

[394] See Adibe, J. (2012) *Op.cit.*, p.56
[395] See Akanbi, M. M. *et. al.* (2013) *Op.cit.*, p.114
[396] See Ladan, M.T. (1998) *Op.cit.*, p.13
[397] Unreported Suit No. FHC/KD/91C/2008. Ruling delivered by M.L. Shuaibu J. on February 4, 2011

investigative duty, he was at Wave Network Cyber Café, Ilorin Kwara state where he met the accused person before a computer system. In front of the accused was a yahoo email address of ThomasDukeforlove@yahoo.com which the accused was working on. The prosecution witness analysed the said email address in the presence of the accused and same indicated that the accused has opened the email address under the name of Thomas Duke from United State. A further analysis of the said email address indicated that the accused had sent email containing false pretence to one Louise Barco with email address of charlo1360@yahoo.com attaching pictures of a white male which was titled "Hope you will like it" and to one Richard Duke of megadesigne@yahoo.com which was titled "Employment form." The accused confirmed in his extra judicial statement to the EFCC operatives that he obtained $1000 from one Christopher Detroy of the United States of America in which he said he collected the money at Benin Republic bearing false name of Mary Johns.

The contention of the Defence counsel was that the entire gamut of the charge *vis a vis* the applicable penal sanctions does not clearly disclose *prima facie* case against the accused person. That the evidence of the prosecution witness did not disclose element of conspiracy as one person cannot commit the offence of conspiracy. The Defence further contended that there was no evidence to prove the essential ingredient of the offence of attempt because for an act to be punishable as an attempt, it must not be remote to the actual offence but very proximate to it. That there was nothing outside the extra judicial statement of the accused person to show that the accused person actually obtained the alleged sum.

The trial court held that by the evidence of the prosecution's sole witness, the accused was linked with the exhibit 'A' series, the computer print outs which piece of evidence was admitted without contest. On exhibit 'B' series, that is, the extra judicial statement of the accused person which the Defence counsel submitted required corroboration, the court stated that the issue bordering on the credibility of witness is outside the purview of no case submission as such the court called upon the accused to enter his defence.

Also, in *FRN vs. Olasaidi Dare*,[398] by an amended charge dated 28th October, 2008, the accused person allegedly attempted to defraud one Heather Wickens with email address heatherwickens@hotmail.com by having found in his possession documents with the subject entitled "Hello" in which the accused claimed to be one Ronald Hud, a computer engineer, a single parent residing in Green Valley, Arizona, U.S.A. which he knew to be false.

At the trial, it was contended on behalf of the accused that the fact that the accused stated that "I am Ronald Hud" in the documents without more is not punishable under the Act, thus, not an attempt to defraud another. It did not show what property of Heather Wickens, the accused attempted to obtain from her by false pretence.

As regards the liability of the accused to facts electronically generated, the Defence counsel submitted that the accused cannot be in possession of facts which were electronically generated from a computer system belonging to the operators of the cyber café. That the *AFFA 2006* does not punish emotional effusion expressed in the document of another without more; even if that other is living within or outside Nigeria.

The court convicted and sentenced the accused person to 4 years imprisonment. And ordering the forfeiture of the accused GSM handset to the Federal Government of Nigeria, the court noted that:

> ...The word "false pretence" was defined under section 20 of the *AFFA 2006* to mean representation whether deliberate or recklessly made by word, in writing or by conduct of a matter of fact or law and which the person making it knows it to be false or does not believe it to be true. In exhibit 'A' series, the accused has presented himself as an engineer living Green Valley, Arizona. However, in his extra judicial statement and evidence in court, the Accused said his name is Olasaidi Dare, a student of the University of Ado Ekiti who lived at No. 91, Old Otta Road, Lagos, while cross-examined, he said he is not a computer engineer and also not a single parent living in Green Valley Arizona, U.S.A. He does not have a daughter named Timmy and that he used the email ronaldhud@yahoo.com to send several letters but none was delivered… from the above, it is very clear that the accused person made a representation which was in fact false. There is willingness on the part of the accused to brag about

[398] Unreported Suit No. FHC/KD/68C/2008. Judgment delivered on April 2, 2012 by Hon. Justice M. L. Shuaibu. The prosecuting counsel in the case Miss Fatsuma Mohammed Esq, a staff of the EFCC was a course mate of the Researcher at the university. She was quiet, taciturn but intelligent student.

> something planned or foreseen, the state of being set to do something. In other words, these was false pretence by the accused to obtain something as a result of false pretence and same was done with intent to defraud unsuspecting victim. Thus, the prosecution need not establish the exact property of Heather Wickens the accused attempted to defraud and the computer system from which Exhibit 'A' series were generated does not necessary have to belong to the accused person…

The above reasoning of the trial court no doubt captured the culpability of the accused person in the case. Nevertheless, while the punishment of forfeiture of the instrument of the crime is commendable, the punishment of 4 years imposed on the accused person falls short of the 7 years minimum provided by the Act.[399]

In *FRN vs. Nvene*,[400] the accused, a final year Law student of Enugu State University of Technology, Enugu was charged on two counts charge of forging/uttering a document knowing same to be false document punishable under section 1(2) of the *Miscellaneous Offences Act,* 2004 and for attempt to obtain money by false pretence with intent to defraud, by sending an email containing false pretence to wit: Request for Financial Assistance to Carryout Welfare Projects for Swiss/German/Italian Nationals in Nigeria from Bank Cantohale Neuchate. The accused sent the mail to the said Bank Cantohale Neuchate purporting to be written by Lord's Providence Swiss/German/Italian Welfare Association thereby committing an offence contrary to section 8(b) and punishable under section 1(3) of the *AFFA 2003.*

The case of the prosecution was that the accused used an unregistered association, that is, Lord's Providence Swiss/German/Italian Welfare Association of Nigeria to defraud foreigners.

The court convicted the accused for the offence of forgery and uttering a document under 1(2) of the *Miscellaneous Offences Act 2004* but declined jurisdiction to entertain the

[399] Section 8 provides that the punishment for attempt to commit an offence under the Act would be as prescribed for in the main offence under the Act.
[400] (2005-2010) ECLRI

offence of attempt to obtain money by false pretence under the *AFFA 2004* (as amended). The court held that:

> "Even though by the combined effect sections 315(1) (a) and 4(b) of the *1999 Constitution*, the *AFFA 2004* as well as the *EFCC Act 2004* are existing laws; this court has no jurisdiction to try cases under the *AFFA* as same are exclusively vested in the state High Courts…"

It should be noted that the case of *FRN vs. Nvene (supra)* was decided under the repealed *AFFA 2004* which conferred jurisdiction to try offences under the Act on State High Court only.[401] However, with the amendment of the *AFFA* in 2006, the jurisdiction to try offences under the Act is now vested on the Federal High Court, the High Court of the Federal Capital Territory and the High Court of the states of the Federation.[402]

Under section 8 of the Act, those who conspire, aid, abet, counsel, procure, invite, induce or attempt the commission of the offences under the Act are punished with the same penalty as is prescribed for the offence under the Act.[403]

In *FRN vs. Helen Laoye*,[404] the accused (a Director, Micro Economic Planning, Ministry of Special Duties, Office of the Governor) was arraigned on two counts charge of conspiracy to obtain money by false pretence contrary to sections 8(a) and 1(3) of the *Advance Fee Fraud and other Fraud Related Offences Act* and obtaining money by false pretence contrary to section 1(3) of the *AFFA*. The accused, Helen Laoye, Dr. E. O. Balogun (at large), Segun Oguntiyimbo (at large), Yemi Olawale (at large) and Bayo Oyetunde (at large) sometimes in February 2004 conspired to obtain and subsequently obtained the sum of N4,000,000 (Four Million Naira) from Messrs Segun Olorunfunmi and Adeola Adepoju, Director of East Atlantic Business Systems Support Services by falsely pretending that the sum represented part payment of security deposit/contract grant guarantee in respect of an

[401] Section 12 of the *AFFA 2005*.
[402] Section 14 of the *AFFA 2006*.
[403] It has been stated that conspiracy is separate offence and it does not merge with the main offence. As such if two or more persons are charged with an offence, they may be charged with conspiracy to commit that offence and the actual offence itself. With respect to an attempt to commit an offence, unlike conspiracy, it merges with the crime if it is eventually committed. A person is thus charged with committing the main offence. See Chukkol, K. S. (2010) *Op.cit.,* p.61 and 68.
[404] (2007-2011) ECLR 69

Information Technology Project to be financed by Department for International Development (DID), Palace Street, London, United Kingdom.

Convicting and sentencing the accused person, the court per Obadina, J, held that:

> ...Conspiracy simply means the meeting of two or more minds to carry out an unlawful purpose in an unlawful way. The purpose of the two minds or more is to commit an offence... in order to prove conspiracy, it is not necessary that there should be a direct communication between each conspirator and every other. All that is needed is that the criminal design is common to all of them. Proof of how they connected with or among themselves is not necessary for there could even be cases where one conspirator may be in one town and the other in another town and they may never have seen each other but there could be acts on both sides which could lead the court to the inference... all of them need not be in one place at the same time for a charge of conspiracy to be upheld... in order to establish the offence of obtaining by false pretence, the prosecution must prove that there is a pretence, that the pretence emanated from the accused person, that it is false, that the accused knew of its falsity or did not believe in its truth, that there was an intention to defraud, that the thing is capable of being stolen... I have listened to the plea of learned defence counsel, it is unfortunate that the accused abused her office by indulging in this kind of scheme. She stands to lose all her years of service with the Federal and the Oyo State Government. The sentence under the *AFFA* is mandatory. The court has no discretion to exercise. I therefore sentence the accused to 10 years imprisonment for each of counts 1 and 2. The sentence to run concurrently and to take effect from when she was first arraigned in this court. I make order that she refund the sum of N4,000,000 (Four Million Naira) obtained from Messrs Segun Olorunfunmi and Adeola Adepoju as restitution upon her release from custody.

In Helen Laoye's case the court imposed the mandatory sentence of 10 years for each of the 2 counts and ordered a restitution of the N4,000,000 (Four Million Naira) defrauded by the accused to the victims upon her release from custody. While the imposition of the maximum sentence even though same was to run concurrently and to take effect from the date of the first arraignment is commendable, the order that the N4,000,000 (Four Million Naira) sum defrauded by the accused is to be paid after release of the convict from custody puts a clog in the victims effort at achieving justice. It means that the victims may have to wait until after the convict served her term of imprisonment to be able to collect their money. At any rate, how could the victim raise the sum during her terms of imprisonment? It is submitted that the court ought to have ordered that the convict's estate or properties be used

for the purpose of settling the restitution sum. That way, the victims may have their money before the expiration of the prison terms to be served by the convict.

In *FRN vs. Usman & 3 Ors*,[405] the accused persons were arraigned on charges of conspiracy to obtain goods by false pretences and obtaining goods by false pretence contrary to sections 8(a) and 1(3) of the *AFFA*. The accused persons represented to the nominal complainants that they were in charge of special projects of the Federal Housing Authority. The accused persons issued Local Purchase Orders (LPOs) to the nominal complainants who supplied the items and products to them believing they were dealing with the Federal Housing Authority, but were not paid their money. While convicting and sentencing the accused persons to various terms of imprisonment, the court held that:

> ...Conspiracy is the meeting of two or more minds to carry out an unlawful purpose or to carry out a lawful purpose as an unlawful way… the purpose of the meeting of the two minds is to commit an offence. While the law does not require the physical meeting of the minds in a predetermined or known place, an offence of conspiracy could be committed by written communication, the prosecution must establish that the criminal minds really met somewhere and to hatch a crime. The prosecution is required to prove the circumstances from which the Judge may presume or infer conspiracy since it is common ground that conspiracy may not be proved by direct evidence…

(e) Possession of Fraudulent Documents

By section 6 of the Act, a person who is in possession of a document containing a false pretence which constitute an offence under the Act commits an attempt to commit an offence under the Act if he knows or ought to know that the document contains false pretence. The word "document" is defined under the Act to include letters, maps, plans, drawings, photographs, matters expressed or described upon any substance by means of letters, figures or marks intended to be used for the purpose of recording that matter, and a document transmitted through fax, a telex machine or any other electronic or electrical devices, a telegram and a computer print out.[406] Thus, fraudulent activities committed

[405] (2010) ECLR 184
[406] Section 20 of the *AFFA 2006*

through the internet telephone, telex machine or any other electronic or electrical device are covered by the Act.[407]

In *FRN vs. Oyekwere Peter Ndigwe*,[408] the accused person stood trial on the allegation of possession of documents containing false pretence contrary to section 6 and punishable under Section 1(3) of the *AFFA 2006*. The accused was found in possession of documents entitled "Nigerian National Petroleum Corporation" and "Nigerian Liquefied Natural Gas" wherein the documents contain proposals for the transfer of $30,000,000 and $19,000,000 to a safe account. In the documents, the accused claimed to be the Chief Accountant of the establishments and he solicited to transfer the said amounts into the account of the beneficiaries because civil servants in Nigeria are not authorised to operate foreign account.

At the trial, the prosecution called one witness and tendered printed documents from the accused email and the accused statement which were admitted as Exhibits 'A' and 'B' respectively. PWI (Chukwunonso Okoro) an operative of the EFCC Lagos was part of the team that raided Shalom World Cyber café situated at Onitsha on 2nd April, 2008. That he purchased a ticket like other customers and positioned himself near the accused as the activities of the accused person appeared suspicious. He was browsing when other members of his team came in and he quickly got up and told the accused to suspend whatever he was doing at the material time. With the accused by his side he printed out the contents of the accused mail box which was ibechinasool@yahoo.com. And while printing the documents, the accused was endorsing on each page to the effect that same where printed out from his mail box.

The accused testified in his own defence to the effect that on 2nd April, 2008 he went to a printing press to print complimentary cards at Onitsha and he wanted his email address to be on the card. He was directed to a Cyber café as they do not give email address at the

[407] See Akanbi, M. M. *et. al.* (2013), *Op.cit.*, p.116.
[408] Unreported suit No. FHC/KD/116C/2008. Judgment delivered on January 9, 2011.

printing press. At the Cyber café, a boy was assigned to do the email address for him as he does not know how to operate a computer. He waited behind the boy who sat on the system when suddenly he heard voice instructing everybody to lie down and he did thinking that it was armed robbery operation. Later PWI matched his back and asked him to stand up. PWI brought some documents which he asked him to sign. When he hesitated, he was slapped and forced to sign. He was taken to Anika Cental Police Station where he was chained by the legs, he was hit by on the face which resulted to some cracks on his tooth and bleedings. He was advised by another detainee to cooperate with his Assailants to avoid being killed. He then endorsed based on what was dictated to him.

Discharging and acquitting the accused person on all the two counts charge, the trial court per Shuaibu J. observed that:

> ...the evidence of the prosecution in establishing the allegation in the two counts charge is mainly the endorsement on Exhibit 'A' series and the extra judicial statement Exhibit 'B'… the documents the accused said belonged to Michael, the boy who was helping him to browse. The court is therefore left with the responsibility of evaluating the accused extra judicial statement in the sense that even if the endorsement by the accused on Exhibit 'A' is a confession within the contemplation of Section 27 of the Evidence Act. It is instructive to say that the said confessional statements were never taken before a superior officer in accordance with the Judge's Rule. Although mere failure to accommodate the practice does not affect the efficacy or evidential value of a confession which a trial court found to be freely and voluntarily made but then it is a commendable precaution for ensuring that enthusiastic junior officer will not endeavour to be tempted to obtain confession to secure conviction… However, to convict an accused person as on alleged confessional statement, the statement must pass the following tests among others; (a) is there anything outside the confession to show that it is true?; (b) is it corroborated?; (c) was the prisoner one who had the opportunity of committing the offence?... Corroborative evidence must be evidence which confirm in some material particular not only that the crime has been committed but it was the accused who committed it… the statements having failed to pass the tests, no conviction can properly be founded on it… the prosecution has not proved the allegations beyond reasonable doubt against the accused person…

However, in *FRN vs. Churchill Joshua Essien (Alias Michelle Logan),*[409] the accused person stood trial on six counts charges of principally having on his possession some documents containing false pretences with intent to defraud unsuspecting victims. The accused in the case was alleged to have been found in possession of several documents via his email entitled michelcole83@yahoo.com bearing different subjects namely; "Honey I have a problem," "Hello dear, now my leave letter have been approved," "Dear, hope you like it," "Cash the cheque my love" and "Pick up your money." Evidence was led by the prosecution revealing how the accused used a female picture to pose as a girl and also used the name Michelle Cole while in actual fact he works and schools in Nigeria. The accused has been sending mails to Nate for dating and requested for money.

It was contended on behalf of the accused that the email belonged to a female and the accused is not a female. That since the documents were only in the mail box of the accused and not in the sent box, it would be unreasonable to conclude that the accused could intend a crime by what he received by an unknown sender at that.

The trial court convicted and sentenced the accused to four (4) years imprisonment on each count with effect from the 31st day of March, 2008 being the date he was first arrested and the sentence was to run concurrently. The trial held that:

> It is no longer in dispute that the documents printed out at the café was from the computer which the accused person was found on… the court has no hesitation in lending credence to the evidence of prosecution witnesses that the accused was using the system in which the Western Union Money Transfer document was printed out. Likewise, the other documents were printed out from the email address supplied by the accused. Therefore, the said documents Exhibit 'B' and 'C' series of the accused were found in possession of the accused person. He was exercising dominion over them. On whether the accused has attempted to defraud the unsuspecting recipients, the evidence of prosecution witnesses is imperative as there was a physical act by the accused which was proximate to the complete offence. These acts would have been completed but for the interruption by the EFCC operatives… the facts that the contents of Exhibits 'B' and 'C' series are incorrect imply the fraudulent element… on the strength of this corroborative evidence, the prosecution have proved its case beyond reasonable doubt against the

[409] Unreported Suite No. FHC/KD/73C/2008. Judgment delivered on June 1, 2012

> accused person. He is accordingly found guilty on all the six counts charge…

Also, in *FRN vs. Emejuru Prince Patrick*[410] *(aka Patterson)*, the accused person was found in possession of electronic mails entitled "Hello my love" and "My Dear" wherein he sent as Patterson to Celia Guzman and one Oksana Navia of Spain and Russia respectively. The accused expressed interest in having relationship with both Celia Guzman and Oksana and he claimed to be in a position of getting a job for the said Oksana in the United Kingdom which the accused knew to be false and the same was with intent to defraud and which acts constitute an offence under section 6 of the *AFFA, 2006* and punishable under section 1(3) of the same.

At the trial, the prosecution called a sole witness, one Chukwunonso Okoro, an operative of the EFCC attached to the Advance Fee Fraud Unit in Lagos. The witness tendered the computer printout documents and the extra judicial statement of the accused which were admitted as Exhibits 'A' and 'B' respectively. The evidence of the prosecution was that sequel to a report of internet fraud perpetrated at cyber cafés across the country, he arrested the accused person at UC Network Cyber Café situate at University Road, Nsukka, Enugu State on the 1st day of April, 2008. That he printed out five (5) electronic mails contained in the accused sent items folder. The documents were as follows:

i. Document the accused sent to a woman call Anna with email address anytka28@yandex.rh entitled "Dearest Love."

ii. Document sent to a woman called Marina with email address – bepest04ek@yahoo.com entitled "My dear."

iii. Document sent to a Russian woman called Oksana with email address – lesenya@ranygler.rh entitled "Hello my love."

iv. Document sent to another Russian woman called Ekaterina777@yahoo.com entitled "Hi Honey."

v. Document sent to a Spanish woman called Celia Guzman whose email address is cguzman364@hotmail.com entitled "Hello My Love."

[410] Unreported Suit No. FHC/KD/119C/2008. Judgment delivered on July 25, 2011

After printing the documents, the accused endorsed each stating that the documents belonged to him and that they were printed from his mail box which is pattersonwoods@yahoo.com and that same were printed in his presence.

The issue for consideration in the case was whether or not the prosecution has proved the guilt of the accused person beyond reasonable doubt. The court held while convicting and sentencing the accused person to three (3) years imprisonment with effect from the date of his arrest, that:

> ...the offence of obtaining property by false pretences… could be committed by oral communication or in writing or even by conduct of the accused person. However, an honest belief in the truth of the statement on the part of the accused which later turns out to be false cannot find a conviction as false pretence… in the case at hand, the accused had in Exhibit 'B' admitted ownership of the email address pattersonwoods@yahoo.com to which Exhibit 'A' series were found and that he represented to the recipients that he was living in the United Kingdom. The entire story concerning the accused is totally false and thus the accused had made the false pretence to the said recipients… even though, there was no money or financial request in Exhibit 'A' series, there was indeed an intention on the part of the accused to create a relationship by means of deceit as the accused represented himself to be a contractor living in the United Kingdom which is false…

It is observed that the cases of *FRN vs. Churchill Joshua Essien (Alias Michelle Cole), and FRN vs. Emejuru Prince Patrick (aka Patterson) (supra)* are some of the rare cases were conviction for the offences of possession of documents containing false pretences, possession of electronic mails and attempts to obtain property by false pretences were secured after the whole trial process. Most of the other convictions were obtained by way of plea bargain between the prosecution and the accused counsel. For example, in *FRN vs. Iriobekhai Jude Collins*,[411] the accused stood trial on an amended charge of possession of fraudulent documents with intent to defraud contrary to section 6 and 8 of the *AFFA 2006* and punishable under the same Act. The accused Iriobekhai Jude Collins (m) aka "Natasha Williams" on or about the 9th day of April, 2008 at Mab Cyber Café, Abeokuta, Ogun State was found in possession of fraudulent documents headed; "Amateur Match, the Sexiest Adult

[411] Unreported Suit No. FHC/KD/158C/2008. Judgment delivered on February 15, 2010.

Dating Community," "Windows Live Hotmail" and attachment from the mail box titled "Your Account Login Information," containing information which the accused knew to be false.

On 15th February, 2010 when the case came up for continuation of trial, counsel to the accused, Olugbenga E. Oguniran Esq informed the court that the accused person has decided to change his plea from not guilty to guilty and Dalyop E. Vou Esq of counsel for the prosecution not opposing. The court convicted and sentenced the accused person to seven (7) years on each count. Meaning the accused was sentenced to forty-nine (49) years imprisonment. However, the sentence was to run concurrently from the first date of his arrest being 9th April, 2008. At best, the accused will serve for 5 years imprisonment.

Likewise, in *FRN vs. Prince Onyechere*,[412] the accused person under the false pretence that he was Dr. Joseph Sanusi, the former Central Bank of Nigeria Governor with intent to defraud obtained the sum of $1,800 and $300 Dollars from one Lafon Rene, a French citizen and Mrs Theresa Kanfman of California, U.S.A. respectively thereby committed an offence contrary to section 1(1) (a) *AFFA 2006* and punishable under subsection 1(3) of the Act.

On 16th December, 2009, H. M. Osuwa Esq. counsel for the accused person informed the court that the accused desires to change his plea from not guilty to guilty plea and J. Bwala Esq. of the prosecution not opposing. The court convicted and sentenced the accused to seven (7) years imprisonment on each count of the charge with effect from the day of his arrest being 5th April, 2008. The sentence was to run concurrently.

(f) Electronic Telecommunication Offences, etc

Section 12(1) of the *AFFA 2006* imposes a duty on any person or entity providing an electronic communication service or remote computing service by email or any other form to obtain the names and address of their customers or subscribers. Any customer or subscriber who fails to furnish the information specified above or with intent to deceive, supplies false

[412] Unreported Suit No. FHC/KD/93C/2008. Judgement delivered on December 16, 2009.

information or conceals or disguises the information required under the section commits an offence and is liable on conviction to imprisonment for a term not less than 3 years or a fine of N100,000.[413] The punishment for any person or entity providing electronic communication service or remote computing service by e-mail or any other form, who fails to comply with the provisions of the Act is a fine of N100,000 and the forfeiture of the equipment or facility used in providing the service.[414]

Section 13 of the Act imposes a duty on Telecommunication and Internet Service Providers and Internet Café to maintain register with the EFCC and maintain a register of fixed line customers which shall be liable to inspection by any authorised officer of the commission. There is also a duty on Global System of Mobile Communication (GSM) or non-fixed line service providers to submit on demand to the commission such data and information as are necessary or expedient for giving full effect to the performance of the function of the commission under the Act.

In *FRN vs. Nnachi Ephraim*,[415] the accused person was charged for failure to register Primegate Cyber Café, (No. 1 Okpara Street, Abakaliki Layout, Ebonyi State) with the Economic and Financial Crimes Commission thereby committing an offence contrary to section 13(1) (a) and punishable under section 13(5) (c) of the *AFFA 2006*. At the trial, both the prosecution and the defence called one witness each and tendered exhibits. The case of the prosecution was that the accused who identified himself as the manager of the cyber café and had been operating the café since 2004 did not register with the EFCC in violation of the Implementation Guidelines for Cyber Café Owners, Private Telephone Operators and the extant laws.

The accused contended during trial that Primegate Cyber Café was taken over by Artifice Colony located in the same address, which was registered with the EFCC with serial No. 737 on Cyber Café Registration. That the offence with which the accused was charged is

[413] Section 12(2) of the Act.
[414] Section 12(3) of the Act.
[415] Unreported Suit No. FHC/KD/95C/2008. Judgment delivered on March 19, 2010.

not a strict liability offence, as such the prosecution must prove its case beyond reasonable doubt, that:

i. that the accused is a person in the management of the premise being used as an internet café;

ii. the internet café is not registered with the EFCC;

iii. the accused knows or ought to know that he should be registered with the EFCC; and

iv. the failure to register with the EFCC is with intent to conceal or disguise the nature of the business.

The accused further contended that in proof of the allegation, the prosecution relied on sign boards at the major road and another at the premises bearing the name Primegate Cyber Café. That the accused had by documentary evidence shown that the actual cyber café operating at No. 1 Okpara Street, Abakaliki was Artifice Colony Nigeria Ltd., and not Primegate. That the mere fact that sign boards were mounted is not a sufficient proof of the requirement that the premises was being used as an internet café by Primegate which was not registered with the EFCC.

Convicting the accused for the offence charged, the court held that:

> Parties in this case are at *ad idem* that the accused was manager at Primagate Cyber Café situate at No. 1, Okpara Street, Abakaliki, Ebonyi State which cyber café was neve registered with the EFCC as evidenced in the testimonies of both the Prosecution and Defence witness as well as Exhibits 'B' and 'C'. The only contention is whether as at the 4th of April 2008 when the EFCC visited Primagate Cyber Café at No. 1 Okpara Street, Abakaliki, the cyber café has ceased to exist. Put differently, whether Artifice Colony Nigeria Ltd has effectively taken over the operation of the Primegate Technologies as at the time of the visit by the operatives of the EFCC. The evidence of the prosecution was that on their visit on the 4th day of April, 2008, the sign boards of Primegate were conspicuously place at the entrance of the café and also at the main road. The evidence of the Defence is that the mere fact that sign boards were mounted as not sufficient proof that the premises was being used was an internet café called Primegate Cyber Café which was not registered with EFCC… it is imperative to state that the provision of section 13(1) of the *AFFA* under which the accused was charged deals with duties of Telecommunication and Internet Service Providers and Internet Cafés. It makes it mandatory for those service providers either as an individual or an entity to, including the owner or person in the management of any premises used as a telephone or internet café to have same registered with the EFCC. Failure of which

> constitute an offence punishable under subsection (5) and (6) of section 13 of the Act. In the instant case, the evidence is overwhelming that the accused is the manager of a cyber café (Primegate) which did not register with EFCC. It is beyond argument at least from the accused own extra judicial statement that he administers or supervise the *AFFA*irs of the said cyber café since January 2008. It is settled that proof beyond reasonable doubt is attained when the evidence is so strong against the accused as to leave only a remote probability in his favour… on the strength of the above and considering the credible evidence placed before the court by the prosecution, they have in my view proved the allegation contained on the charge in this case beyond reasonable doubt against the accused person… the accused is accordingly found guilty as charged...

However, in *FRN vs. Maduka Nnamdi Stanley,*[416] the accused, a civil engineering student of University of Port Harcourt, stood trial on one count charge of failure to register the internet café which he manages with the EFCC contrary to section 13(1) (a) and punishable under section 13(5) (c) of the *AFFA 2006*. The accused pleaded not guilty to the charge. At the trial, the prosecution called one witness and tendered two exhibits marked as Exhibits 'A' and 'B' (List of Registered Cyber Cafes and Implementation Guidelines) respectively. The accused testified in his own defence and tendered Exhibits 'C' and 'C1' namely Notification of Registration and Website Registration Problem respectively.

The evidence of the prosecution was that on 30th March, 2008 they received an intelligence report of cybercrimes activities at Digital Connect Store Internet Café located at No. 8 Hill View, Independence Layout, Enugu State. The EFCC operatives went to the said cyber café and arrested the network manager and took some computers to the Enugu Zonal Office of the EFCC. Later on 21st April, 2008, the accused person came to the Zonal Office and identified himself as the manager of the café. Their investigation revealed that the cyber café was not registered with the EFCC. Under cross examination, the prosecution witness said he was aware that the accused was an employee at the cyber café. He did not know whether the café is now registered with the EFCC.

The accused contended in his defence that in March, 2008 his cousin who resides in Florida, U.S.A. called to inform him that his cyber café at No. 8 Hill View, Independence

[416] Unreported Suit No. FHC/KD/112C/2008. Judgment delivered on February 19, 2010.

Layout, Enugu was raided by the EFCC. That as a result, the Network Technician was arrested and that he should go down to Enugu and find out. He went to Enugu Zonal Office of the EFCC and demanded to see the said Technician but was eventually arrested while the said Technician was subsequently released on bail. That some EFCC staff told him that the café was not registered whereupon he promptly notified his cousin who insisted that same was duly registered. His cousin sent him letters (Exhibits 'C' and 'C1') to prove that the café was registered. That he could not have been the manager of the said café being a student of civil engineering, University of Port Harcourt while the café is located at Enugu. That he has never been to the cyber café except on this occasion.

Discharging and acquitting the accused person, the court held that:

> … In the instant case, the accused was alleged to be the owner of the Digital Connect Store Internet Café and that being the manager, he has failed to register same with the EFCC. The prosecution sole witness testified that the accused presented himself to the EFCC staff as the Zonal Office as the owner of the said cyber café. It is not in doubt that by Exhibit 'B', the Implementation Guidelines, all Internet Service Providers and cyber cafes are required to register with the Corporate Affairs Commission (CAC) and EFCC. Also, on the strength of the list of the registered cyber cafes, in Exhibit 'A', Digital Connect Store Internet Café was not on the list which presupposes that it was not so registered as at the material date… it is not enough in a charge of this nature to establish that the cyber café in question was not registered with EFCC without disclosing the person on whom that responsibility rest. The responsibility going by the letters of the provisions of section 13(1) of the *AFFA 2006* is vested on the owner or manager of the cyber café or Internet Service Provider… the word 'ownership' generally connotes the totality or bundle of rights of the owner over and above every other person on a thing… the fundamental question is that has the prosecution established that the accused has a complete or total right over Digital Connect Store Internet Café? Is there any scintilla of evidence to show that the accused supervise the *AFFA*irs of the internet café in question? The answer is definitely no… the evidence of PWI is not sufficiently probative of the offence with which the accused is charged. That being the position, the prosecution cannot in my view be said to have proved its case beyond reasonable doubt against the accused…

Also in *FRN vs. Imo Idiong (supra*), it was alleged that the accused failed to register the premises, which he knowingly and wilfully permits to be used in sending scam mails, that

is, Stallionet Cyber Café at No. 59 Etta Agbor Road, Calabar and thereby committed an offence under section 13(5) (a) (b) of the *AFFA 2006* among other charges.

The accused in his defence stated that it was not his responsibility to register the café with the EFCC. Under cross examination, he denied being the manager of the cyber café. The owner is one Mr. Victor Akpan which the prosecution did not say anything about him. Relying chiefly on section 13(1) of the *AFFA* and sections 37 and 65 of the Companies and Allied Matters Act (CAMA) to the effect liability for any offence committed by a company cannot be visited on its employee, the court held that:

> The evidence on registration or non-registration with the EFCC is very scanty. However, the duty of securing registration with the EFCC within the contemplation of section 13(1) (a) of the Act depend solely on the nature of the enterprise concerned… By Exhibit 'E', 'B' and 'C' Stallionet Cyber Café is a limited liability company and hence the responsibility rest squarely on the said entity. In the light of the foregoing, the prosecution in my view has not discharged the evidential burden of proving its case beyond reasonable doubt against the accused person…

3.2.3 The Criminal Law of Lagos State, 2011

The *Criminal Law of Lagos State* No. 11, 2011[417] provides for computer and electronic data misuse offences.[418] The law makes provision for offences of unauthorized access to computer material; unauthorized access with intent to commit or facilitate commission of further offences; unauthorized modification of computer data; unauthorized modification of computer data with intent; and electronic data of public record.

The Lagos State law on computer and electronic data misuse offences is a replication and 'copy-cat' of the United Kingdom's (UK) Computer Misuse Act, 1990, which provisions has been examined under municipal global best practices on cybercrime. To the best of the knowledge of this researcher, there is no conviction recorded by the Lagos State courts on the provisions of this law.

[417] Officially titled: A Law to Provide Rules on Criminal Conduct, Regulate Public Order and for Connected Purposes.
[418] Chapter 41: Sections 385-389 of the Law.

3.3 An Overview of Developments of Legislation and Cyber Security Policy for Combating Cybercrimes in Nigeria.

This part of the study makes an overview of the recent developments of legislation on cybercrimes in Nigeria with the view to establish the efforts and/or attempt made by Nigerian governments to enact anti-cybercrimes laws and cyber security in Nigeria.

3.3.1 Computer Security and Critical Infrastructure Protection Bill 2005

The Nigerian government in 2005 sponsored the Computer Security and Critical Infrastructure Protection Bill[419] with the view to secure computer systems, networks and protect critical infrastructure in Nigeria by prohibiting certain computer based activities and to impose liability for global crimes committed over the internet. The Cybercrimes Bill requires all service providers (Telephone and Internet) to record all traffic and subscriber information for such period as specified by the president and to release the information to any law enforcement agency on the production of a warrant.[420] Such information may only be used for legitimate purposes as determined by a court of competent jurisdiction or other lawful authority.[421]

Part II of the Bill provides for the offences of unlawful access,[422] disclosure of access,[423] fraudulent electronic mail messages,[424] computer forgery,[425] computer fraud,[426] interference with computer system with the view to modify, destroy any data, program and software held in the computer system,[427] misuse of devices,[428] denial of service,[429] unlawful access code, identity theft,[430] interception of communication,[431] duty of service providers,[432]

[419] Officially titled: "A Bill for an Act to Secure Computer Systems and Networks and Protect Critical Information Infrastructure in Nigeria by Prohibiting certain undesirable Computer-Fraud based Activities and for Matters connected therewith". See www.nassnig.org/nars/legislation.php?.id... See also www.cybercrimes.gove.ng/site/index.php? Accessed on September 12, 2013
[420] Section 12 of the Bill
[421] Section 12 (3), *Ibid.*
[422] Section 3, *Ibid.*
[423] Section 4, *Ibid.*
[424] Section 5, *Ibid.*
[425] Section 6, *Ibid.*
[426] Section 7, *Ibid.*
[427] Section 8, *Ibid.*
[428] Section 9, *Ibid.*
[429] Section 10, *Ibid.*
[430] Section 11, *Ibid.*

cyber squatting,[433] cyber terrorism,[434] intellectual property rights violation using computer,[435] using computer for unlawful sexual purposes,[436] attempt, conspiracy and abetment,[437] and tampering with computer evidence.[438] The punishment for the offences are from a maximum term of imprisonment for 25 years and fine between N15 to N20 million naira or both.[439]

However, the Bill did not provide for independent monitoring of the law enforcement agencies carrying out the provisions, nor does the Bill define "law enforcement agency," "lawful authority," "critical information infrastructure," or what constitute "personal data." The Bill may conflict with section 37 of the *Constitution of the Federal Republic of Nigeria*, 1999 which guarantees the privacy of citizens including their homes, telephone conversations and telegraphic communications.[440] The where about or status of this Bill cannot be ascertained by this researcher, perhaps it is abandoned by its sponsors.

3.3.2 Cyber Security and Data Protection Agency Bill 2008

The House of Representatives Committee on Drugs, Narcotics and Financial Crimes in Nigeria held a public hearing on the Draft Legislation on Cyber Security and Data Protection Agency Bill[441] on Wednesday 8th July, 2009.[442] The Bill was sponsored by Hon. Etim Bassey and it proposes to establish a Cyber Security and Information Protection Agency which will be responsible for enforcement of the provisions of the Bill; investigation of cybercrimes; promoting and adopting anti-cybercrimes measures in all facets of the security; investigating all reported cases of cybercrimes and ensuring the prosecution of individuals,

---

[431] Section 13, *Ibid.*
[432] Section 14, *Ibid.*
[433] Section 15, *Ibid.*
[434] Section 16, *Ibid.*
[435] Section 17, *Ibid.*
[436] Section 18, *Ibid.*
[437] Section 19, *Ibid.*
[438] Section 28, *Ibid.*
[439] See for example section 22 of the Bill for the offence against critical information infrastructure.
[440] The exception to section 37 of the *CFRN* 1999 can be seen under section 45 of the *CFRN* 1999. It provides for restriction on and derogation from fundamental rights in the interest of defence, public safety, public order, public morality, public health or for the purpose of protecting the rights and freedom of other persons.
[441] Officially titled: "A Bill for an Act to provide for the establishment of the Cyber Security and Information Protection Agency charged with the responsibility to secure Computer Systems and Networks and liaison with the relevant Law Enforcement Agency for the enforcement of Cybercrimes Law and for related matters".
[442] Retrieved from www.jidaw.com/security/.../nig. on January 12, 2012 at 10.12pm

corporate organization involved in cybercrimes; registration and regulation of service providers in Nigeria with the views to monitor their activities; creating public awareness on the nature and forms of cybercrimes.[443]

The Agency shall consist of the Chairman who shall be the National Security Adviser and Executive Vice Chairman and four other members appointed by the President subject to confirmation of the Senate. The Bill is divided into several sections identifying various types of cybercrimes and prescribing measures for offenders. For example the offences of unauthorised disclosure of access, access to program data or data base held in computer for unlawful purpose or gain, the conviction attracts not less than 3years terms of imprisonment or N500,000 (five hundred thousand naira) fine.[444] It is an offence under the Bill to send fraudulent electronic email message and spamming with intent to defraud. The punishment is imprisonment for not less than 3years or N500,000 (five hundred thousand naira) fine or both.[445]

It is also an offence to misuse devices, codes to overcome information security measures.[446] The punishment for the offence of identity fraud, that is, where a person assumes the identity of another person with intention to defraud or deceive is not less than 3years or a fine of not less than N500,000 (five hundred thousand naira) fine or both.[447]

Cyber terrorism is a major section of the Bill. The Bill provides that any person, group or organization that intentionally accesses any computer or network for purposes of terrorism commits an offence and shall be liable on conviction to not less than N10million fine or a term of imprisonment for not less than 20years or both.[448]

One of the critical components of the Bill is the prescribed responsibilities of service providers. Every service provider shall keep all traffic, subscriber information on its

[443] Section 1 of the Bill
[444] Sections 7 and 8, *Ibid.*
[445] Sections 9 and 10, *Ibid.*
[446] Section 12, *Ibid.*
[447] Section 14, *Ibid.*
[448] Section 20, *Ibid.*

computer or network for such period of time as the agency may require.[449] The Bill has a section on pornography in the electronic environment. It identifies several threats to children using computers and makes provision for their protection.[450] Offences against critical information infrastructure are identified and penalties are prescribed for offenders.[451] The punishment under section 26 of the Bill shall be a fine of not less than N15million or imprisonment for a term not less than 25years or both. Where the offence resulted in death, the offender shall be liable on conviction to imprisonment for life with no option of fine.[452]

The Bill makes it possible to use electronic evidence as primary evidence in courts. It states that: "Notwithstanding anything contained in any enactment or law in Nigeria, information contained in any computer which is printed out on paper, stored, recorded or copied on any media shall be deemed to be primary evidence under this Bill."[453]

The power to initiate criminal proceedings is vested on the proposed Agency.[454] The Federal High Court or State High Court shall have jurisdiction to try offenders under the Bill.[455] Nothing in the Bill shall preclude the institution of a civil suit against a person liable under the Bill by any person interested.[456] The Bill contains information on powers of authorized officer to search and arrest,[457] obstruction of law enforcement officer,[458] tampering with computer evidence,[459] forfeiture of compensation,[460] attempt, conspiracy and abetment.[461] Like its predecessor, this Bill appears to be abandoned by its sponsors.

3.3.3 Electronic Fraud (Prohibition) Bill 2008

The attempt by the Senate to combat the rising scourge of cybercrimes in Nigeria was made by Senator Ayo Arise who sponsored a Bill entitled "A Bill for an Act to provide for

[449] Section 15, *Ibid.*
[450] Section 22, *Ibid.*
[451] Section 26, *Ibid.*
[452] Section 26 (3), *Ibid.*
[453] Section 31, *Ibid.*
[454] Section 33, *Ibid.*
[455] Section 28, *Ibid.*
[456] Section 27, *Ibid.*
[457] Section 29, *Ibid.*
[458] Section 30, *Ibid.*
[459] Section 32, *Ibid.*
[460] Section 34, *Ibid.*
[461] Section 23, *Ibid.*

the Prohibition of Electronic Fraud in all Electronic Transactions in Nigeria and for other Related Matters." The Bill provides for 7years jail term for, and in case of second conviction, a 14years jail term for the offence of intercepting electronic messages. In this regard, the Bill states that:

> "Any person who unlawfully destroys, or aborts any electronic mails or procession through which money and for valuable information is being conveyed, is guilty of a felony and is liable to imprisonment for 7years and upon second conviction shall be liable to 14 years imprisonment."[462]

Also, the stealing and forging of electronic cards, credit card, debit card, smart card, ATM card or any other related electronic payment system attracts 7years imprisonment.[463] Section 25 of the Bill prohibits e-banking and e-finance fraud. It states that:

> "Any person who being employed by or under the authority of any banking or other financial institutions who either directly or indirectly unlawfully diverts electronic mails, with the intent to commit or omit any act is to benefit directly or indirectly, is liable to imprisonment for 7years or a fine of N5million or both."

It is also a crime under the Bill to spread virus or infect IT infrastructure with hostile and dangerous software programs with intent to damage or manipulate a computer record or data belonging to the Government, Educational, Research or any financial institution. The punishment is 7year jail term or N5million fine.[464] Hoaxes capable of threatening or affecting the security of the country or that is capable of inciting the general public against the government attracts 7years imprisonment or N5million fine or both.[465]

The offence of e-pornography is provided under section 16(2) of the Bill. It provides that; "Any person who, knowingly sends pornographic images to another computer by way of unsolicited distribution shall be guilty of a misdemeanour and upon conviction shall be sentenced to 1year imprisonment or a fine of N250,000 or both." The Bill has reportedly gone through the second reading in the Senate and was referred to its Committee on

[462] Sections 7-8, *Ibid.*
[463] Sections 19-21, *Ibid.*
[464] Section 16(1), *Ibid.*
[465] Section 16(3 , *Ibid.*

Judiciary, Human Rights and Legal Matters when as usual with the Nigerian political class, it was abandoned.[466] However, parts of its provisions appear to have incorporated in the recently assented Cybercrimes Act, 2015.

3.3.4 Cyber Security Bill, 2011

The *Cyber Security Bill, 2011* aims at providing effective, unified and comprehensive legal framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. The Bill is intended at enhancing cyber security, protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.[467]

Part II of the Bill provides for the offences and penalties under the Bills such as unlawful access to a computer, unauthorized disclosure of access code; data forgery; computer fraud; system interference; misuse of devices; denial of service; identity theft and impersonation; child pornography; record retention and preservation; unlawful interception; cyber squatting; cyber terrorism; failure of service providers to perform certain duties; racist and xenophobic offences; attempt, conspiracy and abetment; and corporate liability.[468]

Parts III and IV of the Bill provide for the security and protection of critical information infrastructure and aspects of search, arrest and prosecution respectively. While Part V of the Bill provides for international cooperation covering the issues of extradition; mutual assistance request; expedited preservation of data, evidence pursuant to a request and form of request.

It is submitted that the provisions of the *Cyber Security Bill, 2011* met the requirements of the international legal instrument and standard such as the Council of Europe's Convention on Cybercrimes, 2001.[469]

---

[466] Agbajor, C. (2012) 'Senate set to Combat Cybercrimes.' Retrieved from www.Nigeriaobservernews.com January 10, at 10.38pm

[467] Part I of the *Cyber security Bill, 2011.* For general discussion on the *Cyber Security Bill, 2011,* see George-Maria Tyendezwa, T. G. (nd) 'Legislation on Cybercrime in Nigeria: Imperatives and Challenges.' Retrieved from www.ncc.gov.ng... on March 30, 2015 at 11.00pm

[468] Sections 2 – 18 of the Bill.

[469] George-Maria Tyendezwa, T. G. (nd) *Op.cit.,* p.5.

3.3.5 Nigerian Cybercrimes Bill, 2013

The *Cybercrimes Bill, 2013*[470] seeks to provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection and punishment of cybercrimes in Nigeria; ensure the protection of critical national information infrastructure; and promotes cyber security and the protection of computer systems and networks, electronic communications; data and computer programs, intellectual property and privacy rights.[471]

The Bill is divided into eight parts. Part I provides for the objectives and application of the Bill. Part II deals with the protection of critical information infrastructure. Part III provides for the offences and penalties. Part IV provides for duties of service providers, while Part V provides for aspect of administration and enforcement. In Part VI, the power of search, arrest and prosecution is dealt with. Part VII provides for jurisdiction and international cooperation. Part VIII is the miscellaneous aspect. The Act applies throughout the Federal Republic of Nigeria.[472]

Part III of the Cybercrime Bill, 2013 provides for the offences and penalties under the law. The offences include: offences against critical national information infrastructure,[473] unlawful access to a computer,[474] unlawful interception of communication,[475] unauthorised modification of computer data,[476] system interference,[477] misuse of devices,[478] computer related forgery,[479] computer related fraud,[480] identity theft and impersonation,[481] child pornography and related offences,[482] cyber stalking,[483] cyber squatting,[484] cyber terrorism,[485]

[470] Officially titled:"A Bill for an Act to provide for the Prohibition, Prevention, Detection, Response and Prosecution of Cybercrimes and for other Related Matters, 2013"
[471] Section 1 (a), (b) and (c) of the Bill.
[472] Section 2, *Ibid.*
[473] Section 5, *Ibid.*
[474] Section 6, *Ibid.*
[475] Section 7, *Ibid.*
[476] Section 8, *Ibid.*
[477] Section 9, *Ibid.*
[478] Section 10, *Ibid.*
[479] Section 11, *Ibid.*
[480] Section 12, *Ibid.*
[481] Section 13, *Ibid.*
[482] Section 14, *Ibid.*

racist or xenophobic offences,[486] attempt, conspiracy, aiding and abetting,[487] corporate liability,[488] duties of service providers,[489] interception of electronic communications,[490] and failure of service provider to perform certain duties.[491]

The provisions of the *Cybercrimes Bill, 2013* was substantially incorporated in the enacted *Cybercrimes Act, 2015*.

3.4 Cybercrimes (Prohibition, Prevention, etc) Act, 2015

The Act[492] provide for 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 promotes cybersecurity and protection of computer systems and networks, electronic communication, data and computer programme, intellectual property and privacy right.[493]

The Act is divided into 6 parts and 59 sections. Part I provides for the object and application of the Act. Part II deals with protection of critical national information infrastructure. Part III provides for the offences and penalties, while Part IV deals with duties of financial institutions. Part V is concerned with administration and enforcement, while Part VI covers arrest, search and seizure.

The President may, on the recommendation of the National Security Adviser, by order published in the Federal Gazette, designate certain computer systems, and/or networks, whether physical or virtual, and/or the computer programmes, computer data and/or traffic data vital to this country that the incapacity or destruction of, or interference with such system and asset would have a debilitating impact on security, national or economic security,

---

[483] Section 15, *Ibid.*
[484] Section 16, *Ibid.*
[485] Section 17, *Ibid.*
[486] Section 18, *Ibid.*
[487] Section 19, *Ibid.*
[488] Section 20, *Ibid.*
[489] Section 21, *Ibid.*
[490] Section 22, *Ibid.*
[491] Section 23, *Ibid.*
[492] Officially titled 'An Act to provide for the Prohibition, Prevention, Detection, Response, Investigation and Prosecution of Cybercrimes and for Other Related Matters, 2015. Assented by the President in May, 2015.
[493] Section 1 of the Cybercrimes Act, 2015.

national public health and safety, or any combination of those matters as constituting critical national information infrastructure.[494] The Presidential order made under subsection 1 may prescribe minimum standard, guidelines, rules or procedure in respect of:

(a) the protection or preservation of critical information infrastructures;

(b) the general management of critical information infrastructure;

(c) access to, transfer and control of data in any critical information infrastructure;

(d) infrastructural or procedural rules and requirement for securing the integrity and authenticity of data or information contained in any critical national information infrastructure;

(e) the storage or coordinating of data or information regarded critical national information infrastructure;

(f) recovery plans in the event of disaster or loss of the critical national information infrastructure or any parts of it; and

(g) any other matter required for the adequate protection, management and control of data and other resources in any critical national information infrastructure.[495]

The Act provides for the offences against critical national information infrastructure,[496] unlawful access to computer,[497] electronic fraud/online fraud using cyber cafe,[498] system interference,[499] intercepting electronic messages/e-mails electronic money transfers,[500] tampering with critical infrastructures,[501] wilful misdirection of electronic messages,[502] unlawful interception,[503] computer related forgery,[504] computer related fraud,[505] theft of electronic devices,[506] unauthorised modification of computer system, data/system interference,[507] fraudulent misrepresentation of electronic signature,[508] cyber terrorism,[509]

[494] Section 3(1), *Ibid*.
[495] Sections 3(1) and (2) (a-g), *Ibid.*
[496] Section 5, *Ibid.*
[497] Section 6, *Ibid.*
[498] Section 7, *Ibid.*
[499] Section 8, *Ibid.*
[500] Section 9, *Ibid.*
[501] Section 10, *Ibid.*
[502] Section 11, *Ibid.*
[503] Section 12, *Ibid.*
[504] Section 13, *Ibid.*
[505] Section 14, *Ibid.*
[506] Section 15, *Ibid.*
[507] Section 16, *Ibid.*
[508] Section 17, *Ibid.*

financial institutions, posting and authorised options,[510] fraudulent issuance of e-instruction,[511] reporting of cyber threat,[512] identity theft and impersonation,[513] child pornography and related offences,[514] cyber stalking,[515] cyber squatting,[516] racist or xenophobic offences,[517] attempt, conspiracy, aiding and abetting,[518] importation and fabrication of e-tools,[519] breach of confidence and fabrication of e-tools,[520] manipulation of ATM/Point of Sales (POS) terminals,[521] employees responsibility,[522] phishing, spamming, spread of computer virus,[523] electronic cards related fraud,[524] dealing in card of another,[525] purchase or sale of card of another,[526] use of fraudulent device or attached e-mails and websites,[527] duties of financial institutions,[528] and duties of service providers.[529] The penalties under Act ranges between 1-15 years imprisonment, life imprisonment and payment of fine between N250,000 – N25,000,000.

It is the view that most of the provisions of the crimes provided under the *Cybercrimes Act, 2015* may actually be difficult to enforce. Giving the fact that the nature of the evidence required in relation to cybercrimes are quite distinct from those of traditional crimes. These types of information are fragile and can be easily lost or damaged.[530] In cases of child pornography for instance, it may be difficult to prove that a person downloaded the

---

[509] Section 18, *Ibid.*
[510] Section 19, *Ibid.*
[511] Section 20, *Ibid.*
[512] Section 21, *Ibid.*
[513] Section 22, *Ibid.*
[514] Section 23, *Ibid.*
[515] Section 24, *Ibid.*
[516] Section 25, *Ibid.*
[517] Section 26, *Ibid.*
[518] Section 27, *Ibid.*
[519] Section 28, *Ibid.*
[520] Section 29, *Ibid.*
[521] Section 30, *Ibid.*
[522] Section 31, *Ibid.*
[523] Section 32, *Ibid.*
[524] Section 33, *Ibid.*
[525] Section 34, *Ibid.*
[526] Section 35, *Ibid.*
[527] Section 36, *Ibid.*
[528] Section 37, *Ibid.*
[529] Section 38, *Ibid.*
[530] See Abdullahi, I. *et al* (2016) "Cybercrimes (Prohibition, Prevention, etc) Act, 2015: Issues and Challenges in Nigeria." Paper Presented at Nigeria Association of Law Teachers (NALT) Conference, Nasarawa State University, Keffi, p.14.

illegal material knowingly or intentionally since someone else can hack into a system and store data on its drive without the user's knowledge or permission.[531]

Section 37 of the *Cybercrimes Act,2015* provides for duties of financial institutions and it is to the effect that any financial institution that makes unauthorised debit on a customer's account shall upon written notification by the customer reverse such debit within 72 hours, failing which such financial institution shall be guilty of an offence and liable on conviction to restitution of the debit and a fine of N5,000,000.[532] In the case of *Dr Abiodun Olusanya vs Eco Bank Plc.*[533] The Plaintiff, a medical doctor sought among others, an order directing the Defendant to credit his account with the sum of N199,641.12 (One hundred and ninety-nine thousand, six hundred and forty one naira, twelve kobo) being the total sum of unauthorised withdrawals negligently allowed by the Defendant from the Plaintiff's account number 0730001010808 domiciled at the Defendant Bank; N1,000,000 (One million naira) general damages against the Defendant for its negligence conducts allowing such withdrawals from the Plaintiff's account and interest on the claimed at 2% per annum from March 30, 2009 till final payment of the sum claimed.

The Plaintiff's case was that in March 2009 his ATM card got stuck in the Access Bank ATM machine located at Ahmadu Bello University Teaching Hospital (ABUTH), Shika when he went to make withdrawals. Between March 29 and 31, 2009 a number of unauthorised withdrawals in the sum of N199,641.12 (One hundred and ninety-nine thousand, six hundred and forty one naira, twelve kobo) were made from his account with the Defendant. Not having an alert system then, the Plaintiff was not aware of the withdrawals until in May 2009 when he went to the Defendant bank to make withdrawals and he was told that he did not have the amount he wanted to withdraw in his account. Not satisfied, the Plaintiff requested for his statement of account from the Defendant and he discovered the

[531] *Ibid.*
[532] Section 37(3), *Ibid.*
[533] Unreported, Suit No. KDH/Z/182/2009. Judgment delivered by Her Lordship M.L. Mohammed on March 20, 2014

unauthorised withdrawals made from his account. On May 5, 2009, the Plaintiff wrote a complaint to the Defendant's Manager requesting for reversal of the unauthorised withdrawals. The Defendant did not reply the Plaintiff's letter of complaint. The Plaintiff though our law firm wrote the Defendant, demanding a reversal of the unauthorised withdrawal. The Defendant replied that it was investigating the complaint and will get back to us but it never did.

In its defence, the Defendant alleged that the Plaintiff was not only fraudulent but a gold digger. That the Plaintiff made the withdrawals himself or through his girlfriend or relations because only the plaintiff, his girlfriend or relations could know the Plaintiffs PIN number. That the Defendant was not liable for the Plaintiff's loss because the Plaintiff did not disclose his PIN number to any of the Defendant's staff. Besides, the withdrawals were made via Zenith Bank ATM located at ABUTH Shika as such the Defendant was not liable to the Plaintiff. The Plaintiff replied that he neither made the withdrawals nor his relations as he did not disclose his PIN number to anybody. He has been happily married with children four years before the date of the incidence. He did not have a girlfriend.

Under cross-examination, the defendant witness admitted that when they discovered that it was the Plaintiff, his girlfriend or relations that perpetrated the fraudulent withdrawals, they did not report the Plaintiff or the case to the police or any security agency for the purpose of investigation and possible prosecution. The Defendant witness also admitted that nowadays, it is possible to hack into a person's account details and make such withdrawals without the account holder's knowledge and or consent. That it is possible to withdraw money from another bank's ATM machine, yet the amount withdrawn will be from that person's account in the Defendant bank. That by entering a PIN code, a customer is communicating with his account in the Defendant bank.

The trial court entered judgement in favour of the Plaintiff, directing the Defendant to credit the Plaintiff's account with the sum withdrawn from the account; N50,000.00 (fifty thousand naira) general damages was awarded against the Defendant and interest of 10% per

annum from March 30, 2009 till the judgement sum is fully paid. The Defendant has appealed the judgement of the trial court to the Court of Appeal, Kaduna Division after paying the entire judgement sum to the Plaintiff following the execution and attachment of its movable properties.

The point being made here is that the Defendant Bank, through its employees had made fraudulent withdrawals from the Plaintiff's account and had refused to reverse such withdrawals despite several notifications. Had the *Cybercrimes Act, 2015* been enacted when the Plaintiff's cause of actions arose, the Plaintiff could have petitioned the Defendant to the relevant enforcement authority with the view to unravel and possibly prosecute the perpetrators of the fraudulent withdrawals from the Plaintiffs account with the Defendant. The Plaintiff did not report the Defendant to the police because he did not have confidence in police to diligently investigate and prosecute the case.

3.5 Nigeria's National Cybersecurity Policy and Strategy 2014

The Nigeria's National Cybersecurity Policy and Strategy 2014 are products of Inter-agency Committee[534] set up by the Office of the National Security Adviser (ONSA) with the view to chart a course towards an assured and trusted presence in Nigeria's cyberspace,[535] and to provide a cohesive road map initiatives and implementation mechanism for achieving the national vision on cybersecurity.[536]

The National Cybersecurity Policy sets out the strategic intent of the government in mitigating the country's cyber risk exposure by prioritizing the country's need while focusing on key areas, curtailing escalation of cyber threats that are inimical to the national security

[534] Members of the Inter-agency Committee and the National Cybersecurity Policy and Strategy comprised of Representatives of the Office of the National Security Adviser (ONSA), Nigerian Communications Commission, Federal Ministry of Communications Technology (FMOCT), Federal Ministry of Justice (FMOJ), Economic and Financial Crimes commission (EFCC), Galaxy Backbone Ltd, Nigeria Communications Satellite Commission, Central Bank of Nigeria (CBN), National Information Technology Development Agency (NITDA), Continental Project Affairs Associates among others. On December 23, 2014, the then National Security Adviser, Col. M. S. Dasuki (rtd) signed the National Cybersecurity Policy and Strategy documents.
[535] Para. 3.3 of the National Cybersecurity Policy.
[536] Para. 1.3 of the National Cybersecurity Strategy.

posture and the Nigerian economic well-being.[537] Some of the specific objectives of the National Cybersecurity Policy are: to facilitate an effective legal framework and governance mechanism for Nigeria's presence in cyberspace and cybersecurity echo system; to develop information security and control mechanism for the protection and safety of Nigeria's national critical information infrastructure and its associated economic infrastructures operating in cyberspace; to promote emergence of an appropriate legislative environment with respect to freedom of access to information, intellectual property, data protection and privacy right; to develop a framework for inter-agency collaboration on combating cybercrime and cybersecurity; to establish multi-stake holder partnership, cooperation and leadership advisory mechanism for information sharing, intelligence gathering and coordinated response among others.[538]

The Nigeria's Cybersecurity Strategy (NCSS) is the nation's strategy to provide a cohesive measure and strategic actions toward assuring security and protection of the country's presence in cyberspace, safeguarding critical information infrastructure, building and nurturing trusted cyber community.[539] The NCSS comprises of short, medium and long term mitigation strategies covering all national priorities, addressing the nation's cyber risk exposure, specific key cyber threats inimical to national interest such as cybercrime, cyber terrorism, cyber conflict, cyber espionage and child online abuse and exploitation.[540] These threats have significant capability to damage the integrity of the nation, disrupt critical information infrastructure operations, undermine government operations and national security.[541]

Within the global network of networks, there are critical structural flaws which can be exploited for criminal intents and purposes against the country to compromise the confidentiality, integrity, availability and accessibility of the nation's information systems

[537] See the executive summary of the National Cybersecurity Policy.
[538] Para. 3.3.2 of the National Cybersecurity Policy.
[539] Para. 1.1.1 of the National Cybersecurity Strategy.
[540] *Ibid.*, para. 1.1.2
[541] *Ibid.*, para.1.1.3

and critical information infrastructures. State and non state actors involved in cybercrimes are adequately equipped with sophisticated cyber tools to cause damage with unprecedented dimension. Thus, the security inclusion of cyberspace domain will help the country prepare and respond to security threats and address the country's weakness in digital vulnerability as well as strengthening Nigeria's ability to provide counter measures in partnership with other legitimate state and non state actors. This is the strategic rationale for the development of the National Cybersecurity Policy and the context within which the National Cybersecurity Strategy is articulated for national security readiness.[542]

3.6 Selected Municipal Legislation for Combating Cybercrimes

This part of the study examines the best practices of municipal laws of selected countries. This is done with the view to appreciate the development and progress made by such countries in combating cybercrimes and how such progress may influence the Nigerian experience.

3.6.1 The United Kingdom's (UK) Computer Misuse Act 1990

The *UK's Computer Misuse Act (CMA) 1990* is the first piece of legislation designed to specifically address computer misuse. The Act was a response to growing concern that existing legislation was inadequate for dealing with hackers. The *Computer Misuse Act* came into existence because legislation intended for other purposes did not always fit the particular facts before the court. This occurred in the case of *R. vs. Gold and Schifreen,*[543] Gold and Schifreen were hackers who gain unauthorised access to the Duke of Edinburgh's computer files contained in British Telecom Prestel Gold Network. They were convicted of committing an offence contrary to section 1 of the *Forgery and Counterfeiting Act* (FCA) 1981 for making a false instrument. On appeal, their convictions were quashed as the court said that the electronic impulses that formed the password could not be an instrument within the definition of section 8(1)(d) of the FCA.

[542] Para. 1.6, *Ibid.*
[543] (1988) 2 WLR 984; for detail analysis on the case of *R. vs. Gold & Schifreen*, see Bainbridge, D. I. (2008) *Introduction to Information Technology Law*. 6th Edition, Pearson Longman, England, pp.438-441

Although, in some cases, the prosecution succeeded in obtaining a conviction, for example, in *R. vs. Whitely,*[544] Whitely, a computer hacker was convicted of criminal damages. He gained unauthorised access to a computer network and altered data contained on disc in the system, thereby causing the computers in question to be shot down for periods of time.

As a result of the problem of prosecuting such cases, a Royal Commission was set up and following their recommendations, the *Computer Misuse Act* was enacted.[545] The Act makes provisions for securing computer material against unauthorised access or modification and for connected purposes. It sets out three computer offences, namely; unauthorised access to computer material, [546] unauthorised access with intent to commit other offence,[547] and unauthorised modification of computer material.[548]

The perceived problem with section 3 of the CMA has involved Denial of Service attacks and interference by authorised users of system.[549] Although section 3 of the CMA does not specifically refer to Denial of Service attacks of the type now possible, its lack of precision and technology neutral language appears to provide sufficient flexibility for such a case to be prosecuted.

3.6.2 The United Kingdom (UK) Fraud Act 2006

Like the Nigerian *Advance Fee Fraud Act 2006*, the *UK Fraud Act* was enacted in 2006 but it fully came into force on 15th January, 2007.[550] The Act deals with some deficiencies of the *Theft Act 1968* and *1978* especially when it comes to ICT fraud. It is now clear that 'phishing', obtaining information such as a person's bank account details by sending an email purporting to be from that person's bank is a criminal offence. This remains

[544] (1991) 1993 CAR 25 CA
[545] See ICF Legal Sub Group. Reform of the *Computer Misuse Act* 1990.
[546] Section 1 of the Act.
[547] Section 2, *Ibid.*
[548] Section 3, *Ibid.*
[549] Denial of Service attack is a malicious attack intended to disrupt information systems; it can be committed in many ways. It attempts to overload the web servers or ISPs with automatically generated messages. Other types of attack can include disrupting servers operating the Domain Name System (DNS) and attacks directed at routers.
[550] Bainbridge, D. I. (2008) *Op.cit.,* p.424

the case even if nothing further has been done with the information thus obtained or even before the email has been transmitted.[551] Section 1 of the Act creates three new forms of fraud namely:

(a) Fraud by False Representation

This fraud occurs where a person dishonestly makes a false representation, intending by making the representation to make a gain for himself or another or to cause loss to another or to expose another to a risk of loss. A representation may be as to fact or law, including representation as to the state of mind of the person making it or other person. It may be expressed or implied. A representation is 'false' if it is untrue or misleading and the person making it knows that it is or might be untrue or misleading. A representation is regarded as 'made' if it is submitted in any form to any system or device designed to receive, convey or respond to communications with or without human intervention. Thus, a representation by email to a computer or by Short Message Service (SMS) to a mobile phone is included. A representation will also be made where it is sent to an online bank with instruction to pay funds into another account.

Section 2 of the *Fraud Act 2006* is said to be wider than the old deception offences under sections 15 and 15A of the Theft Act 1968 which required the offender, by any deception to dishonestly obtain property belonging to another with the intention of permanently depriving the other of it. For breach of section 2 of the *Fraud Act 2006*, there is no need for the gain or loss to actually happen or it does happen, for it to be permanent.[552] The three forms of *mensrea* required for section 2 of the *Fraud Act 2006* are dishonesty, the intention by making the representation to make a gain or cause a loss and knowledge that the representation is untrue or misleading.

[551] *Ibid.*
[552] *Ibid.*, p. 425

(b) Fraud by Failing to Disclose Information

Under section 3 of the *Fraud Act 2006,* where a person dishonestly fails to disclose to another person information which he is under a legal duty to disclose and intends, by failing to disclose the information, to make gain for himself or another or to cause loss to another or to expose another to a risk of loss. The offence may be relevant in transactions between governmental institutions, and individuals or corporate bodies that can be conducted online. The offence may also be committed by a politician who dishonestly fails to disclose an interest in a company bidding or negotiating for a government contract.[553]

(c) Fraud by Abuse of Position

The offence under section 4 of the *Fraud Act 2006* occurs where a person dishonestly abuses a position which he is expected to safeguard, intending by that abuse to make a gain for himself or another or to cause loss to another or to expose another to a risk of loss. For example, where an employee of a software company uses his position to make unauthorised copies of his employer's software to sell for his benefit or where an employee sends an email containing confidential information belonging to the employer to a rival company, whether for his own personal gain or with the intention of causing his employer a loss. Section 1(3) of the *Fraud Act 2006* sets out the penalties for section 1 fraud which are: on summary conviction, imprisonment for a term not exceeding 2 months and/or fine, on conviction, on indictment, the imprisonment for a term not exceeding 10 years and/or fine.

(d) Articles Used in Fraud

There are two forms of offences involving articles for use in fraud. The first is the possession of such an article under section 6 and the second is making or supplying such articles under section 7 of the *Fraud Act 2006.* 'Article' is the defined under section 8 of the Act to include any program or data held in electronic form. It will include a machine for counterfeiting bank notes or credit cards, counterfeit goods and infringing copies of Compact

[553] *Ibid.,* p.426

Disks (CDs) and Digital Video Disks (DVDs). The offence appears to be strict liability in that there is no requirement that the person intends that the article is to be used for fraud or knows that it is to be, or may be so used.

(e) Obtaining Services Dishonestly

This offence under section 11 of the *Fraud Act 2006* replaces section 1 of the *Theft Act 1978* which provides for the offence of obtaining services by deception. This suffered from the problem that it might not have applied where the deception did not operate on a human being, such as where services was obtained by entering a password or other access protocol which was checked automatically by a computer. Furthermore, if the fraudster succeeded in obtaining the services there was no offence of theft of a service with which he could be charged. The new offence is committed by a person who obtains services for himself or another by a dishonest act where:

(i) the services are made available on the basis that payment has been, is been or will be made for or in respect of them;

(ii) he obtains them without any payment having been made for or in respect of them or without payment been made in full; and

(iii) when he obtains them he knows that they are been made available on the basis described in paragraphs (i) and (ii) above.

The maximum penalties for offence of obtaining services dishonestly are that on summary conviction, imprisonment for a term not exceeding 12 months (6 months in Northern Ireland) and/or a fine not exceeding the statutory maximum. On conviction on indictment, the maximum penalty is for a term not exceeding 5 years and/or a fine.

Most of the new offences under the *Fraud Act 2006* can be committed without the completion of the relevant gain or loss actually taking place, making the law of attempts redundant for these offences.[554] In terms of tackling ICT fraud, the old deception offences suffered from the probability that it was not possible at law to deceive a machine. The *Fraud Act 2006* brought in a number of offences appropriate to tackle ICT fraud including

[554] *Ibid.*, at p.433

dishonestly transferring funds electronically, phishing, using bogus websites to obtain personal details such as bank account details, spyware and dishonest use of telecoms and information services. It is therefore recommended in this study that the Nigerian *Advance Fee Fraud Act 2006* be amended to incorporate similar offences as contained in *UK Fraud Act 2006 albeit* with necessary modifications to suit our peculiar circumstance.

3.6.3 The United States Computer Fraud and Abuse Act 1986

In the Unites States, the first federal computer crime legislation was the *Computer Fraud and Abuse Act 1986*.[555] Both the States as well as the Federal Government have their own cybercrimes laws. In the states, perpetrators of cyber offences are prosecuted under the statutes similar to the *Californian Penal Code* dealing with unauthorised access to computers, computer systems or computer networks. The statutes deal with tampering, interfering, damaging or unauthorised access of computer data.[556] The *Computer Fraud and Abuse Act 1986* was intended to reduce cracking of computer systems and to address federal computer related offences. The Act governs cases where computers of the federal government or certain financial institutions are involved, where the crime is between the states or where computers are used in inter-states or foreign commerce. The Act defines "protected computers" to mean a computer exclusively for the use of a financial institution or the United States government or in the case of a computer not exclusively for such use, used by or for a financial institution or the United States government and the conduct constituting the offence affect that use by or for the financial institution or the government or which is used in inter-states or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects inter-states of foreign commerce or communication in the United States.[557] Offences under the Computer Fraud and Abuse Act (CFAA) include:

[555] 18 USC 1030
[556] See for example, the *West Virginia Computer Crimes and Abuse Act.*
[557] See 18 USC 1030(e)(2)

(a) Fraud and Related Activity in Connection with Computer

The CFAA contains seven sections. The first section protects against the knowing access of government computers to obtain classified information.[558] The second section proscribes the intentional access a computer without, or in excess of authorisation, to thereby obtain information from a financial institution, the federal government or any protected computer involved in interstate or foreign communications.[559] The third section is concerned with the intentional and unauthorised access of government computers or computers used by the government.[560] The fourth section addresses the access and fraudulent use of a protected computer and is triggered if the value of the use exceeds $5,000.[561] The fifth section is the main anti hacking subsection. The subsection applies to whoever knowingly causes the transmission of a program, information, code or command and as a result of such conduct, intentionally causes damage without authorisation to a protected computer.[562] Section 1030(a) (5) (B) prohibits unauthorised access that recklessly causes damage to a protected computer. Section 1030(a) (5) (C) covers negligent damage to a protected computer. It is intended to punish the activity of hackers who do not intend to harm the systems but accidentally cause harm to the computer in the process. The sixth section is concerned with unauthorised trafficking of computer passwords.[563] While the seventh section covers extortion threats against computer or network owners.[564] The section is invoked if the hacker threatened to launch an attack against the victim when the victim pays the hacker any money or other thing of value.[565] Perhaps, a summary of some criminal cases decided under the *Computer Fraud and Abuse Act* may be pertinent here.

[558] Section 1030(a) (1)
[559] Section 1030(a) (2)
[560] Section 1030(a) (3)
[561] Section 1030(a) (4)
[562] Section 1030(a) (5) (A)
[563] Section 1030(a) (6)
[564] Section 1030(a) (7)
[565] For further discussion on the provisions of CFAA see Eric, J. S. and William, P. R. 'Cybercrimes: A Practical Approach to Application of Federal Computer Crime Laws.' Retrieved from http://www.law.cornell.edu/uscode/18/1030/htm/sansinstitute2004 on April 3, 2014.

In *United States vs. Albert Gonzalez,*[566] the accused was charged with the offences of conspiracy, damage to computer systems, wire fraud, access to device fraud, aggravated identity theft among others. The accused and co-conspirators hacked into computer systems and stole credit card information from TJX, Office Max, DSW and Dave and Busters among other online retail outlets in one of the largest crime operations targeting that sort of data. They then sold the numbers to other criminals. Gonzalez pleaded guilty to conspiracy charges and was sentenced to two concurrent 20 year terms in prison.

The case of Albert Gonzalez was reported to be unparallel in the history of cybercrimes, where millions of credit card numbers were stolen.[567] The Federal prosecutors said sending Gonzalez to prison for that long is justified because he was "at the centre of the largest and most costly series of identity theft in the Nation's history. That he knowingly victimized a group of people whose population exceeded tens of millions, the full financial damage of the crimes committed by Gonzalez and his co-conspirators is difficult to access." Government claimed that companies, banks and insurers lost close to $200 million dollars and that Gonzalez's credit and debit card theft victimized group of people whose population exceeded that of many major cities and states.[568]

In an attempt to reverse his guilty plea and sentence, Gonzalez petitioned the U.S. District Court of Massachusetts, blaming his Attorneys for not properly representing or informing him about his defence options. Gonzalez claimed that all the criminal activities he admitted to in court were actually done with the full knowledge and the direction of the U.S. Secret Service. Gonzalez had begun working as confidential informant for the Secret Service in 2003, soon after his apprehended in connection with series of ATM theft. Over the next several years, he helped the Secret Service to infiltrate various hacking groups, leading the

[566] 08 CR 10.2.2.3 PBT US District Court of Massachusetts. Retrieved from http://fserrov.com/pdf/gonzalezindic timent.pdf. on December 26, 2015 at 2.10pm
[567] Weil, N. (nd) "Gonzalez Sentenced for Multi-Million Dollar Credit Card Scam." Retrieved from http://www. pcworld.com/… on February 8, 2016 at 8.32am
[568] *Ibid.*

arrest of many of them.[569] The government countered that simultaneously to government work, Gonzalez resumed his criminal activities under the noses of the Secret Service agents, who were paying him $75 thousand dollars per annum. Gonzalez argued that his only motive was technical curiosity and obsession with conquering computer networks but chat logs the government obtained showed Gonzalez confiding in his accomplices that his goal was to earn $15 million dollars from his scheme, buy a yatch and then retire.

In *United States vs. Morris*,[570] the creator of Morris worm, an early internet virus, was convicted under the Act for causing damages and gaining unauthorised access to federal interest computers. On appeal, the Court of Appeal held that the statute punishing anyone who intentionally accesses without authorisation federal interest computers and damages or prevents authorised use of information in those computers causing loss of $1,000 or more does not require Government to demonstrate that the accused intentionally prevented authorised use and thereby caused loss and there was sufficient evidence to conclude that the accused acted without authorisation within the meaning of the statute.

In *Robins vs. Lower Merion School District*,[571] the Complainants charged two sub urban Philadelphia High Schools who secretly spy on students by surreptitiously and remotely activating webcams embedded in school issued laptops the student were using at home. The schools admitted to secretly snapping over 66,000 web shots and screen shots, including webcam shots of students in their bedrooms.

Likewise, in *United States vs. Delmark,*[572] the accused, an adult was sending pornographic visual depictions of children to a Florida law enforcement person who was posing as a 12 year old boy. In determining the sentence guidelines, the court added four steps to the sentencing because the accused use of a computer to solicit sex from a minor, a violation of federal laws, which makes it illegal to use a computer to transmit such images.

[569] Vijayan, J. (2011) "Albert Gonzalez Who is Serving a 20 Year Sentence Wants to Reverse His Guilty Plea." Retrieved from http://www.computerworld.com/... on February 8, 2016 at 8.42am
[570] 982 F.2d 504, Decided on March 7, 1991
[571] US Eastern District of Pennsylvania. Retrieved from www.content.usatoday.com... on January 7, 2014 at 11.54am
[572] 99F.3d.80 (2d Gr.1996)

The Sentencing Guidelines Commission permits the court to determine the level of sentencing, and an Appeals court affirmed that the court did not abuse its discretion in this case.

In *United States vs. Sablan,*[573] the accused, a fired bank employee, used her password to log into her previous employer's bank computer in order to damage files. The accused was charged with computer fraud under the CFAA. She argued that the computer fraud statute was invalid because it did not have a *mensrea* requirement. She was convicted under the Act which provided punishment for whoever intentionally access a federal interest computer without authorisation by means of one or more instances of such conduct alters, damages or destroys information in any such computer and cause a loss of at least $1,000.

In *United States vs. Nosal*,[574] an ex-employee of an executive recruiting firm was prosecuted on the theory that he induced current company employees to use their legitimate credentials to access a company's proprietary database and provided him with information in violation of corporate computer-use policy. The government claimed that the violation of this private policy was a violation of the *Computer Fraud and Abuse Act* (CFAA). Following a decision issued in 2009 by the Ninth Circuit, the district court ruled that violations of corporate policy are not equivalent to violations of federal computer crime law.

In *United States vs. Sullivan*,[575] the accused was convicted in the United States District Court for the Western Carolina for intentionally causing damage to protected computer. The accused appealed. The Court of Appeal held that the items seized from the accused home and home computer was admissible under the Acts rule, and the conviction was supported by evidence.

In *United States vs. PFC Bradley E. Manning,*[576] the accused , a first class private in the US Army was charged for knowingly exceeding his authorised access on a secret internet

[573] 92F.3d 865 (9th Cir.1996)
[574] 676 F.3e 854 (9th Cir.2012)
[575] 40 Fed. Appx. 740 (4th Cir.2002)
[576] Retrieved from http://www.reuters.com/article/.../us-usa-wikileaks-manning-idUSBRE97J0JI20130821 on May 28, 2014 at 5.03pm

protocol router network computer and obtained information that have been determined by the US government pursuant to an executive order or statute to require protection against unauthorised disclosure for reasons of national defence, to wit: a classified video of a military operation filmed at or near Baghdad, Iraq on or about 12th July, 2007 and deed wilfully communicated, delivered and transmitted to a person not entitled to receive it, with reason to believe that such information could be used to the injury of the United States or the advantage of any foreign nation, in violation of 18.US Code section 1030(a)(1), such conduct been prejudicial to good order and discipline in the armed forces. The court martial found the accused guilty of 20 of the 22 charges he faced mostly of espionage, theft, fraud and sentenced him to 35 years in prison amongst others for leaking hundreds of thousands of classified documents to the website wikileaks.

The trial of Bradley Manning exposes the double standards of the United States who in one breath preaches and encourages freedom and or access to information in other countries of the world, yet it could not mustered the courage to accept the true revelations coming from its military operations in Iraq. In 2001, the *Computer Fraud and Abuse Act* was amended by the *US Patriot Act, 2002*.

3.6.4 The United States Patriot Act, 2001

The US *Patriot Act*,[577] was developed as anti-terrorism legislation in response to the September 11, 2001 attack. The law received little Congressional oversight and debate and was signed into law by President G. W. Bush on October 26, 2001. The Act authorises the interception of electronic communications for the collection of evidence related to terrorism, computer fraud and abuse.[578] The Act clarifies the definition of protected computers and increases fine and prison terms for damage.[579] The *Patriot Act* gives sweeping search and surveillance to domestic law enforcement and foreign intelligence agencies and eliminates

[577] Officially titled: "The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act PL107-56)". The Act was introduced as H.R 3162 by Representative James Sensenbrenner in October 2001
[578] Sections 201 and 202
[579] Section 814

check and balances that previously gave courts the opportunity to ensure that those powers are not abused. The Act expands law enforcement surveillance and investigative powers[580] and is said to represent one of the most significant threat to civil liberties, privacy and democratic traditions in the United States history. For example, the Act expands the type of information to which law enforcement official may obtain access and permits service providers to divulge the contents of communications in emergencies. Law enforcement official may obtain access to information including records of session times and durations, temporary network addresses, and means and source of payments, including credit card and bank account numbers.[581] Section 212 of the Act permits service providers to voluntarily release the contents of communications if they reasonably believe that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay. The Act makes it easier for the FBI to install 'trap and trace' devices in order to monitor the communications of citizens who are not suspected of any terrorism or espionage activities.[582] It allows the FBI to secretly order anyone to turn over business records or any other tangible things so long as the FBI tells the secret *Foreign Intelligence Surveillance Act* (FISA) court that the information sought is for an authorised investigation to protect against international terrorism or clandestine intelligence activities.[583] Section 271 permits service providers to invite law enforcement to assist in tracking and intercepting a computer trespasser's communications.[584]

3.6.5 The United States Homeland Security Act, 2002

The United States *Homeland Security Act*, 2002[585] directs US Sentencing Commission to re-evaluate federal sentencing guidelines for crimes involving computer related fraud and hacking offences, especially against restricted federal government

[580] Section 214 of the Act
[581] Section 210 of the Act
[582] Section 214 of the Act
[583] Section 215 of the Act
[584] Retrieved from http://www.eff.org/Privacy/Surveillance/Terrorism/20011031... on April 4, 2014 at 3.46am
[585] Introduced as H.R.5005 by Representative Richard Armey in June, 2002.

systems.[586] The Act increases prison term and penalties for violation of the CFAA, prohibits internet advertising of illegal surveillance devices, and allow law enforcement agencies to make trap and trace installations without a court order in the case of national security interests or an attack on a protected computer as defined by the CFAA.[587] The Act expanded the power of *Patriot Act* section 212 by allowing communication providers to use the emergency exception to disclose ones data to any government entity, not just law enforcement. The *Patriot Act* and *Homeland Security Act* provisions are quite draconian, coming from a country that prided itself as the leading light in democracy and human rights.

3.6.6 The Indian Information Technology Act, 2000

The *Indian Penal Code* of 1860 was found insufficient to cater for needs of new crimes emerging from internet expansion. Even some of the traditional crimes of conspiracy, solicitation, fraud, espionage are now being committed through the internet which necessitated a new law to curb them. It was in this background that the *Information Technology Act* (ITA) 2000 was enacted in India for prevention and control of cybercrimes. Before the enactment of the ITA, the law applicable to cyber offences was the *Indian Penal Code* which was enacted back in 1860 when no one thought of computer technology or cyber criminality.[588]

The ITA is based on the *United Nations Commission on International Trade Law* (UNCITRAL) Model Law on e-commerce 1996 in furtherance of the United Nations General Assembly resolution urging the member states to enact or reverse their cyber laws to create a uniform environment for regulating e-commerce at international level. The objective is to provide legal recognition for transaction carried out by electronic data into storage and other means of electronic communications which involves use of alternatives to paper based

[586] Section 225
[587] Sections 896 and 225 of the Act.
[588] For detailed discussion on *Indian Information Technology Act*, see Paranjape, N. V. (2010) *Op.cit.*, pp.142-149

methods of communication and storage of information to facilitate electronic filing of documents.[589]

Thus, the ITA seeks to prevent offences which result in e-commerce and e-governance. The cyber offences contained in ITA include: unauthorised access,[590] failure to furnish information, return, etc.,[591] tampering with computer source documents,[592] hacking,[593] publishing of information which is obscene in electronic form,[594] failure to comply with directions of controller[595] failure to assist in decryption[596]accessing protected systems,[597] misrepresentation,[598] penalty for breach of confidentiality,[599] publishing digital signature certificate false in certain particulars,[600] and publishing digital signature certificate for fraudulent purposes.[601]

It should be noted that the main objective of ITA 2000, was to create an enabling environment for e-commerce. It can be seen that some cyber offences have not been included. Besides, the working of the Indian *Information Technology Act*, 2000 brought to the fore its deficiency as such an Information Technology (Amendment) Bill was introduced in the Indian Parliament. The amendments seek to remove the deficiencies of the principal Act and provides for stringent punishment for cybercrimes.[602]

3.6.7 The South African Electronic Communications and Transactions Act

In early 2001, the South African Law Commission released a discussion paper on computer related crime and also recommended that legislation should be considered to introduce new cyber offences. This led to the *Electronic Communications and Transactions*

[589] *Ibid.*, p.143
[590] Section 43 of the Act
[591] Section 44, *Ibid.*
[592] Section 65, *Ibid.*
[593] Section 66, *Ibid.*
[594] Section 67, *Ibid.*
[595] Section 68, *Ibid.*
[596] Section 69, *Ibid.*
[597] Section 70, *Ibid.*
[598] Section 71, *Ibid.*
[599] Section 72, *Ibid.*
[600] Section 73, *Ibid.*
[601] Section 74, *Ibid.*
[602] See Paranjape, N. V. (2010) *Op.cit.*, p.142

(ECT) Act,[603] which was assented to on 31st July, 2002 and has been in operation since 30th August, 2002.[604] The ECT Act eradicated several *lacunae* that previously existed in the South African law in respect of the emergence of various types of cybercrimes, such as hacking, creation of malicious computer code, unauthorised access, unauthorised modification of data as well as the possession and distribution of hardware devices and software programs that facilitate the commission of cybercrimes. The specific provisions of the ECT Act include: unauthorised access,[605] unauthorised modification of data and various forms of malicious code, [606] denial of service (dos) attacks,[607] unauthorised interceptions,[608] devices,[609] extortion,[610] computer related fraud,[611] and theft.[612]

It can be discerned from the foregoing that the ECT Act was enacted to facilitate and regulate electronic communications and transaction. The focus of the Act is to protect data (electronic communications) or data messages and other related crimes. South Africa has made appreciable progress in its effort at combating cybercrimes with the enactment of the ECT. The ECT has created a legal certainty of what may and may not constitute cybercrimes. So far, South Africa is the only country in Africa to sign the *European Convention on Cybercrime* even though it is yet to ratify the Convention. South Africa has complied with the first part of the Convention in terms of which member states are obliged to criminalize acts or omissions that affects computer integrity and security. It is the view here that Nigeria, like South Africa should sign the *European Convention on Cybercrimes* so as to benefit from its cooperative and collaborative provisions, particularly with the much more advanced countries in cyber technology.

---

[603] Act no. 25 of 2002
[604] Mc Afee Virtual Criminology Report: North American Study into Organised Crime and the Internet. A Paper written for Council of Europe's Interface Conference. 10th-11th March, 2009, Strasbourg, France. Retrieved from www.mcafee.com/us/localcontent...report.pdf on May 25, 2014 at 3.59pm
[605] Section 86(1) of the Act.
[606] Section 86(2), *Ibid*.
[607] Section 86(5), *Ibid*.
[608] Section 86(3), *Ibid*.
[609] Section 86(4), *Ibid*.
[610] Section 87(1), *Ibid*.
[611] Section 87(2), *Ibid*.
[612] There has been increase in reported crimes where user identities and passwords have been compromised and theft and fraud committed.

3.7 Concluding Remarks

The pain is taken here to examine the legal framework for combating cybercrimes, developments of legislation on cybercrimes and cyber security as well as best practices of selected countries with the view to reveal some of the intricacies involved in the enactment of legislation and prosecutions of cyber related crimes in Nigeria. It can be clearly discerned from the pre-May 2015 statutory and judicial authorities referred to above that they are inadequate to combat the menace of cybercrimes in Nigeria. Hitherto, the absence of comprehensive legal and or judicial pronouncement in the area grossly exposed the problem. However, in Nigeria, the recent enactment of the *Cybercrimes Act, 2015* provides a comprehensive legislation that deals with specific cyber offences. Even at that, only 29 offences were provided under the *Cybercrimes Act, 2015*, while as at 2012, 74 species of cybercrimes were identified and new ones are emerging on nearly daily basis.[613] The existing laws may not be perfect, and no law is, they are nevertheless a step in the right direction towards making the internet a safer place for business, research and other use. As our reliance on computers and the internet continue to grow, the importance of the laws to protect the people from cyber criminals will continue to grow as well. From the discussions above, it is clear that until May 2015, when the *Cybercrimes Act,* 2015 was assented by the then Nigerian President, Nigeria lacks specific legal framework to effectively tackle the menace of cybercrimes. The fact that Nigeria ranks number three in the world and tops African nations in cybercrimes ranking means that the legislation on cybercrimes then, were inadequate and ineffective to curb the crimes. Besides, it can be seen from the cases cited above that the accused persons are essentially youth or university students who should be mindful of their trainings as leaders of tomorrow but they preferred the fast albeit illegal lane to success by way of fraudulent activities. This calls for serious concern for the future of the country Nigeria. In view of the above, this study recommends the amendment of the *AFFA* 2006,

[613] Aaushi, S. and Srinidhi, R. (2012) *Op.cit.*

which was the main legislation on cybercrimes in Nigeria to be in tune with some best practices such as the *UK's Fraud Act, 2006*.

CHAPTER FOUR

AN EXAMINATION OF THE EFFICACY OF THE INSTITUTIONAL FRAMEWORKS FOR COMBATING CYBERCRIMES IN NIGERIA

4.1 Introduction

Combating the spectre of cybercrime has been on the national agenda over the past decade.[614] Several initiatives directed at protecting the interest of Nigerians on cyberspace have been put forward. Agencies such as the Nigerian Cybercrime Working Group (NCWG), Nigeria Communications Commission (NCC), Economic and Financial Crimes Commission (EFCC), etc. have all worked towards curving the menace of cybercrimes. This chapter is an attempt to examine the efficacy of the institutional measures put in place with the view to stem the tide of cybercrimes in Nigeria.

4.2 National Institutional Framework for Combating Cybercrimes

4.2.1 Nigeria Cybercrimes Working Group (NCWG)

The Nigeria Cybercrimes Working Group (NCWG) is an inter-agency body comprising law enforcement, intelligence, security as well as information and communication technology (ICT) agencies of government and key private sector ICT organisations.[615] It was established on March 31, 2004 by the Federal Executive Council (FEC) on the recommendation of the President. The NCWG was made up of National Security Adviser (NSA), the Nigeria Communications Commission (NCC), Department of State Security (DSS), National Intelligence Agency (NIA), Nigeria Computer Society (NCS), Nigeria Internet Group (NIG), Internet Service Providers (ISP) and National Information Technology Development Agency (NITDA) among others. The group was created to deliberate on and propose ways of tackling the malaise of cybercrimes in Nigeria. This includes:

(a) educating Nigerians on cybercrimes and cyber security.

[614] Sesan, G. *et al* (2013) *Op.cit.,* p.16
[615] See Chawki, M. (2009) *Op.cit.,* p.13

(b) undertaking international awareness programs for the purpose of informing the world of Nigeria's policy on cybercrimes and to draw global attention to steps taken by the Nigerian government to rid the country of cybercrimes.

(c) providing legal and technical assistance to National Assembly on cybercrimes and cyber security in order to promote general understanding of the subject matter.

(d) carry out institutional consensus building and conflict resolution amongst law enforcement, intelligence and security agencies in Nigeria for the purpose of easing any jurisdictional or territorial conflict or concern over duties overlap.

(e) reviewing in conjunction with the office of the Attorney General of the Federation (AGF), all multilateral and bilateral treaties between Nigeria and the rest of the world on cross border law enforcement known and Mutual Legal Assistance Treaties (MLAT) for the purpose of amending the operative legal framework to enable Nigeria secure from and render assistance to its MLAT partners in respect to cybercrimes.[616]

It may not be out of place if one asserts that since the inauguration of the NCWG, the body had very little to show. The only significant accomplishment of the NCWG was the draft Nigerian Cybercrimes Bill 2014. Even the Draft Cybercrimes Bill which was introduced by the NCWG was withdrawn by its coordinator when the unacknowledged source of the Draft was pointed out.

Critics of the NCWG observed that there was likelihood of resource duplication with the EFCC.[617] In particular, it was the view that the statutory and functional composition of the NCWG shared similar mandates with those of the EFCC. Statutorily, the EFCC was created to combat advance fee fraud which includes the Nigerian 419 email. Similarly, the Draft Nigerian Cybercrimes Bill mandates functions of the NCWG to include fighting Nigerian cybercrimes. Thus, in terms of functional responsibilities, the NCWG was a clear duplication of the EFCC.[618] Whereas the EFCC has made several arrests, prosecutions and secured convictions of cyber criminals in Nigeria, the NCWG failed to facilitate and ensure the passage of any of the various Cybercrime Bills hitherto pending in the National Assembly.

[616] *Ibid.*
[617] See for example, Oyesanya, F. (nd) 'A Performance Review of EFCC and the Nigerian Cybercrimes Working Group.' Retrieved from http://www.nigeriavillagesquare.com/articles/femi-oyesanya/...html on May 5, 2014 at 3.51am
[618] *Ibid.*

4.2.2 National Information Technology Development Agency (NIDTA)

In 2001, the National Policy on Information Technology was put in place by the Nigerian government with the view to, among others, utilise information technology for sustainable national development, global competitiveness, education, wealth or job creation, poverty eradication, as well as guarantee that the country benefits maximally and contributes meaningfully by providing global solution to the challenges of the information age.[619] The policy also sought to protect and promote the interest, assets and safety of Nigeria, Nigerians by developing knowledgeable manpower with commensurate discipline and IT skills – set capable of efficiently generating and effectively utilising information in a timely manner for national decision making.[620]

Specifically, the National IT Policy's objectives with respect to national security and law enforcement are to safeguard life and property of all Nigerians both at home and abroad; preserve the territorial integrity of Nigerian borders and assets; and to provide alternative carrier opportunities for Nigerian citizens.[621] The government in collaboration with the NITDA and other stakeholders will frame appropriate legislation to among others, promote and secure electronic fund transfer and digital transaction payment system; protect government data, records and information in digital form; establish and enforce cyber laws to combat computer crime.[622] The responsibility of implementing the National IT Policy lies with the NITDA.

Thus, the National Information Technology Development Agency Act 2007 establishes the National Information Technology Development Agency to facilitate the growth and development of information technology in Nigeria.[623] NITDA regulates, monitors, evaluates and verifies progress on an on-going basis under the supervision and

[619] Paragraphs 2, 3 and 4 of the National Information Technology Policy. Retrieved from http://www.nidta.govs.ng/document/nigeriaitpolicy.pdf on May 15, 2014 at 3.57am
[620] Chapter 12, para. 12.1 of the National IT Policy.
[621] *Ibid.*, paragraph 12.2
[622] *Ibid.*, Chapter 13, para. 13.2-13.3
[623] Retrieved from www.blackfriars.law.com on March 20, 2014 at 5.24pm

coordination of the Federal Ministry of Communication Technology.[624] The major objective of the Agency is to bring government and its services to the people through IT and also ensure that Nigeria becomes a key player in the IT world.

In order to achieve its objectives, section 6 of the Act gives the Agency the power to exercise the following functions:

(a) provide guidelines to facilitate the establishment and maintenance of appropriate infrastructure for information technology and system application in Nigeria;

(b) introduce appropriate regulatory policies and incentives to encourage private and public investments in the information technology;

(c) determine critical areas for information technology requiring research intervention and facilitate research and development in such areas;

(d) advice the government on ways of promoting the development of information technology in Nigeria;

(e) develop guidelines for networking of public and private sector establishment;

(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 development of guideline for setting up of information technology systems.

NITDA's mission is to make Nigeria an IT capable country as well as using IT as an engine for sustainable development.[625] Part of NITDA's mandate is to ensure the safety of the Nigerian cyber space and a successful implementation of an electronic government program. In this regard, NITDA formulate the National Information Systems and Network Security Standards and Guidelines in January, 2013, Draft Guidelines on Data Protection in September, 2014, Guidelines on Nigeria Content Development in Information and Communication Technology (ICT) in December, 2013 and the Standard for Digital and Computer Forensics in Nigeria in March, 2014.

[624]Retrieved from http://www.nitda.govs.ng/... on May 15, 2014 at 4.11am
[625] *Ibid.*

(a) National Information Systems and Network Security Standards and Guidelines

The National Information Systems and Network Security Standards and Guidelines document is applicable to public sector organisations such as the federal and state ministries, federal and state departments, federal and state agencies, local governments, private sector organisation, companies and non-governmental organisations (NGOs).[626] The document prescribes minimum standards on seven (7) areas of network security and cyber forensic:

(i) Categorisation of Information;

(ii) Minimum Security Requirements;

(iii) Intrusion detection and protection;

(iv) Protection of Object Identifiable Information (OII);

(v) Securing Public Web Server;

(vi) System Firewall;

(vii) Cyber Forensic.[627]

The purpose of the document is to set minimum standards to be adopted by all organisations that do business in Nigeria for categorisation of all information collected, processed and stored using ICT systems based on the objectives of providing required levels of information security according to risk levels, threat thresholds and impact in order to guaranty confidentiality, integrity, availability, survivability and continuity business processes and information systems in Nigeria.[628] It further provides guidelines on information security control areas within each category and prescribes minimum information security requirement for the management operation and technical control for information in each category.

(b) Guidelines on Data Protection

The National Guidelines on Data Protection are issued by the NITDA in accordance with the NITDA Act 2007. They are specifically issued pursuant to section 6, 7 and 18 of the

[626] See para. 1.4 of the National Information Systems and Network Security Standards and Guidelines.
[627] *Ibid.*, Para 1.3
[628] *Ibid.*, Para. 2.1(a)

NITDA Act and is subject to periodic review by NITDA. A breach of the Guidelines shall be deemed to be a breach of the Act.[629] The Guidelines are mandatory for federal, states and local government agencies and institutions as well as private sector organisations which own, use or deploy information systems of the Federal Republic of Nigeria. They serve as reference for data collectors, data custodians, data processors, data systems auditors, data controllers, data personnel among others. Additional protection and security guidelines may be developed and used at organisation discretion in accordance with these guidelines.[630]

The scope of the Guidelines cover the processing of personal data whole or partly by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. The Guidelines does not cover the processing of personal data, processing operations concerning public security, defence, national security and the activities of the nation in areas of criminal law. These Guidelines covers data controller or processor (organisation) or the data subject (person) operating within Nigeria and Guidelines also covers organisations based outside Nigeria if the processed personal data of Nigeria resident.[631]

The Data Protection Guidelines apply to all data controller in public and private sector as defined in these Guidelines. The purpose of the document is to prescribe guidelines for all organisations or persons that control, collect, store and process personal data of Nigeria resident within and outside Nigeria for protecting of a specific category of data commonly known as Personal Data or Object Identifiable Information (OII). It prescribes minimum data protection requirements for the collection, storage, processing, management, operation and technical controls for information in this category.[632]

---

[629] See Guidelines on Data Protection Draft Version 3.1 Published by National Information Technology Development Agency (NITDA), September 2013. Retrieved from http://www.nitda.govs.ng/ on May 15, 2014 at 4.11am
[630] *Ibid.*
[631] *Ibid.*, at p.3
[632] *Ibid.*

(c) Guidelines for Nigerian Content Development in Information and Communications Technology (ICT)

In the exercise of the powers conferred in it by section 6 of the NITDA Act the NITDA issued the guidelines on Nigerian Content Development in Information and Communications Technology. The Guidelines came into effect on December 3, 2013 and it applies to the federal, state, local council, ministries, departments and agencies (MDA), private section institutions, business enterprises and individuals. The relevant part of this Guideline shall form part of any existing or future requirement for periodic accreditation and renewal of licence of Information and Communications Technology Companies including ISPs, Telco, etc. and for the grant of approval or permission for the establishment of new manufacturing or assembly plants, software houses and allied facilities.[633] The Guidelines were issued for the purpose of achieving the following national objectives amongst others:

(i) enable the local ICT industry to contribute meaningfully towards the achievement of national development targets;

(ii) facilitate efforts to build capacity and equip Nigerians to serve as active workers and participants in the local ICT industry;

(iii) provide a framework for the regulation and legislation on the creation, distribution and use of Information Technology and its associations within Nigeria;

(iv) promote and encourage an environment within Nigeria that is welcoming to foreign investments in Information and Communications Technology, as well as the export of indigenously made ICT goods and services.[634]

Essentially, the documents provide guidelines for ICT hardware, indigenous hardware development, ICT services, network and internet services, data and information management and human capital development in ICT.[635] The enforcement of the Guidelines shall be by NITDA and the relevant authorities in both the public and private sectors, including federal, state, and local bodies in charge of ICT procurement, regulation and development under the framework to be developed by NITDA.[636] NITDA shall amend or review these Guidelines

[633] Paras. 1.0, 2.0 and 4.0 of the Guidelines.
[634] *Ibid., Para*. 5
[635] *Ibid.,* Paras. 10-15
[636] *Ibid.,* Para 6.0

periodically or where the need arises in consultation with stakeholders. In reviewing them, the Agency shall be guided by global trends and practices in Information and Communications Technology and the developmental aspirations of Nigeria.[637]

(d) Standards for Digital and Computer Forensics in Nigeria

The Draft Standards for Digital and Computer Forensics in Nigeria was prepared by First Digital and Techno-Law Forensics Company for the National Technical Committee (NTC) meeting on Standards for Digital and Computer Forensics in March 2014. The NITDA Act empowers NITDA to develop such standards. The objectives of the Standards document are to develop the standard for the implementation of digital and computer forensics in Nigeria in terms of electronic evidence acquisition, examination, analysis and presentation in a manner that will be admissible in the law courts; to develop standards for forensic laboratories where admissible forensic evidence could be extracted and to develop standards for the quality of forensic laboratory staff.

The scope of the Standards document covers all areas of digital and computer forensic evidence obtained from computers, laptops, servers and other digital or electronic storage devices, including phones and mobile devices, video, photo, digital fingerprint and other biometric data. The Standards document is meant for those involved in the investigation and prosecution of incidents or offences which require the collection and examination of digital evidence in Nigeria. Besides, the document is intended for use in the recovery of computer based electronic evidence. The document is not a comprehensive guide to the examination of that evidence as such shall be subject to review and update from time to time in view of the dynamic nature of information technology. The document was developed to ensure that in a crime which involves a high-tech element the digital forensic examiner collects all relevant evidence in a timely and appropriate manner.

[637] *Ibid.*, Para 7

It is observed that for over 10 years after the adoption of the Nigeria's IT Policy and 7 years after the establishment of NITDA, there is little commitment towards the actualisation of the ideals of the policy in respect of cyber laws and security.

4.2.3 Nigerian Communications Commission (NCC)

The Nigerian Communications Commission (NCC) was established under the *Nigerian Communications Act*.[638] The NCC is the independent national regulatory authority for the telecommunication industries in Nigeria. The NCC is responsible for creating enabling environment for competition among operators in the industry as well as ensuring the provisions of qualitative and efficient telecommunications services throughout the country.[639] In furtherance of its mandate, the NCC has put in place Guidelines for the Provisions of Internet Service Providers (ISP) and other Internet Protocol based Telecommunication Services.[640]

The Guidelines require ISPs to ensure that users are informed of any statement of cybercrimes prevention or acceptable internet use published by the NCC or any other authority and that failure to comply with these acceptable use requirements may lead to criminal prosecutions.[641] Internet Service Providers are further required to cooperate with enforcement and regulatory agencies investigating cybercrimes or other illegal activity and must provide any service related information requested by the NCC or any other legal authority.[642] These include information regarding particular users and the content of their communications, while contacting the NCC in the event they became aware of any complaint or activity indicating internet use for the commission of an offence. March 15, 2009 was the deadline for all cyber cafe operators and Internet Service Providers in Nigeria to register with the NCC or face the wrath of the NCC. The NCC gave the deadline in a notice titled "Final

[638] Cap. N 97 LFN 2004.
[639] Section 3 of the *Nigerian Communications Act.*
[640] The Guidelines are made Pursuant to Section 70(2) of the Act.
[641] See Para. 5 of the Guidelines.
[642] *Ibid.,* Para. 6. Any other authority in this context is said to include the EFCC and the CBN. For further discussion on the NCC Guidelines for the provision of internet service, see Oyewume, A. O. (2012) 'The ICT Revolution and Commercial Sectors in Nigeria: Impact and Legal Interventions' *University of Ibadan Law Journal*, Vol.2, No.1, May, pp.201-223.

Warning to Illegal Telecom Operators and Service Provides." The notice stated that the decision was necessary in order to curb cybercrimes and bring security to Telecom sector.[643] The NCC has created a new department called New Media and Information Security in line with global trend in the fight against cybercrime.[644] It has been submitted that the possibility of encroachment on the fundamental right to privacy necessitates the putting in place of laws, rather than mere guidelines, which strike the right balance between law enforcement and protection of human rights.[645]

4.2.4 Economic and Financial Crimes Commission (EFCC)

The Economic and Financial Crimes Commission (EFCC) was established by the *EFCC (Establishment) Act, 2004* and was charged with the responsibility for the enforcement of all economic and financial crimes laws.[646]

The EFCC is vested with the powers to investigate, prevent and prosecute financial crimes such as the Advance Fee Fraud, corrupt practices among others.[647] It was established in response to pressure from the Financial Action Task Force (FATF) which named Nigeria as one of the 23 non-cooperative countries in the international community's efforts to fight financial crimes.[648] The EFCC is also responsible for identifying, tracing, freezing, confiscating and seizing proceeds of economic crimes. EFCC also host the Nigerian Financial

---

[643] See Muhammed, H. 'NCC Clamps down on Illegal ISPs, Cyber Cafes.' *Daily Trust.* Monday, February 23, 2009, p.55

[644] See 'Regulator Shines Path to Cyber Security Challenges in Nigeria.' Retrieved from http://www.world cybersecurityconference.org/new-content php. On March 30, 2015 at 8.30pm

[645] *Ibid.*, p.219

[646] See the Explanatory Memorandum to the Schedule to the *EFCC Act, 2004;* The EFCC is composed of members from the Central Bank of Nigeria, the Ministries of Foreign affairs, Finance and Justice, the National Drug Law Enforcement Agency, the National Intelligence Agency, the State Security Service, the Corporate affairs Commission, the Nigeria Deposit Insurance Corporation, the Commissioner for Insurance, the Nigerian Prison Service, the Nigerian Immigration Service, Inspector General of Police, four eminent Nigerians with cognate experience in finance, banking, law, accounting and a secretary. See section 2 of the *EFCC Act*

[647] In *Moore vs. EFCC,* (*2010)* ECLR 312 at 314, it was held that sections 6 and 7 of the *EFCC Act*, 2004 is clear on the functions of the Commission… this case as stated in the petition of the Respondents relates to forgery of signature on a document purportedly filed by a private company of individual. The crime, if it occurred, did not violate existing legislation governing economic activities of government and its administration. The alleged crime can not by any stretch of imagination be ascribed to any of the functions stated in section 6 and the special function in section 7 of the *EFCC Act*. If it were so, the EFCC could interfere in any criminal matter, there will have been no need to establish it as a special commission, independent of our Nigeria Police Force. This is not to send the wrong signal that the court is stifling investigation of crime. It is important that special law enforcement agencies stick to the letter of the law establishing them.

[648] Chawki, M. (2009) *Op.cit.,* p.11

Intelligence Unit (NFIU) vested with the responsibility of collecting suspicious transaction reports from financial and designated non-financial institutions, analysing and disseminating them to relevant government agencies and other financial intelligent units all over the world.[649] The NFIU complements the EFCC's Directorate of Investigations but does not carry out its own investigations. It has access to records and data banks of all government and financial institutions and has entered into agreement on information sharing with several financial intelligence centres.[650]

One of the cases of cybercrimes handled by the EFCC was the case of *FRN vs Amadi*,[651] the accused was charged on amended five (5) count charge of attempting to obtain money by false pretence contrary to sections 5(1), 8(b) and 1(3) of the *Advance Fee Fraud and other Fraud Related Offences Act*. The accused was alleged to have attempted to obtain the sum of US $125,000 from Fabio Fajans by sending a payment schedule containing false pretence to the said Fabio Fajans requesting for money to enable him process the transfer of US $2,500,000 being the contract sum for the generators Fabio Fajans was purported to have supplied to the Federal Government of Nigeria for the All African Games, 2003. The accused was said to have falsely represented to the said Fabio Fajans that the sum of US $125,000 represented the 5% processing fees of the total contract sum of US $2,500,000.

The prosecution witness PW1,[652] who acted as *agent provocateur* stated that the EFCC was informed about the existence of a person sending out emails in the name of Alh. Nuhu Ribadu, the Chairman of EFCC. He found on investigation, the existence of three fake websites. He wrote to the infodex of the websites making fictitious enquiries about Golf Bank of Nigeria, which does not exist. The operator of the fake website responded and series of communication ensued. The prosecution witness subsequently introduced himself as Fabio

[649] *Ibid.*
[650] *Ibid.*
[651] (2005) 2 QCCR 129.
[652] Abdulkarim Chukkol is of the Advance Fee Fraud Unit of the EFCC and Head of the Cybercrimes Unit, Lagos Office. He is responsible for investigating Cybercrimes at the EFCC. In one of the interviews he granted to this Researcher in the course of this research, he reliably informed this Researcher that the EFCC is now receiving ICT training from reputable international security organizations such as the FBI, Organization for Economic Cooperation and Development (OECD) and Microsoft among others.

Fajans, an Italian. During the series of communication, the operator made a number of false pretences including sending a forge CBN Payment Schedule and a forged FBI letter to the prosecution witness. The false pretences were made with the intent of obtaining the sum of US $125,000 from the said Fabio Fajans. The prosecution witness stated that the domain name of the fake www.efccnigeria.com was registered in the name of one Prince Mike. PW2 the Investigating Police Office (IPO) testified that he traced the Internet Service Provider (ISP) through which the fake website was operated to Multi-links. He got the phone number of the Multi-link's line used, and an address which led him to the accused person. The accused person was arrested and his computer set, Multi-links telephone box, the receipt for the purchase of the telephone line and the tenancy agreement of the accused apartment were recovered. PW3, an officer of the Multi-links testified that the accused bought the Multi-links line from one of their approved agent. The sum of all the evidence adduced from the prosecution was to show that all the fraudulent emails and fake websites were operated by the accused using the recovered computer set and the Multi-links telephone line. PW4, an officer of the CBN state in his evidence that the payment schedule purportedly issued by the CBN was forged.

The accused testified in his own defence. He admitted the ownership of the website. He stated that the words 'efcc' used by him stands for Edmond Felicia Chibuzor Chinyere. The first letters of the names of his father, his mother, his own name and his wife's name. He denied forging the CBN Payment Schedule. He denied ever mentioning or answering Ribadu in his email. He denied the knowledge of anyone called Fabio Fajans. He denied any transaction involving CBN. He said no EFCC documents or materials were recovered in his house.

Convicting the accused person, the court held per Obadina J., that:

> ... proving the authorship of an email could require as little as a party's admission that he or she wrote the email, the testimony of the receiving party, or even a *subpoena* to the sender's ISP combined with an expert witness in forensic computing to testify about the emails header. In the instant case, the evidence before the court

> which is uncontradicted is that the subscriber to Multi-links no. 7946846 sent emails to one Fabio Fajans using efccnigeria.com mail box and the mails were purportedly signed by Alh. Nuhu Ribadu. The subscriber to the Multi-links line is the accused person... the evidence before the court established conclusively that the accused is the same person who purported to be Alh. Nuhu Ribadu, Chairman of EFCC and who communicated with PW1 alias Fabio Fajans in the bundles of documents admitted as Exhibit P1. The evidence of PW1 and the document tendered by him proved the authorship of the emails... in the instant case as far as the purported Alh. Nuhu Ribadu (that is the accused person) was concerned Fabio Fajans was real. PW1 acted throughout as an *agent provocateur*. The testimony of PW1 is not tainted neither is it prejudicial... it was not contradicted during cross examination... the witness was very professional and thorough in his explanations as testimony in the visual display... Under section 5(1) of the *Advance Fee Fraud Act*, where a false pretence is contained in a letter or other document, it shall be sufficient in a charge of an attempt to commit an offence under the Act to prove that the letter or other document was received by the person to whom the false pretence was directed. In the instant case PW1 alias Fabio Fajans gave direct evidence that he received the emails containing false pretence from the accused… The accused person denied the allegations in this charge but admitted that he sends mail in the name of Dr. John Wear using the same *modus operandi* as the one in this charge… Now to a consideration of the sentence, Nigeria is seen as a nation of fraudsters and crooks because of the activities of a few who do not want to labour before they get rich. They devise evil and fraudulent schemes to swindle other people of their hard earned money. Such is the prevalence of their activity that a special legislation had to be enacted to curb them. The accused person is one of such fraudsters who must be made to face the full wrath of the law to serve as a deterrent to others like him. On count 1, pursuant to sections 8(b) and 1(3) of the Advance Fee Fraud and other Fraud Related Offences Act… the accused person is sentenced to 10 years imprisonment with no option of fine. On count 2, the accused person is sentenced to 3 years imprisonment. The sentences to run concurrently.

Dissatisfied with the judgment of the trial court, the convict appealed to the Court of Appeal.[653] The Court of Appeal affirmed the judgment of the High Court and dismissed the appeal. Still dissatisfied, he appealed to the Supreme Court in *Amadi vs FRN*.[654] At the Supreme Court, the Appellant contended that the trial court had no right to assume jurisdiction on the case as the proper parties were not before the court. That by virtue of section 211 of the *Constitution of the Federal Republic of Nigeria 1999*, it is only the

[653] Appeal No. CA/L/389/2005
[654] (2008) 18 NWLR (pt 1119) 259

Attorney General of a State or an officer of his department to whom he delegates such power that has the power to institute and undertake criminal proceedings against the Appellant. Therefore, the Respondent in this case lacked the prerequisite power to prosecute the Appellant and by implication the trial court lacked jurisdiction. The Appellant also contended that the offences on which he was charged and convicted were not proved beyond reasonable doubt.

Unanimously dismissing the appeal, the Supreme Court held on the competence of the EFCC to institute criminal proceedings that:

> ...the EFCC is a common agency responsible for both the Federal and State economic and financial crimes and as such it qualifies as any other authority to institute criminal proceedings under section 211(1)(b) of the 1999 Constitution, thus Mr. Hassan being a staff of the EFCC who signed the charge was competent to do so... by virtue of the provisions of section 5(1) of the Advance Fee Fraud and other Fraud Related Offences Act, where a false pretence, which constitute an offence under the Act is contained in a letter or document, it shall be sufficient in a charge of an attempt to commit an offence under the Act to prove that a letter or other document was received by the person to whom the false pretence was directed... "other documents" referred in section 5(3) of the Act includes a document transmitted through a fax or telex machine or any other electronic or electrical device, a telegram and a computer printout... the appellate court will have no jurisdiction to upturn judgments that are the products of admissible evidence and based on reasonable conclusion. In the instant case, the Supreme Court decline to upturn the findings of facts of the lower courts...

The case of *Amadi vs FRN* represented a very important stage in the fight against cybercrimes by the EFCC in Nigeria. It is one of the cases where the apex court in Nigeria pronounced on internet or computer related crime.

In 2013, the EFCC recorded 177 convictions in different courts across the country.[655] Of the 117 convictions recorded by the EFFC, 57 are in relation to offences of obtaining by false pretences and possession of documents containing false pretences under the *Advance Fee Fraud Act* 2006, which was the principal enactment for combating cybercrimes in Nigeria. This represents 49 percent of the total convictions secured by the EFCC in the year.

[655] See EFCC Record of Conviction, 2013 at www.efccnigeria.org. Note that the EFCC is yet to publish its record of convictions for the successive years of 2014 and 2015.

It is observed from the cases handled by the EFCC that the courts have exercised wide discretions in sentencing the convicts to the various terms of imprisonment. And, far from applying the maximum term of imprisonment as provided by the *AFFA 2006*,[656] the courts have resorted to giving different terms of imprisonment for the same offence,[657] and in some cases, with option of fine.[658] The least sentence under the *AFFA 2006* is 3 years imprisonment.[659] It is doubtful if the sentences given by the courts could serve the purpose of deterrence intended by the law makers. The point being made here is that the courts seem reluctant in applying the exact punishment for the offences committed. This, it is submitted may not deter subsequent commission of the offences. It is certainly not a good way of combating cyber and related crimes in Nigeria. Whereas the convictions recorded by the EFCC in 2013 are commendable, however the punishments imposed by the courts vary from the minimum terms of imprisonment for 6 months and the maximum of 91 years.[660]

In its bid to combat cybercrimes, the EFCC is collaborating with foreign anti-crime enforcement agencies such as the London Metropolitan Police, US FBI, Royal Canadian Mounted Police, and the Anti-Fraud Squad of the Western Australian Police.[661] For example, in 2010, it was reported that the EFCC in collaboration with the Serious Organised Crime Agency (SOCA) of the United Kingdom, made a recovery of N26.5 billion from perpetrators

[656] That is, not less than 7 years without option of fine for the offences of obtaining property by false pretence and fraudulent invitation under sections 1(3) and 4 of the *Act;* not less than 5 years without the option of a fine for other fraud related offence, use of premises and laundering of funds obtained through unlawful activities under sections 2(c), 3 and 7(2)(b); and not less than 3 years imprisonment for Director, secretary, employee or other staff of financial institution who facilitates, contributes or otherwise is involved in failure to exercise due diligence stipulated under section 7(3) of the Act.

[657] See for example the cases of *FRN vs. Olasaidi Dare* and *FRN vs. Churchill Joshua Essien* (4 years instead of the 7 years minimum); *FRN vs. Emejuru Prince Patrick, FRN vs. Akinloye Akintunde, FRN vs. Auwal Ibrahim* (3 years instead of the 7 years minimum); *FRN vs. Aturu Oluwafemi Victor, FRN vs. Michael Adewumi Fashole, FRN vs. Ibini Kayode, FRN vs. Solomon Rowland Uzor, FRN vs. Juventus Nonso LLodi, FRN vs. Jelili Gbenga* and *FRN vs. Daniel Danfulani & Anor* (6 months instead of the 7 years minimum); *FRN vs. Esosa, FRN vs. Abu Yusuf, FRN vs. Jeje Olaniran, FRN vs Dare Akanni Joel, FRN vs. David Omowunmi* and *FRN vs. Immaculate Aziegbemi* (1 year instead of the 7 years minimum); *FRN vs. Godembache, FRN vs. Okonta Vincent Chinedu, FRN vs. Ugoji T. Ugoji, FRN vs. Oyekanmi Adewale* and *FRN vs. Koredede Onanuti* (2 years instead of the 7 years minimum)

[658] See for example the cases of *FRN vs. Auwal Ibrahim, FRN vs. Nathaniel Abutor, FRN vs. Ugoji T. Ugoji, FRN vs. Maigari Bello Ibrahim T.* and *FRN vs. Bashir Ali & Anor.*

[659] See for example, liability of director, secretary, employee or other staff of financial institution and duties of telecommunication and Internet Service Providers and internet cafes under sections 7(3) (b) and section 13(5) (c) of the *AFFA 2006.*

[660] See Serial Nos. 1, 2, 5 and 109 of the 2013 EFCC Record of Convictions.

[661] See EFCC Partners Australian Police in Fighting Internet Fraud. Retrieved from http://efccnigeria.org/efcc/index... on May 16, 2014 at 5.41pm

of cybercrimes in 3 years.[662] Within the period, the EFCC intercepted 12,000 scam mails that were intended to swindle their recipients of various sums of money and have secured 300 convictions in cybercrimes cases.[663] It is hoped that through cooperation of this nature the EFCC and other law enforcement agencies could overcome the huddles of their investigations stopping at international borders. By working with other international enforcement agencies, the EFCC hopes to increase its capacity to track down and prosecute the perpetrators of cybercrimes and reduce financial impact on their victims. The partnership will also provide the basis for higher level cooperation which will mean that the agencies will share evidence and information on investigations and prosecution of transnational crimes. Although at inception, the EFCC's cybercrimes operations were inhibited due to lack of technical know-how, ICT software and other technical infrastructures. However, according to the Head of Cybercrimes Unit, Lagos Office of the EFCC, the situation has improved as a result of the constant and intense training received by staff of the Commission by international organisations such as FBI, Microsoft and SOCA.

4.2.5 Office of the National Security Adviser, Department of State Security and Directorate of Cybersecurity

The Department of State Security was established by the *National Security Agencies Act*.[664] Section 1 of the Act provides that, for the effective conducts of national security there shall be established the State Security Service, which shall be charged with the responsibility for the prevention and detection within Nigeria of any crime against the internal security of Nigeria; the protection and preservation of all non-military classified matters concerning internal security of Nigeria; and such responsibilities affecting internal security within

[662] See Amaefule, E. (2010). 'EFCC, SOCA Recover N26.6 billion in 3 years.' Retrieved from http://home.rica.net/alphae/419coal/news2010.htm on March 2, 2014 at 11.54am

[663]This researcher has made several efforts to get many of such cases where the EFCC secured convictions in cyber related offences but with little success. Staff of the courts where some of the cases were tried as well as some of the EFCC staff were not disposed to releasing information to the researcher. Nevertheless, the researcher is greatly indebted to Hon. Justice M. L. Shuaibu, formerly of the Federal High Court, Kaduna Division, Mr. Abdulkarim Chukkol, Head of Cybercrimes Unit, Lagos Office of the EFCC, Barr. M. S. Salisu and B. M. Buhari of the EFCC Kano Office, Barr. Fatsuma Mohammed and J. Bwala of the EFCC Abuja Office, who through their tremendous assistance availed the researcher with some of the cases and materials referred to in this study.

[664] Cap. N 74 LFN 2004

Nigeria as the National Assembly or the President may deem necessary.[665] In furtherance of its general duties of crime prevention and detection, the Directorate for Cyber Security was created as a permanent autonomous body within the office of the National Security Adviser (NSA) to take over all the assets and liabilities of the Nigerian Cybercrimes Working Group (NCWG), including all uncompleted projects.[666]

The main mandates of the Directorate for Cyber Security are to develop and implement a National Cyber Security Policy for Nigeria, drafting and/or proposing all relevant laws required to be enacted by the National Assembly for the security of computer systems and networks in Nigeria pursuant to the National Strategies on Cyber Security, establishing a National Computer Emergency Readiness and Response Mechanism with Early Warning System (EWS) and alerts for all cyber related emergency in the country, establishing a National Computer Forensics Laboratory and coordinating the training and utilisation of the facility by all law enforcements, security and intelligence agencies on cybercrimes and cyber security, developing effective framework and interfaces for inter-agency collaboration on cybercrimes and cyber security, coordinating Nigeria's involvement in international cyber security cooperation to ensure the integration of Nigeria into global frameworks on cyber security, 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, and establishing platforms for Public Private Partnership (PPP) on cyber security.[667]

---

[665] It should be noted that in addition to the State Security Service, section 1 of the Act established other security agencies such as the Defence Intelligence Agency (DIA) and National Intelligence Agency (NIA). The DIA is charged with the responsibility for the prevention and detection of crime of a military nature against the security of Nigeria; the protection and preservation of all military classified matters concerning the security of Nigeria, both within and outside Nigeria and such other responsibilities affecting defence intelligence of a military nature, both within and outside Nigeria as the President or the Chief of Defence Staff may deem necessary. The NIA on the other hand is charged with the responsibility for general maintenance of the security of Nigeria outside Nigeria, concerning matters that are not related to military issues; and such other responsibilities affecting national intelligence outside Nigeria as the National Defence Council (NDC) or the President may deem necessary. See generally sections 1 and 2 of the Act.

[666] Adewale, K.S., Isiaka, R.M., and Olayemi, R.T. (2011) 'An Inquiry into the Awareness Level of Cyber Security Policy and Measures in Nigeria.' *International Journal of Science and Advanced Technology* (ISSN 2221-8386) Vol. 1 No. 7, September. Retrieved from http://www.ijsat.com on May 16, 2014 at 2.21am

[667] *Ibid.*

Under the *Cybercrimes Act, 2015*,[668] the Office of the National Security Adviser (ONSA) is empowered to coordinate all security and enforcement agencies under the Act and shall in the process provide support to all relevant security, intelligence, law enforcement agencies and military services to prevent and combat cybercrimes in Nigeria; ensure formulation and effective implementation of a comprehensive cybersecurity strategy and a national cybersecurity policy in Nigeria,[669] establish and maintain National Computer Emergency Response Team (CERT) coordination centre responsible for managing cyber incidences in Nigeria; establish and maintain a National Computer Forensic Laboratory and coordinate utilization of the facility by all enforcement, security and intelligence agencies; establish appropriate platforms for Public Private Partnership (PPP); coordinate Nigeria's involvement in international cybersecurity cooperation to ensure the integration of Nigeria into the global framework on cybersecurity; and do such other acts that are necessary for the effective performance of the functions of the relevant security and enforcement agencies under the Act. This is quite an enormous responsibility given to the ONSA, one may concede.

It is obvious, that the ONSA exercises the aforementioned powers with the Cybercrime Advisory Council established under section 42(1) of the Act. Part of the powers and functions of the Cybercrime Advisory Council is to create enabling environment for members to share knowledge, experience, intelligence and information on regular basis and shall provide recommendations on issues relating to the prevention and combating cybercrimes and the promotion of cybersecurity in Nigeria. The Cybercrime Advisory Council shall also formulate and provide general policy guidelines for the implementation of the provisions of the *Cybercrimes Act 2015*, as well as advise on majors to prevent and combat computer related offences, cybercrimes, threats to national cyberspace and other cybersecurity related issues.

[668] Section 41(1) (a-h) of the Act
[669] These have been carried out by the former National Security Adviser, Col. M. S. Dasuki (rtd).

Like the NCWG, the Directorate for Cyber Security's efforts at combating cybercrimes in Nigeria are less heard of and/or appreciated. Their activities are highly secretive, restrictive and protective.

4.2.6 Nigeria Police Special Fraud Unit

The Special Fraud Unit of the Nigeria Police is responsible for the investigation of high profile, local and international fraud cases particularly the advance fee fraud (419), cybercrimes and information technology frauds.[670] However, little is known of the efforts made by the Nigeria Police to combat the menace of cybercrimes in Nigeria. Efforts made by the researcher to elicit information regarding the Police activities with respect to cybercrimes in Nigeria met brick walls. Most of the cybercrime cases being prosecuted in Nigerian courts were instituted by the EFCC, the police having resorted to investigating less sophisticated traditional crimes. The problem of the Nigeria Police may not be unconnected with the massive corruption prevalent in the system, incompetence and absence of trained and specialised manpower skilled in cybercrimes prevention, detection and prosecution.[671] This perhaps, informed the call for an independent agency to handle cyber offences in Nigeria.

4.2.7 Computer Crime Prosecution Unit, Federal Ministry of Justice

As part of its commitment at combating cybercrimes, the Federal Government in Nigeria approved the establishment of the Computer Crime Prosecution Unit (CCPU) under the supervision of the Public Prosecution Department of the Federal Ministry of Justice.[672] The CCPU is to collaborate with agencies such as the EFCC, the Telecoms and banking sectors in its bid to combat cybercrimes in Nigeria.[673] Officers of the CCPU are said to have commenced training in basic prosecutor's courses and electronic evidence handling among

[670] Retrieved from http://www.npf.govs.ng/departments/crime-investigation. Accessed on the May 18, 2014 at 8.30pm

[671] For example, the researcher submitted a complaint on behalf of a client who was receiving injurious text messages from an unknown person using a Glo line to the police for investigation. Till date, no headway was made in apprehending the culprit by the police. Nearly all the officers the researcher met on the case requested for money from the researcher to enable them contact their headquarters at Abuja.

[672] Ani, L. (nd) 'Cybercrime and National Security: The Role of the Penal and Procedural Law.' Retrieved from www.nials-nigeria.org on April 6, 2015, pp.211-212 at 4.15am

[673] *Ibid.*

others, while other modalities for the effective take off of the Unit are being worked out.[674] At best, the CCPU is still in its infancy as such little can be said of its efficacy in combating cybercrimes in Nigeria.

It is nevertheless pertinent to note here that the *Cybercrimes Act, 2015* empowers the Office of the Attorney General of the Federation to strengthen and enhance the existing legal framework on cybercrime with the view to ensure conformity of Nigeria's cybercrime and cybersecurity laws and policies with regional and international standards; maintenance of international cooperation required for preventing and combating cybercrimes and promoting cybersecurity; and effective prosecution of cybercrimes and cybersecurity matters.[675] Besides, law enforcements, security, and intelligent agencies shall develop requisite institutional capacity for effective implementation of the provisions of the Act and shall in collaboration with the office of the National Security Adviser, initiate, develop or organise training programmes, nationally or internationally for officer charged with the responsibility for the prohibition, prevention, detection, investigation and prosecution of cybercrimes.[676] The Attorney General of the Federation is also empowered to make orders, rules, guidelines or regulations necessary for the efficient implementation of the provisions of the *Cybercrimes Act 2015.*[677] The Attorney General of the Federation may in the discharge of his functions, request the assistance from any agency of a foreign state in investigation and prosecution of the offences under the *Cybercrimes Act, 2015,* whether or not any bilateral or multilateral agreement existed between Nigeria and the country to which the request is made.[678] It is submitted that the provisions of section 52 of the *Cybercrimes Act, 2015,* which provides for international cooperation by the Attorney General of the Federation and other foreign countries for the purpose of investigation and prosecution of cybercrimes, whether or not there exist bilateral or multilateral agreement between Nigeria and the other country may be

[674] *Ibid.*
[675] Section 41(1) and (2) of the Act
[676] *Ibid.*, section 41(3)
[677] *Ibid.*, section 57(1)
[678] *Ibid.*, section 53

difficult to enforce. This is because the efficacy of this provision will depend on the will of such foreign country as well as their law enforcement agencies to demonstrate their willingness to assist in the punishment of such crimes.[679] Besides, where there is no extradition treaty between Nigeria and the foreign country, offenders may not be extradited to Nigeria for the purposes of prosecution and this will limit the effect of the Act, to the effect that offences under the Act shall be extraditable under the *Extradition Act*.[680]

4.2.8 The Central Bank of Nigeria

The Central Bank of Nigeria (CBN) Act,[681] established for Nigeria, the CBN as a body corporate with perpetual succession and a common seal and may sue and be sued in its corporate name.[682] In 2003 the CBN reported that the Nigerian banking sector lost over N20 billion from internet fraud and the impact on the nation's cashless policy was significant. Likewise, with the reported theft of N2 billion from the Union Bank of Nigeria by three young undergraduate students of a federal university, the challenges posed by cyber criminals became enormous to the nation's financial system. According the CBN, cyber criminals have succeeded in siphoning off between €60 million and €2 billion in fraudulent transfers from at least sixty banks globally.[683] The CBN reported that the banks lost N20 billion in 2012 through internet fraud.[684] the effect of cyber criminal industry on modern banking sector in Nigeria led to the introduction of new e-banking/electronic products and services by the CBN,[685] in the areas of Regulatory Framework for Mobile Payment Services in Nigeria, 2009; Standard and Guideline on ATM Operations in Nigeria, 2010; Guidelines for Card Issuance and Usage in Nigeria, 2014; and CBN Anti-Money Laundering Regulations, 2013.[686]

---

[679] *Ibid.,* p.14
[680] *Ibid.*
[681] No. 7, 2007
[682] Section 1(1) and (2) of the Act.
[683] Udotai, B. *Op.cit.*
[684] *Ibid.*
[685] Ladan, M.T. *Op.cit.*, n. 47,pp.310-327
[686] *Ibid.*

The CBN was a member of NCWG that draft the first *Cybercrimes Bill, 2004.* The CBN played a vital role in the formulation, enactment, passage and assent to the National Cybersecurity Policy,[687] and National Cybersecurity Strategy[688] and *Nigerian Cybercrimes Act, 2014.* As a member of the Cybercrimes Advisory Council,[689] the CBN shall be the custodian of the National Cybersecurity Fund made pursuant to section 44(1) and (2) of the *Cybercrimes Act, 2014.*[690] The fund is a levy of 0.005 of all electronic transactions by the businesses specified under the second schedule to the Act. The businesses specified under the Act include GSM Service Providers, all Telecom Companies, Internet Service Providers, Banks and other financial institutions, Insurance Companies and Nigeria Stock Exchange. The above functions revealed the role been played by the CBN in combating cybercrime in Nigeria.

4.2.9 The Judiciary

The *Constitution of the Federal Republic of Nigeria* (CFRN) 1999 establishes three categories of High Courts, namely; the Federal High Court, the High Court of the Federal Capital Territory (FCT), Abuja and the High Court of a State.[691] The jurisdictions of the High Courts are provided under sections 251, 257 and 272 of the *CFRN* 1999. It is pertinent to note that the existing legislation on cybercrimes in Nigeria confer jurisdiction on the Federal High Court to try offences and impose penalties under the laws.[692] Section 50 of the *Cybercrimes Act, 2015*, for example, provides that:

> The Federal High Court located in any part of Nigeria regardless of the location where the offence is committed or High Court of FCT shall have jurisdiction to try offences under this Act, if committed –
>
> (a) In Nigeria; or
>
> (b) On a ship or aircraft registered in Nigeria; or

[687] See Appendix III to the NCSP, 2014 at p.48
[688] See Appendix III to the NCSS, 2014 at p.75
[689] See sections 42, 43 and the First Schedule to the *Cybercrimes Act, 2015*.
[690] Section 51 of the *CBN Act, 2007*.
[691] Sections 249, 255 and 270 of *CFRN* 1999.
[692] See for example, sections 14 of the *AFF Act* 2006 and 19 of the *EFCC Act* 2004. See also section 50 of the *Cybercrimes Act*, 2015.

(c) By a citizen or resident in Nigeria if the person's conduct would also constitute an offence under a law of the country where the offence was committed;

(d) Outside Nigeria, where –

(i) The victim of the offence is a citizen or resident of Nigeria; or

(ii) The alleged offender is in Nigerian and not extradited to any other country for prosecution.

The provision of the *Cybercrimes Act, 2015* above is couched to take care of the problem of cyber jurisdiction. However, it is suggested that the High Court of the States and that of the Federal Capital Territory be included among the categories of the courts to try the offences under the Act. The use of the phrase "Federal High Court located in any part of Nigeria regardless of the location where the offence is committed" is intended to cure the allegation of forum shopping levelled against some of the enforcement institutions saddled with the responsibility of prosecuting economic crimes generally. For example, in *Ibori vs. FRN*,[693] the Court of Appeal, per Amina Augie JCA, held that the trial of the 2nd Appellant, Chief James Ibori (the former Governor of Delta State) by the EFCC on an amended count charge of corrupt enrichment, money laundering and allied offences before the Federal High Court Kaduna amounted to forum shopping. The Court ordered that the matter be transferred to the Chief Judge of the Federal High Court for onward transfer and assignment to the Judicial Division where the 129 counts in the charge levelled against the Appellants were allegedly committed.[694]

However, when the matter was eventually transferred to the Delta State Division of the Federal High Court situated at Asaba for the purpose of trial *denovo,* the Appellants (accused persons at the Federal High Court) were 'miraculously' discharged by the Federal High Court. The 2nd Appellant (Chief James Ibori) was nonetheless rearrested in Dubai, United Arab Emirate and extradited to United Kingdom where he was tried, convicted and

[693] (2009) All FWLR (pt. 487) 159.
[694] *Ibid.*

sentenced to various terms of imprisonment on the same count charge which the Nigerian Court could not try him.

Besides, in *FRN vs. Prince Rapheal Akpiaifo*,[695] the accused and others at large were charged on amended Eight (8) count charge of conspiracy to commit unlawful act, to wit; obtaining money by false pretence contrary to section 8(a) and punishable under section 1(3) of the *AFFA* 2006. The second count alleged that the accused with others at large on or about 28th day of October, 2010 within the jurisdiction of the High Court of Kano State, with intent to defraud and did through internet hacking of an e-mail from M.U.R.G. Co. Nig. Ltd, Kano, on behalf of West Waves General Trading LLC to Alfa Exchange United Emirates induced Alfa Exchange United Arab Emirates to deliver the sum of $600,000 (Six hundred thousand US Dollars) to Shenzen Zhiyuan International Trading Co. Ltd. by false pretence and thereby committed an offence contrary to section 1(1)(b) and punishable under section 1(3) of the *AFFA* 2006.

Counts 3, 4, 5, 6, 7 and 8 alleged that the accused with others at large with intent to defraud forged various documents entitled: "RNATONL: YOUR SWIFT CONFIRMATION BY RZZ-ADVICE ONLY dated 29th September, 2010," "PARTY LEDGER (Multi CCY) date 20th-22nd September, 2010," "ALFA EXCHANGE, DUBAI, UNITED ARAB EMIRATES T.T. APPLICATION dated 21st September, 2010" thereby committed an offence contrary to section 366 and punishable under section 364 of *Penal Code*.

By a preliminary objection dated 27th June, 2011, the accused counsel prayed the trial court to quash the charge preferred against the accused on the ground that the statement of the witness or proof of evidence filed in the charge has no correlation whats ever with the charge filed against the accused person. That the application to prefer the charge was a gross abuse of court process. In response, the prosecuting counsel filed a written address dated 12th July,

[695] Unreported suit No. K/EFCC/03/2011. Ruling delivered on 30th May, 2012 by His Lordship Hon. Justice A. M. Bayero, High Court No. 17, Kano.

2011 and the preliminary objection was moved, argued and adjourned for ruling. Delivering its ruling on 30th May, 2012, the court held that:

> ...it is important to state that from the onset that the only proofs of evidence before this Honourable court are the written statement of the accused person and those of Mr. Fidelis Kwaghelade and Mr. Aminuddeen Muhammad. The intended statements of Messrs Murtala Abdullahi Jega, Information Technology expert, Alfa Exchange, Danjuma Audu, Philip Timba, Gabriel Ochere and representative of UBA Plc, since they were not annexed to the Application to Prefer a Charge against the accused person, this Honourable court is not enjoined to consider them in determination of this Notice of Preliminary Objection... the court observed that all the Eight (8) head counts of the Amended Charge have the following at its opening sentence: 'that you Rapheal Akpiaifo and others now large...' the court however observed that nowhere in the proof of evidence to show who those others now at large are and I so hold. The first count charge is for the offence of criminal conspiracy and obtaining money by false pretence contrary to section 1(3) of the *AFFA* 2006, while count two is charging the accused with others at large for the offence of internet hacking and also obtaining money by false pretence. Counts 3-8 relate to the offence of forgery contrary to section 364 of the *Penal Code*. The first count, as I earlier stated, is for the offence of conspiracy... I have carefully gone through the proof of evidence and discovered that nowhere is it shown who those with whom the accused conspired with... Conspiracy is a secret planned by two or more persons to do something harmful or illegal/unlawful... It cannot be committed by one person... I hereby hold that the accused alone cannot commit the offence of conspiracy... The first count charge is therefore quashed. As regard the second charge, it relates to hacking of an e-mail. I have gone through the proof of evidence and discovered in the statement of Aminuddeen Muhammad, an operative with EFCC that: 'the suspect admitted that he knows about the hacked money amounting to $600,000 (Six hundred thousand US Dollars) belonging to the complainant but he was not the one that hacked the money but his business partner in China.' However, the accused in his statements stated thus: 'regarding the allegation that I blocked the complainant e-mail address, I don't know about that. I did not partake in the intervention of the money and diversion of the money...' It therefore follows that contrary to the statement of Aminuddeen reproduced above, the accused statement is apt and direct that at no time did he hacked the complainant e-mail transaction and I so hold. The second count is therefore quashed... As regards counts 3, 4, 5, 6, 7 and 8 all relating to forgery, I have gone through the proof of evidence filed by the prosecution and discovered that it did not disclose any link between the accused person and commission of the offence of forgery contrary to section 364 of the *Penal Code* and I so hold. There is nowhere where it is stated in the statement of the accused person that he forged any document... The statement of the accused is not a confessional statement to the effect that he forged any document to commit an offence... The statement of the witnesses to

> be called by the prosecution did not allude to any document forged by the accused person. It therefore follows that in the absence of any statement in the proof of evidence linking the accused person to the alleged offence of forgery, this Honourable court has no other option but to quash counts 3, 4, 5, 6, 7 and 8 of the charge. They are accordingly quashed... The proof of evidence clearly does not disclose an offence against the accused and I do think that amounts to abuse of court process and I so hold. The accused is accordingly discharged.

The case of *FRN vs. Prince Rapeal Akpiaifo* represent a sad development and unfortunate meltdown in Nigeria's quest at combating the menace of cybercrimes. In the course of this research, this researcher was in Kano and had the opportunity of studying the case file of *Prince Rapeal Akpiaifo.* With due respect to the Honourable court, this researcher is not on agreement with the ruling of the Honourable court. The decision of the court begets more questions than answers to the problem.

To start with, it is an elementary principle of Nigeria's justice system and the same was judicially acknowledged in plethora of cases that the courts do not determine the substance or merit of a case in an interlocutory stage.[696] The ruling of the Honourable court in *Prince Rapeal Akpiaifo*'s case did not seem to adhere to such judicial directives. The learned trial court had gone ahead to determine the substance of the case even before taking oral or documentary evidence to establish the culpability or otherwise of the accused person. While it is conceded that the offence of conspiracy cannot be committed by an individual, it is possible to try an accused person for conspiracy if his/her co-conspirator(s) is/are at large. The accused, Prince Rapeal Akpiaifo, 39 years old, native of Ugboha, Uromi Local Government of Edo State together with a Chinese nationale named Dexiong Adam Wu of Wenan Center, Wenjin North Road, Shenzhen, China on or about 28th October, 2010, hacked into the e-mail of M.U.R.G Bureau de Change Ltd, Kano. The e-mail was sent to her sister company West Waves Trading LLC instructing Alfa Exhange Co. Dubai, United Arab Emirates to transfer the sum of $600,000 (Six hundred thousand US Dollars) to a company

[696] See the cases of *Nabore Properties Ltd vs. Peace-cover Nig. Ltd & Ors* (2014) LPELR 22586; *Uma & Ors vs. Effiom & Ors* (2013) LPELR 21407; *Obikoya vs. Wema Bank* (1989) 1NSCC 113

named Ample Spring Holding Ltd into a bank account with China Citi Bank. The accused, who at that point in time was resident in China and married to a Chinese woman named Wendy Xend, intercepted the e-mail and fraudulently caused the said $600,000 (Six hundred thousand US Dollars) to be transferred to Shanzhen Zhiyuan International Trading Co. Ltd at Shenzhen Development Bank Ltd in China, a company belonging to his co-conspirator, Dexiong Adam Wu.

The information made available to Nigerian authorities by the Interpol shows that the accused immediately transferred the sum $550,000 (Five hundred and fifty thousand US Dollars) to his private account in China. And on 29th and 30th October 2010, he transferred $440,000 (Four hundred and forty thousand US Dollars) and $40,000 (Forty thousand US Dollars) to Harlem Group, a company in Japan. The accused also transferred $50,000 (Fifty thousand US Dollars) to his personal account No. 03870131000209 with UBA Plc, Agbor Road, Benin City, Nigeria. The accused was arrested in Nigeria when he went to make withdrawal from his account with UBA Plc in Benin City.

A careful perusal of the accused extra-judicial statement to the EFCC which statement the trial court relied on to quash the charges against the accused person reveals that the accused initially denied any knowledge of the criminal transaction and even claimed that the amount of $50,000 (Fifty thousand US Dollars) he sent to his UBA Plc account in Nigeria was his personal money.[697] In the accused's subsequent statement to the EFCC, he admitted knowledge of the criminal transaction. The accused stated in his own words as follow:

> ... In addition to my earlier statement, I work for a China man as agent cos I help him to some transaction most of the time... The person that pay the money to my account is Adam Wu. Meanwhile the whole document used to post money to my account is with the China man and a paper I used to sent the money from China to Nigeria is in China. The money I first sent is 50,000 USD and later I sent 10,000 USD which is 60,000 USD. (N9,000,000) presently the total money left in my account is 14,000 USD and N900,000 left and I have used N6,000,000 since I came to Nigeria... The Chinese man by name Adam Wu is my Boss that sometime I assist him in some transaction. Adam open his computer and saw about 500,000 US Dollars in the computer, which is seventy

[697] See the Nigeria Police Statement of Witness/Accused C2 (P) dated 16th November, 2010.

> five million naira (N75,000,000). The Chinese man told me, they ordered for caterpillar part (pumbs)... The Chinese man told me that he cannot mail the specification of the parts in China according to the customer demand that is why he ordered the part in Japan. Four days later the Chinese transferred five hundred and fifty thousand US dollar into my China account. The following day... I transfer about five hundred US Dollars to a company account in Japan to buy the caterpillar pumb (part) all the paper used in the transaction are with Adam Wu... After the whole business, the Chinese payed me my commission for the old and new transaction about fifty thousand dollars which I send to Nigeria through Bank UBA and mail to my state...[698]

Even with the above admission on the part of the accused, the trial court did not see any reason why the case should proceed to trial and/or final determination, particularly for the offences of conspiracy to defraud and fraudulent conversion of the sum of $600,000 (Six hundred thousand US Dollars) equivalent to the sum of N75,000,000 (Seventy five million) in Nigeria's currency. A further perusal of the charge shows that the prosecution annexed List and Summary of Evidence of all the witnesses it intended to call and rely on during trial thereby puncturing the claim of the trial court that no proof of evidence of the witnesses was annexed to the charge. It is the view of this researcher that the trial court ought to have allowed the prosecution to establish the merit or otherwise of its case instead of terminating it *ab initio*.

Adam Wu, the Chinese national, who the accused (Prince Rapheal Akpiaifo) made reference to in connection to the alleged offence, was, according to the Report from Interpol to the EFCC, arrested by the Chinese Police tried, convicted, sentenced and executed in respect to the crime. While the Nigerian accused who was earlier on granted bail by the trial court and who was not in court on the date the court read its ruling discharging him, had escaped and his where about is still unknown to the EFCC or Nigerian authorities. This case clearly represents one of the instances where the courts serve as a clog in the wheel of effective prosecution of cybercrimes in Nigeria.

4.3 International Institutional Collaborations in Combating Cybercrimes

[698] See Nigeria Police Statement of Witness/Accused C2 (Q) and C2 (R) dated 18th and 19th November, 2010 respectively.

Cybercrimes have obvious transnational dimension. Thus, the limitations of territorial sovereignty mean that cyber criminals may not have much to fear from law in jurisdiction where their activities affect and cause harm. To address this enforcement concern, governments have made attempt within various international organisations and fora to achieve a harmonised approach to outlawing cybercrime activities and thereby try to prevent the appearance of cybercrimes havens. The most significant inter-governmental institutions in the area have been the International Police (Interpol) and Financial Action Task Force (FATF), hence a review of their activities.

4.3.1 The International Police (Interpol)

The International Criminal Police Organisation, otherwise known as the Interpol, is an organisation that facilitates the collaboration between all the police forces around the world.[699] The organisation consists of 186 member countries and had developed and implemented an international police communication system called 1-24/7. The purpose of the system is to enable and facilitate the exchange of information among the member police forces. The police forces from member countries can look for and verify data with direct access to Interpol's databases.[700]

The Interpol is committed to the global fight against cybercrimes as well as tackling cyber enabled crime. Most cybercrimes are transnational in nature therefore, Interpol is the natural partner for any law enforcement agency looking to investigate these crimes on a cooperate level.[701] By working with private industry Interpol is able to provide local law enforcement with focused cyber intelligence derived from combining input on a global scale. Interpol's main initiatives in cybercrimes focused on operational and investigative support; cyber intelligence and analysis; digital forensic; innovation and research; capacity building and national cyber reviews.[702]

---

[699] Retrieved from http://eprints.qut.edu.au/43400/1/Ali_Alkaabi_Thesis.pdf on May 18, 2014 at 5.17pm
[700] *Ibid.*
[701] Retrieved from http://www.interpol.int/crime_areas/cybercrimes/crime on December 29, 2015 at 8.50pm.
[702] *Ibid.*

Interpol supports and facilitates international collaboration among the police forces in combating worldwide crimes such as cybercrimes. Interpol's work on combating cybercrimes are designed to assist cooperation between the member countries via a list of contact officers reachable for cybercrimes investigation; enhance the exchange of information on cybercrimes between member countries; support member countries in the incidence of cybercrimes investigation attack; build up partnerships with other international and private organisations.[703] Interpol has also established collaborative work with the private sector in countering the spread of cybercrimes. For example, Interpol and Microsoft organised the meeting of the Botnet Task Force (initiated by Microsoft in 2004) to tackle and address the growing threats of Botnets.[704]

The Interpol is committed to becoming a global coordinating body on detection and prevention of digital crimes through its Interpol Global Complex for Innovations (IGCI) in Singapore, a key component of which is the Digital Crime Centre which provides proactive research into new areas and latest training techniques and coordinates operations in the field.[705] Interpol's main initiative in cybercrimes focus on a comprehensive audit of national legislation, police infrastructure and technical capacity with accompanying recommendation; working with regulatory bodies to develop global strategies as well as advising individual countries on their national approach; representing the law enforcement perspective in the development of new and updated legislation and combining police research with similar activities in other sectors.[706] For instance, more than 500 people have been arrested and 15 call centres shut down in an Interpol coordinated operation targeting multi-million dollar phone and e-mail scams across the Asia Pacific region.[707] Involving 23 countries, Operation First Light 2015 resulted in series of raids across the region with the largest in Indonesia where police arrested 245 Chinese and Taiwanese individuals and in Cambodia where 168

[703] *Ibid.*
[704] *Ibid.*
[705] Retrieved from http://www.interpol.int/crime-areas/cybercrimes on May 18, 2014 at 5.14pm
[706] *Ibid.*
[707] More than 500 Arrested in Interpol Operations Targeting Phone and E-mail Scams. Retrieved from http://www.interpol.int/news… on December 29, 2015 at 11.02am.

Chinese nationals were taking into custody. Korean, Nigerian, Russian nationals were also among those arrested in China, Hong Kong (China), Korea, Thailand and Vietnam during the two-month long operation during which more than 30 suspicious call centres were identified.[708]

Also, in an operation targeting paedophile networks sharing child sexual abuse material via online forums, the Interpol arrested 60 offenders across 15 countries in Americas and Europe and rescued 4 victims.[709] In Argentina, nearly 200 raids were carried out in 47 cities which resulted in the seizure of hundred of computers, mobile phones, video cameras, CDs and memory cards containing thousands of abusive images. Among those arrested was a 25 year old primary school teacher in Guatemala who had been downloading and distributing child abuse images and a man in Chile who had recorded his sexual abuse of an 11 year boy over a period of two years.[710]

4.3.2 Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) is an intergovernmental body established in 1989 by the ministers of its member jurisdictions.[711] The objectives of FATF are to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.[712] In collaboration with other international stakeholders, the FATF also works to identify national level vulnerabilities with the aims of protecting the international financial system from misuse.

In order to fulfil its objectives, the FATF carries out the following tasks amongst others; identifying and analysing money laundering, terrorist financing and other related

[708] *Ibid.*
[709] Online Child Sex Abusers' Forums Targeted in Interpol Coordinated Operation. Retrieved from http://www.interpol.int/news... on December 15, 2015 at 11.05am.
[710] *Ibid.*
[711] The membership of FATF consists of Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Denmark, European Commission, Finland, France, Germany, Greece, Golf Corporation Council, Hong Kong, China, Iceland, India, Ireland, Italy, Japan, Kingdom of the Netherland, Luxembourg, Mexico, New Zealand, Norway, Portugal, Republic of Korea, Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom and United States of America.
[712] Retrieved from FATF Mandate (2012-2020). Retrieved from http://www.fatf.gafi.org on May 18, 2014 at 5.12pm

threats to the integrity of the financial system including the methods and trends involved; examining the impact of measures designed to combat misuse of the international financial system; supporting national, regional and global threats and risk assessments; developing and refining the international standards for combating money laundering, financing of terrorism and proliferation; identifying and engaging with high risk, non cooperative jurisdictions and those with strategic deficiencies in their national regimes, and co-ordinating action to protect the integrity of the financial system against threats posed by them.[713]

It is a well known fact that terrorists have been using the internet to communicate, extort, intimidate, raise funds and coordinate operations. Hostile states have highly developed capabilities to wage cyber wars.[714] They have capabilities to paralyse large parts of communication networks, cause financial meltdown and socio-economic and political unrest. Cyber terrorism is the adoption of terrorism to computer resources whose purpose is to cause fear in its victims by attacking electronic resources. It is generally understood to mean unlawful attacks and threats of attack against computers, computer networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify cyber terrorism an attack should resolve in violence against persons or property or at least cause enough harm to generate fear.[715] In June 2007, an attack originated from China shut down the unclassified network in the Pentagon for a week.[716] Other targets for cyber attacks include power grids, energy infrastructures, banking and financial services, defence services, defence industry,

[713] *Ibid.*

[714] In 2007, the first cyber war was started in Estonia. The country defended itself for a month from a Denial of Service (DOS) attacks that clogged the country's servers, routers and switches. Although the attacks were said to emanate from Russia, millions of bots from around the world were combined into a botnet, forming a giant network used to mount the attack. Anyone who is networked is vulnerable to these attacks. See Traynor, 'Russia Accused of Unleashing Cyber War to Disable Estonia.' *The Guardian*, May 17, 2007. Retrieved from http://www.guardian.co.uk/russia/article/... on May 18, 2014 at 5.12pm

[715] There is a well developed criminal underground market that is connected to the mafia in Russia and web gangs and affiliated groups around the world. A well organised crime groups that had taken control of a global billion dollar crime network powered by skilful hackers and money moles targeting known software security weaknesses. In Russia, these criminals post stolen credit cards numbers, social security numbers, Paypal and ebay credentials. See Traynor, *Op.cit.*, n.524

[716] See Thornburgh, 'Inside the Chinese Hack Attack,' *Times.* August 25, 2007. Retrieved from http://www.times.com/time/nation/printout/... on May 18, 2014 at 5.14pm

emergency response networks and telecommunications.[717] It was reported that nine out of ten businesses in the United States were affected by cybercrimes.[718]

The internet is transforming money laundering. With larger amount, traditional money laundering techniques still offer a number of advantages, but the internet offers several advantages. Online financial services offer the option of enacting multiple worldwide financial transactions very quickly. The internet has helped overcome the dependence on physical monetary transactions. While transfers replaced transport of hard cash as the original first step of suppressing physical dependence on money. Money laundering is generally divided into three phases: placement, layering and integration. With regard to placement of large amount of cash, the use of internet might not offer tangible advantages. However, the internet is especially useful for offenders in the layering (masking) phase. In this context, the investigation of money laundering is especially difficult when money launderers use online casinos for layering. The internet offers offenders the possibility of cheap and tax-free money transfer across borders. Current difficulties in the investigation of internet based money laundering techniques often derive from the use of virtual currencies and use of online casinos.[719]

In a bid to counter that, FATF introduced a number of changes to strengthen the measures to combat money laundering, terrorist financing and other offences in the financial sectors. These include the adoption of a stronger standard for money laundering offences, detailed customer due diligence requirements, extension of customer due diligence and record keeping requirements to designated non-financial businesses and professions such as Accountants, Lawyers, Service Providers, Casinos, etc.[720] The activities of FATF in this

[717] For example, the intentional destruction of communication infrastructure by North Atlantic Treaty Organisation (NATO) forces during the war in former Yugoslavia. Retrieved from www.nato.int/kosovo/press/... on May 20, 2014 at 8.06pm

[718] Emke, J. (2008) 'Trends and Shocks and the Impact of the Acquisition Community.' Defence AT & L, 37(1), 3.

[719] The above illustrates the combination of online casinos and virtual currencies in internet based money laundering scams. By using such services, offenders can make it difficult for law enforcement agencies to track transfer processes and identify the offenders.

[720] Retrieved from http://www.fatf.org/... on May 18, 2014 at 5.09pm

regard allows for sharing of information collected by the member states, increase awareness of the attendant risks to members and exploring money laundering and terrorist financing in the domestic and international financial institutions.

4.4 Problems and Challenges of Enforcement

The modern society today faces with the greatest achievements of technical and technological development associated with rapid expansion of information technology and automation of work activities in all sphares of social life.[721] Such development in modern society has brought a number of benefit on one side, while on the other side the presence of deliberate misuse of this technological achievement has created a number of problems and risks towards individuals and groups in society in general and national safety in particular. Computers and networks can be used to attack victims or prepare global violent act such as terrorism.[722] Cybercrimes represent one of the challenges for today's society. Cybercrimes have been considered as one of the threats for national security in 21st Century. Thus, recent developments in ICT have resulted in new cybercrimes and new criminal methods, with also new methods of investigating cybercrimes. Offenders now use tools to prevent identifications and hamper investigations. This part of the research examines some challenges of fighting cybercrimes in Nigeria.

4.4.1 Cyber Jurisdictions

Cybercrimes often have extra-territorial aspects that can give rise to complex jurisdictional issues. For instance, acts constituting cyber offences may be carried out in different nations. The general principle of international law in this regard is that a crime committed within a state's territory may be tried there (except in respect of a person covered by diplomatic immunity).[723] The Convention on Cybercrimes addresses the issues of

[721] Nuredini, S. A. (2014) "Challenges in Combating Cybercrime." *Mediterranean Journal of Social Sciences.* MCSER Publishing, Rome, Italy, Vol. 5, No. 19, pp.592-598
[722] *Ibid.*
[723] See for example Article 31 of *Vienna Convention on Diplomatic Relations, 1961* which provides that a diplomatic agent shall enjoy immunity from criminal jurisdiction of the receiving state. He shall enjoy immunity from its civil and administrative jurisdiction except in the case of a real action relating to private immovable property situated in the territory of the receiving state, unless he holds it on behalf of the sending state for the

jurisdiction under Article 22 to the effect that jurisdiction should exist when the offence is committed:

(a) in its territory; or

(b) on board a ship flying the flag of that party; or

(c) on board an aircraft registered under the laws of that party; or

(d) by one of its nationals.

Again, the European Convention on Cybercrime requires a member state to establish jurisdiction over its nationals and to prosecute them where as a matter of national law, such persons may not be extradited to a requesting state where the crime was committed.

The Nigeria *Cybercrimes Act 2015* appears to incorporate the provisions of the Convention on jurisdiction under section 50 of the Act. The section provides that:

> 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 –
>
> *(a) in Nigeria; or*
>
> *(b) in a ship or aircraft registered in Nigeria; or*
>
> *(c) by a citizen or resident in Nigeria if the persons conduct would also constitute an offence under a law of the country where the offence was committed; or*
>
> *(d) outside Nigeria, where –*
>
> *(i) the victim of the offence is a citizen or resident of Nigeria; or*
>
> *(ii) the alleged offender is in Nigeria and not extradited to any other country for prosecution.*

---

purposes of the mission; an action relating to succession in which a diplomatic agent is involved as executor, administrator, heir or legatee as a private person and not on behalf of the sending state; an action relating to any professional or commercial activity exercised by the diplomatic agent in the receiving state outside his official functions. A diplomatic agent is not obliged to give evidence as a witness. Note that the immunity of the diplomatic agent does not exempt him from the jurisdiction of the sending state.

Section 50(4) of the *Cybercrimes Act 2015* provides that subject to the provisions of the *Constitution of the Federal Republic of Nigeria*, an application for stay of proceedings in respect of any criminal matter brought under the Act shall not be entertained until judgment is delivered. The section did not state which section of the Constitution, the Act shall be subjected to. Stay of proceedings though discretionally exercised by courts, is usually granted in deserving cases. To say that it shall not be granted until judgment is delivered in a case may be draconian and subject to abuse by courts.

Geographical jurisdiction is such a problem because laws differ from state to state and nation to nation. An act that is illegal in one state may not be against the law in another. These differences complicate issues if the perpetrator is on a location where he or she is doing is not even against the law even though it is a clear cut crime in the location where the victim is. Law enforcement agencies are only authorised to enforce the law within their jurisdiction. Extradition,[724] is difficult at best and often impossible. Under Article 23 of the *European Convention on Cybercrimes*, state parties are under obligation to cooperate with each other in criminal matters. Although some countries have treaties whereby they agree to turn over criminals on request to one another, even in those cases it is usually after an expensive long, drawn out process. For example in *Udeozor vs. FRN*,[725] on 9th June, 2004 the then Attorney General of the Federal Republic of Nigeria signified to the trial court, by an order under his hand, that a request had been made to his office for the extradition of the Appellant. The signification was made pursuant to the *Extradition Act*, Cap. 125 LFN 1990.[726] The request was made by the Diplomatic representative of the embassy of the United State of America, Abuja, for surrendering of the Appellant. The documents accompanying the request for surrender indicated that the Appellant had been charged in the United States District of Maryland, with the offences of conspiracy to commit an involuntary servitude,

[724] The process by which a state or a nation surrenders a suspect to another state or country.
[725] (2007) 10 QCCR 135
[726] Now Cap E25 LFN 2004

harbouring an illegal alien and encouraging an illegal alien to come to, enter and reside in the United States.

At the hearing of the application, the Appellant opposed the grant of the application but was overruled. The application was granted and the Appellant ordered to be remanded in prison custody to await his surrender over to the United States of America. The appellant dissatisfied with the decision appealed to the Court of Appeal which dismissed the appeal.

The above case represented one of the instances where counsel explore delay tactics and legal technicalities to frustrate the trial of persons alleged to have committed offences in other countries other than Nigeria. This attitude is reprehensible and should be eschewed by counsel who are by their callings and profession, ministers in the temple of justice.

4.4.2 Problems of Investigation

Before the issue of jurisdiction comes into play, it is necessary to discover who the cyber criminal is before one can think of making an arrest. This is the problem with an online crime because there are so many ways to hide ones identity. There are numerous services that will mask a users Internet Protocol (IP) address by writing traffic through various servers usually for a fee. This makes it difficult to track down the criminal. The offenders use tools to prevent identification and hamper investigation. However, attempt to track online identity raised serious issues for privacy advocates. An end to anonymity on the internet could have serious consequences in countries where government punishes online dissenters.[727] Cyber criminals exploit the rights and privileges of a free society, including anonymity to benefit themselves.

Under the *Cybercrimes Act, 2015*, the power of arrest, search and seizure are provided under sections 45 of the Act. To enhance such powers, a judge, may open exparte application grant order for the purpose of obtaining electronic evidence in relation to an investigation.

[727] China and North Korea are examples of countries where online dissenters are persecuted. The Chinese legislature recently approved new rules that will tighten government control of the internet by the requiring users to register their real names, and demanding internet companies censor online materials. The regulations are aimed at protecting the personal information of web users and cracking down on abuses such as junk e-mail. The rules also aim to "safeguard national security and social public interest." See Woodsome, K. 'China Tighten Control on Internet Use' *Voice of America (VOA)* News. December 28, 2013.

Wilful obstruction of law enforcement in the exercise of his duty attracts 2 years imprisonment or fine of not more the N500,000.[728] The law enforcement agencies that have the power to prosecute are the relevant "law enforcement agencies." However, consent of the Attorney General of the Federation is required for prosecution under sections 19 and 21 of the Act. It is not discernable to this researcher why the prosecution under section 19 and 21 of the Act is subject to the consent of the Attorney General of the Federation while other provisions that are more cyber specific were not.

4.4.3 Evidential Issues

Another thing that makes cybercrimes more difficult to investigate and prosecute in comparison to most crimes is the nature of the evidence. The problem with digital evidence is that it is fragile and can be easily lost or changed. An investigator can contaminate the evidence simply by examining it, and sophisticated criminal may set up their computer to automatically destroy the evidence when accessed by anyone other than themselves. In cases of child pornography for example, it can be difficult to determine that a person downloaded the illegal material knowingly since someone else can hack into a system and store data on its drive without the user's knowledge or permission if the system is not adequately secured.[729]

In cases of intrusion or cyber vandalism, the cyber criminal often erases all logs that show what happened so that there is no evidence to prove that a crime even occurred, much less where the attack came from. The news is not all that bad because computer forensic has come a long way and there are tools available to investigators that allow them to examine digital evidence without tampering with it. Forensic examiners should be adequately trained to reliably preserve data for presentation in court and recover deleted data. While online anonymity is still achievable, it is getting more difficult with diligent work, it is possible to track down cyber criminals by Internet Protocol (IP) and by clues that they may leave within the content of the data.

[728] Section 46 of the *Cybercrimes Act, 2015.*

[729] Shinder, D. (nd) "What makes Cybercrimes Laws so Difficult to Enforce?" Retrieved from http://www.techrepublic.com/blog/it_security/... on June 28, 2014 at 3.23pm

Hitherto, the issue that directly comes to mind is whether or not evidence gotten through the internet or computer can be admissible in court to aid the prosecution of cybercrimes in Nigeria. The *Evidence Act* was silent on electronically generated evidence and admissibility of the same.[730] This point was captured by Hon[731] when he stated that:

> ...Before the promulgation of the *Evidence Act,* 2011, the admissibility of computer and electronically generated evidence was very difficult, almost impossible, generally speaking, in Nigerian courts, no thanks to the absence of extant provisions in the repealed Act regulating this important aspect of modern-day business and even personal life of humanity...

Thus, in *Tolliver vs. FRN,*[732] the court held that internet and computer derived evidence was inadmissible. In this case, an engineering company brought charges of fraud and breach of contract claims against Nigeria. The company in support of its claims attached news postings printed off the internet and other evidence found in the computer hard disk and attempted to offer them as exhibit. The court held that the news posting in the internet are rife with hearsay and was not properly authenticated by persons with personal knowledge.

Also in *Egbue vs. Araka,*[733] Pats-Acholonu, JCA (as he then was) stated that:

> ...It must be clearly understood that our *Evidence Act* is now more than 50 years old and is completely out of tune with the realities of the present scientific and technological achievements. Most of its sections are archaic and, anachronistic and needs thorough overhaul to meet the needs of our time. But alas it is with us now like an albatross on our neck...

Thus in *UBA Plc vs. Sani Abacha,*[734] the Court of Appeal, held that section 97(1) of the *Evidence Act* will continue to apply to exclude the admissibility of statement of accounts contained in computer print outs unless and until it is amended by an Act of the National Assembly.

This earlier position of the courts in not accepting electronically generated evidence led to ineffectiveness in the prosecution of cases in Nigeria. However, with the enactment of

[730] For detailed discussions on the admissibility of computer generated evidence see Babaji, B. in Chukkol, K. S. (2010) *Op.cit.,* pp.387-476; Osinbanjo, Y. (2001) *Op.cit.,* pp.243-273 and Tar, S. (2006) *Op.cit.,* pp.754-476.
[731] Hon, S. T. (2013). *Law of Evidence in Nigeria.* Pearl Publishers, Port Harcourt, Rivers State, pp.468-521
[732] (1969) 1 NMLR 194 SC; see also *Oguma vs. Associated Co. Nig. Ltd.* (1998) 1 NSCC 395
[733] (1996) 2 NWLR (pt 433) 710
[734] (2004) 3 NWLR (pt 861) 561 at 543

Nigerian Evidence Act, 2011, the position is no longer the same as computer and electronically generated evidence are now admissible by virtue of section 84 of the Act.[735] A consideration of most of the cases,[736] from those jurisdictions have revealed only one pattern: disputes as to admissibility arise only with respect to admissibility of hi-tech evidence generated from the computer, especially evidence that has much to do with accuracy of the computer or any other machine generating it. It is not part of the practice in India and England that spurious objections be raised on admissibility of common place, ordinary documents printed out of the computer, as is being done daily in Nigerian courts.[737] While the amendment of the *Evidence Act, 2011* to incorporate admissibility of computer generated evidence is a welcome development, it may not yet be *uhuru* because the wordings of the said section 84 of the Act appear to be less discernable even to a person trained in the legal profession.

Nevertheless, in *Fani Kayode vs. FRN*,[738] the Court of Appeal ordered that electronically generated statement of account shall be admitted as evidence in the trial of the former Minister of Aviation for money laundering charges. The Accused is facing a 49 count charge before the Federal High Court, Lagos for strange cash lodgements of over N230,000,000 (Two hundred and thirty million naira) in his account at Finbank branch in Apapa, Lagos while he was a Minister. It was held per Dongbem-Mensen JCA, that:

> ...Nowhere in section 97 is the means of making the copy whether by longhand writing, by a duplicating machine or by a computer printout is not relevant. Not from the ordinary wordings of the provisions of section 97(2) (e) (ii) of the *Evidence Act*. In fact in the case of *Anyeabosi vs. R. T. Briscoe Nig. Ltd.* (1987) 3 NWLR (Pt. 59) 108, the Supreme Court held that such book as stated in section 97(2) (e) of the *Evidence Act 2004* have now been replaced by computers and entries therein have replaced entries expected to be found in bound bankers'

[735] Section 84 of the Act which deals generally with admissibility of computer generated evidence, was said to be lifted directly from section 65B of the Indian *Evidence Act*, 1872, as amended and substantially from section 69 of the *English Police and Criminal Evidence Act*, 1984, popularly called in the United Kingdom, the *PACE Act*, 1984. See Hon S. T. (2013) *Op.cit.*, pp.468-469

[736] See for example, East-West Transport Ltd. v. Crown Prosecution (1995) QBD: Cormac Leonard v. Vehicle Inspectorate (1996) QBD.

[737] *Ibid.*

[738] (2010) 14 NWLR (Pt. 1214) 481; also (2010) LPELR-CA/L/349/2009

> books. In that case, the apex court endorsed the admissibility of computer printout as secondary evidence...

Commenting on the provisions of the English statutes from which Nigeria drew inspiration to enact section 84 of the *Evidence Act, 2011,* Awomolo,[739] noted that nothing in those statutes assist computer users in deciding how best to link the records with its makers, a role traditionally performed in relation to physical documents by an autograph signature. Nor, if the document emanates from another computer, is there any provision which will assist in proving when it was sent and from where. Worthy of note is the fact that electronic transaction or stored information may be signed electronically, other self generated output like the ATM tellers may not be so easily authenticated except from the certification of whom ever operated the machine. Least to say, such things as SMS and MMS may have to go through process before their secondary evidence are obtained.[740] It is submitted that the aforementioned calls for brainstorming and redrafting of the *Evidence Act 2011* with input of expert in information technology.[741]

4.5 Concluding Remarks

In this chapter, attempt was made to examine the institutional frameworks for combating cybercrimes in Nigeria. Also of importance are the problems and challenges of enforcement bordering on the issues of cyber jurisdictions, problems of investigation and issue of admissibility of computer generated evidence. It is the view that effective law enforcement is an essential component to fighting cybercrimes, as such this study recognised the importance of engaging all stakeholders from the public institutions, private sectors and academia who are working towards the common goal of safeguarding the cyber space. It is important to harmonise efforts across different sectors in order to share expertise while avoiding duplication of activities already in progress. In this way, enforcement institutions

[739] Awomolo, A. (2013). 'Admissibility of Electronic Evidence.' Retrieved from www.awomolo& associates .com on August 20, 2014 at 3.41am

[740] *Ibid.*

[741] For judicial authorities on electronically generated evidence in Nigeria, see *Yusuf vs. ACB Ltd.* (1976) 1SC 45; *Trade Bank Plc vs. Chani* (2003) 13 NWLR (Pt. 836) 216; *Federal Polytechnic Ede & Ors vs. Alh. Lukman Ademola Oyebanji* (2012) LPELR-19696-Suit No. CA/I/126/2006, where the courts made the best of the situation by expanding the definition 'document' to include computer generated evidence.

may efficiently focus their resources in fighting cybercrimes as they work with other stakeholders to develop a holistic and coordinated response. By encouraging the creation of dedicated cybercrimes investigation units, and updating legal frameworks, enforcement institutions will build a proactive facilitation role in fighting cybercrimes. Moreso that cybercrimes are increasingly becoming major threats to national and international governments in the digital age. In recent years, more and more countries the world over have been forced to evaluate their legal systems to deal with the growing threats of the cybercrimes.

An examination of the institutional measures for combating cybercrimes makes it clear that Nigeria is concerned with the growing menace. It is clear from the foregoing institutional initiatives are taking shape with the view to combat cybercrimes. Nevertheless, cybercrimes do not respect national boundaries. This lack of respect for national boundaries create challenges for the global community in terms of legislative, investigative and prosecutorial capacity and reach which must address technical vulnerabilities in the system it designs and operates which sometimes cover many national jurisdictions. The internet brings criminals together to share information on how to commit crimes and how to avoid detection, adding a new dimension to organised crime. It is therefore, necessary for all and sundry to cooperate effectively with the view to develop, monitor, maintain and update frequently the expertise in policy, law enforcement, prosecution and prevention of cybercrimes.

The Nigerian government is counselled to further heighten her partnership and cooperation with the international community to address the issue of network and cyber security. Since cyber security is a global issue, governments should engage the support of the global community to address it. These steps will ensure greater confidence in the use of internet by Nigerians. To this end, the efforts made at encouraging international cooperation and partnership in the recently enacted *Cybercrimes Act, 2015*, National Cybersecurity Policy and Strategy, 2014 are commendable.

CHAPTER FIVE

SUMMARY AND CONCLUSION

5.1 Introduction

This part of the research dwells on the summary, findings, recommendations and conclusion.

5.2 Summary

This research examined the effectiveness of the legal and institutional frameworks for combating cybercrimes in Nigeria. In so doing, we have identified that the rapid increase in computer interconnectivity and Information and Communication Technology (ICT) have resulted in both positive and negative impacts to humanity. The positive effects of the ICT revolution are seen in terms of the use of ICT in business, industry, medicine, science, engineering, education and government, to mention but a few fields. The advantages of computers are countless and they have profound effect on the society. In today's world, we use computers for everything; searching the internet, online shopping, accessing bank accounts, e-mails and online gaming. Communication is faster and more reliable than in the past. Traditional shopping malls have been replaced by virtual shopping malls and one can acquire almost anything through the internet. Information super highways have made a virtual borderless world possible. One can have access to information located anywhere in the world within seconds on a click of a mouse. Computers are now used for data retrieval systems, systems controlling traffic by land, sea, air and systems indispensable to functioning of banking, industry and commerce amongst other positive sides of the internet revolution.

The negative side of the ICT revolution involves the misuse of the internet for criminal activities. Computers and Information Technology have revolutionised the commission of various crimes leading to a situation where investigators, more often than not, have to play catch up with sophisticated and more organised criminals. Computers have been involved in most types of crime, including theft, fraud, embezzlement, extortion and

espionage.[742] Criminals now use internet for money laundering and other types of crimes. Information technology allows them to carry out these crimes more efficiently with less risk. The use of pseudonyms or online identities provide an anonymity that is attractive to cyber criminals. Nigeria is among the countries in the world that is most affected by the negative activities of cyber criminals popularly referred to as the "*Yahoo Boys.*" These species of computer savvy criminals mostly in their productive age brackets of 20 to 45 years, and generally students of higher institutions of learning,[743] have succeeded in carving for Nigeria negative names and appellations among the comity of nations.[744] Global anti-crimes bodies such as the Interpol and FATF have black listed Nigeria as one of the most crime vulnerable centres in the world. Public as well as private companies around the world have taken steps to block email traffic from Nigeria while some are said to completely denied access to their website of the email traffic from Nigeria.[745]

It is on the basis of the aforestated negative effects of cybercrimes that Nigeria put in place some legal and institutional measures for combating cybercrimes. Such legal and

[742] The revelations from documents leaked by ex-US intelligence contractor, Edward Snowden are still fresh in our memories. Snowden alleged that the US National Security Agency (NSA) has hacked into telephone conversations and data belonging to highly placed political figures such as German Chancellor Angela Merkel's. Bolivian President, Evo Morales and that of Google. 'See Europeans seek answer from US on NSA' retrieved from http://www.voafanti.com/gate/big5/m.voanews.com/a/1780454.html on October 30, 2013. See also "Snowden leaks: Google 'outraged' at alleged NSA hacking" retrieved from http://www.bbc.co.uk/news/world-us-canada-24751821.

[743] See for example the cases of *FRN vs. Nvene and FRN vs. Maduka Nnamdi (Supra).* Police in Nasarawa state arrested a syndicate which specialized in cloning ATM cards to withdraw money from bank accounts of unsuspecting person. The syndicate was made up of made underground students of Enugu State University of Science and Technology and Nnamdi Azikiwe University, Awka, who were arrested while trying to withdraw cash from people's account using the cloned cards. See *Daily Trust.* Monday, November 23, 2009, p.5. Also in 2009, a Federal High Court sitting in Enugu sentenced a graduate of Chemical Engineering of Enugu State University of Science and Technology, Nwanya Odichukwu to 12 years imprisonment over fraud and internet scam. The convict was arrested while sending scam mails at Logon Nigeria Multimedia Cyber Café, located at Chime Avenue, New Haven, Enugu during a raid. Operatives of EFCC who searched his residence recovered a parcel containing an international cashier valued $2 million; a Central Bank of Nigeria draft valued at $500,000 in the name of one Mr. B. R. Butler, a United Kingdom international passport bearing the name of one Jackson Phillips Dennis as well as scanned US Dollars document. See *Daily Trust*. Tuesday, November 10, 2009, p.7.

[744] For example the EFCC, in a Public notice alleged that one Godswill Oyegwa Uyoyou is wanted in connection with a case of criminal conspiracy obtaining money under false pretence and electronic transfer of funds. Godswill, an IT staff of a new generation bank is alleged to have fraudulently connived with some scammers and hacked into his bank's database and obtained the sum of N6,028,000,000 (Six billion and twenty eight million naira). See *The Nation*. September 8, 2014, p.47

[745] See Ladan, M.T. (2010) *Op.cit.*, pp.17-22; Recent studies however revealed positive improvement and commendation in Nigeria's rating among committee of nations by international crime prevention and enforcement institution. See Ladan, M.T. (2013). 'An Appraisal of Legal, Regulatory and Institutional Frameworks in Combating Money Laundering and Terrorism Financing in Nigeria.' Retrieved from http://ssrn.com/abstract=2336025 on August 4, 2015 at 12.46am, see also Ladan, M.T. (2010). *Op.cit.*, pp.9-42.

institutional measures include but are not limited to the *AFFA 2006*, the *EFCC Act 2004*, which established the Economic and Financial Crimes Commission and the recently enacted *Cybercrimes Act, 2015*. In this regard, the study examined the efficacy of the legislative and institutional measures.

In chapter two of the study, attempt was made in providing conceptual clarifications and definitions of some basic terms relevant to the research. Such terms include concepts of artificial intelligences, cyberspace, crime, cybercrimes, cyber jurisdiction, cyber law and cyber security among others. The study revealed that cyberspace spawns cybercrimes because the internet has provided new opportunity for new crimes to emerge. Cyberspace is not a fixed predetermined reality operating according to principles and dynamics that cannot be controlled or altered by man. It is a contracted world, a fabrication that is constant. Criminal actors do not exist in cyberspace, rather, they exist in the physical world and their actions traverse the real world as well as the cyberspace, impacting victims in the real world. With respect to the concept of crime, crime is universal but inevitable in any human society. As a concept, crime has defied a universally acceptable definition. Nevertheless, crime was seen as that act or omission which the state has prohibited or commanded.[746] It thus goes without saying that if any act or omission has not been criminalized by the code or any criminal statute such an act or omission, however heinous, cannot be regarded as an offence in the eyes of the law.[747]

With respect to criminal responsibility, it has been settled that liability in crime is always a function of what the actor believes regarding the nature and consequence of his conduct and what reasons are for acting as he or she does in the light of those beliefs.[748] Thus, criminal responsibility is the legal liability for ones act or omission. It applies to that in which the accused may be responsible for his or her act which constitutes a crime thus making him or her subject to conviction or punishment. To constitute a crime, the intent and the act must

[746] See *R. vs. Tyler* 2 Q B 594
[747] Section 36 (12) of the *CFRN* , 1999.
[748] See Alexander, L. and Ferzan, K.K. (2009) *Op.cit.*, p.41

both concur. That is, the guilty mind *(mensrea)* must coincide with the prohibited act *(actus reus)*. Generally therefore, there is no liability under criminal law unless there is a guilty mind.

In cybercrimes, the component of *actus reus* is easy to identify, it is however, not easy to prove. The commission of the offence may not be in doubt, the problem is the proof of its commission because most steps are electronic in nature.[749] For example, in the offence of cyber fraud, it may suffice if a person sends unsolicited mail to an intended victim or where he or she fills out an online internet order form and eventually claim the proceed of his or her scheme. Every time such a person uses the internet to prosecute his criminal act, the computer performs certain functions which can be said to constitute *"actus reus.*" Nevertheless, recourse has to be made to the laws creating cyber offences to determine the *mensrea* of cyber criminals.[750]

We have seen that the development in computer science and technology led to the emergence of new species of crimes popularly known as cybercrimes. Cybercrimes are criminal acts, the execution of which computers, computer networks and electronic super highway are involved. They involve the use of a computer either as an instrumentality, targets or means of perpetrating further crime. Cybercrimes include credit card fraud, hacking, distribution of viruses and worms. The growth in this new genus of crimes present additional challenges to the legal and institutional frameworks put in place to combat crime generally. The internet, for example, makes it possible for cyber criminals to be located anywhere in the world and to hide their location. Besides, even where the location can be determined, it may be difficult or impossible for the country which was victimized to get jurisdiction over the criminals. The internet has opened a new vista for inter-state conflicts. Cyber warfare makes it possible for countries particularly the developed world to undermine the security and

[749] See Ashaolu and Oduwale (2009) *Op.cit.,* p.15
[750] *Ibid*., p.16

general well-being of other countries.[751] The activities of cyber criminals have resulted in severe economic and financial consequences to individuals, corporate groups and governments, the world over.[752] The specific implications may not be ascertainable because most victims hardly report their losses.

Chapters three and four of the research examined the legal and institutional frameworks for combating cybercrimes in Nigeria respectively. The chapters focused on judicial decisions with respect to some offences under the *Economic and Financial Crimes Commission,* the *Advance Fee Fraud and Other Fraud Related Offences Act* and the *Cybercrimes Act, 2015* being the existing legislation on cybercrimes in Nigeria. Chapter three further made an overview of the development of the legislation for combating cybercrimes in Nigeria. Here, recourse was made to the *Computer Security and Critical Infrastructure Protection Bill 2005, Cyber Security and Data Protection Agency Bill 2008, Electronic Fraud (Prohibition) Bill 2008, Cyber Security Bill, 2011, Cybercrimes Bill 2013* and more particularly the Nigeria *Cybercrimes Act 2015* were examined. Recourse was also made to some municipal legal regimes of selected countries such as United Kingdom, United States, India and South Africa with the view to appreciate the global best practices and how they influence Nigeria's quest at combating cybercrimes. The fact that Nigeria is still rated among one of the most cybercrimes' vulnerable countries in the world is indicative of the failure of these legislation and enforcement institutions enacted/established to check the menace of cybercrimes in Nigeria.[753] The Nigerian criminal law originates from the legal principles that

[751] Recent revelations by Edward Snowden indicated that the United State has been spying on Nigeria's security agencies, especially the State Security Services (SSS), and probably the presidency. In a report published in New York Times, Snowden, the American computer specialist who worked in the US Central Intelligence Agency (CIA) and as a contractor with the US National Security Agency stated that Nigeria's SSS was one of the security agencies across the globe that the US NSA had been listening on. That briefs on information gleaned from intercepting of telephone conversation and hacking of computers of the SSS, other security agencies in Nigeria and other countries are delivered to the Office of the US President, Barrack Obama every morning. See Okpi, A. 'US Spies on Nigerian Security Agencies.' Retrieved from http://www.punchng.com/news/us-spies-on-nigeria-security-agencies on November 3, 2013 at 3.39am

[752] It has been reported that cybercrimes now cost the world over $114 billion (One hundred and fourteen billion dollars) annually. See http://leadership.ng/news/231013/vote-cyber-security-bill-2013, on October 23, 2013 at 4.15am

[753] Nigeria is still listed third in a Report on Global Cybercrime Statistics behind the United Kingdom and United States, by the Internet Crime Complaint Centre (IC3), a joint operation between the FBI and the National

were developed several decades, if not centuries ago. These legal concepts, it is submitted, were not designed to cope with today's advancing technology nor were the traditional methods of detection, investigation and prosecution of crimes designed to bring cybercriminals to book.

Furthermore, the government in Nigeria has put in place some institutional measures for combating cybercrimes. Such measures include the Nigeria Cybercrimes Working Group (NCWG), an inter-agency body comprising law enforcement, intelligence, security as well as ICT agencies. The NCWG is made up of the National Information Technology Development Agency (NITDA), Nigerian Communications Commission (NCC), Department of State Security and Economic and Financial Crimes Commission (EFCC) among others. It is worthy to note that the EFCC is the key agency of the Federal Government established and mandated to combat economic and financial crimes to which cybercrimes are species. The EFCC is empowered to prevent, investigate and prosecute economic and financial crimes and is charged with the responsibility of enforcing the provisions of other laws relating to economic and financial crimes.[754] Advance fee fraud which is listed under the schedule of responsibilities of the EFCC has been a major source of embarrassment to the image of Nigeria.

It is observed that the activities of cyber criminals pose new and difficult challenges for enforcement institutions. The anonymity and global connectivity let the cyber criminal engage online in traditional crimes such as extortion, fraud and pornography on a greatly

---

White Collar Centre. The top ten list includes the United States, The United Kingdom, Nigeria, Canada, Romania, Italy, Spain, South Africa, Russia and Ghana. Scammers living within the United States most often lived in California, Florida, Georgia, Illinois, New York, Pennsylvania and Texas. Men are reported to lose more money to online fraud than women, and also recorded 75% of cybercrime perpetrators. See 'Nigeria, South Africa, Ghana Top Cybercrime in Africa.' Retrieved from www.nairaland.com on August 26, 2014.

[754] The EFCC is the coordinating agency for the enforcement of the provisions of the *Money Laundering Act 2004*; *Advance Fee Fraud Act 2006; Failed Banks (Recovery of Debt and Financial Malpractices in Banks) Act; Banks and Other Financial Institutions Act; Miscellaneous Offences Act;* and any other law or regulation relating to economic and financial crimes including the *Criminal* and *Penal Codes.* See section 7(2) (a)-(f) of the *EFCC Act 2004.*

expanded scale.[755] Crimes can now be committed across national borders or from different continents. Criminals do not need to be physically present to commit the crime. This reduces the risk of capture and prosecution and makes the job of enforcement institutions much harder.[756] The task of identifying, investigating and successfully prosecuting cyber criminals pose ever increasing challenges to enforcement institutions across the globe.

Chapter five dwelt on summary, findings, recommendations and conclusion.

5.3 Findings

We have, from the preceding chapters, noted the Nigerian legislation and institutional measures put in place with the view to curb the menace of cybercrimes perpetrated mainly by Nigerian nationals within and outside the country. While it is conceded that Nigeria has in existence some legislation prohibiting the offences of cheating, obtaining property by false pretence, fraud and related offences,[757] the inadequacy of the legislative measures to combat the various types of cyber specific offences are quite clear and manifest. Some of the legislation[758] were enacted to provide for traditional offences and did not envisage the circumstances where such traditional offences could assume the sophistication and extra-territoriality they are presently through the medium of cyber space.[759] The findings of this study revealed the following:

[755] See McAfee Virtual Criminology Report. North American Study into Organised Crime and the Internet. Paper Written for Council of Europe's Octopus Interface Conference, Strasbourg, France. 10-11 March, 2009. Retrieved from www.mcafee.com/us/localcontent...report.pdf on January 12, 2014 at 8.52pm

[756] *Ibid.*

[757] See for example, sections 419 and 421 of the *Criminal Code;* sections 17 and 320 of the *Penal Code* and sections 1, 3, 4, 5, 6 and 8 of the *AFFA 2005.*

[758] Such as the *EFCC Act, 2004* and the *AFFA, 2005*.

[759] Here, the issues of cyber warfare, cyber terrorism and attacks on critical national infrastructure by countries against one another readily comes to mind. For example, on November 24, 2014, the Sony Pictures Entertainment was hacked. Employees were locked out of their computer network and glowing, red skeletons appear on their screens. An accompanying message says they have been "Hacked by Guardian of Peace #GOP" and all their internal data have been obtained and can be shared. The FBI alleged that North Korea was behind the attack because Sony Pictures upcoming comedy *The Interview,* was about an assassination attempt on Kim Jong Un, the North Korean President. North Korea denied involvement but the US President, Barrack Obama threatened retaliation as a result on December 22, 2014, North Korea experienced internet outage for hours including connectivity issues which continued for several days. Retrieved from www.usatoday.com/stroy/news ... on April 30, 2015 at 5.26am.

5.3.1 The Use of AFFA 2006 to Combat Cybercrimes in Nigeria

Prior to the enactment of the *Cybercrimes Act* in May 2015, cyber criminals were frequently charged under the *AFFA 2006* as a result of the absence of specific legal frameworks for combating cybercrimes in Nigeria.[760] Enforcement institutions lost cybercrime cases in the absence of precise computer crime legislation. Solving this problem led to the enactment of cybercrime legislation drafted with the view to sufficiently provide for the specific offences of cybercrimes.

5.3.2 Lack of Judicial Consistency in Terms of Punishment of Cyber Offenders

The research also found that offenders were not made to face the full wrath of the law with severe penalties as provided under some of the laws.[761] This perhaps accounted for the disparity in punishment given by the courts and/or absence of judicial consistency in terms of punishment for cyber offenders.[762] Equally revealing is the attitude of the Nigerian courts to issues of prosecution of cybercrime cases before them especially with respect to applying the appropriate penalties to established cases of cybercrimes. We have seen instances where the courts issued sentences far below that provided by the laws and court issuing different punishments for the same offences committed by different persons.[763] In the case of *FRN vs. Prince Raphael Akpiaifo (supra)*, for example, the court served as a clog in the wheel of cybercrime prosecution by discharging the accused person who hacked into the e-mails of the nominal Complainant and carted away the sum of N75,000,000 being monies of the nominal Complainant.

5.3.3 Absence of Political Will on the Part of Nigerian Government at Combating the Menace of Cybercrimes

The research also found that the pre-May 2015 state of Nigerian cybercrimes legislation show lack of political will and insufficient attention on the part of the Nigerian

[760] See Table 1 for the EFCC Record of Convictions for the year 2013.
[761] This point has been illustrated through the cases referred to above. See also for example serial no. 1, 2, 5, 16, 23, 30, 69, 73, 74, 76, 91 and 95 of the EFCC Record of Convictions 2013
[762] *Ibid.*
[763] For example of cases where courts dished out different punishments for the same offences committed by different persons, see serial no. 1, 2, 12, 13, 16, 24, 46, 48, 52, 70, 76, 95, 105, 109 and 110 of the EFCC Record of Convictions 2013.

government to combat the menace of cybercrimes as it took the Nigerian Government nearly ten years to enact only one out of the hitherto numerous Cybercrime Bills pending before the National Assembly. It is concluded that with that unnecessary delay on the part of the Nigerian government, the government has failed the expectations of Nigerians with respect to the fight against cybercrimes. Until recently none of the two arms of Nigerian government comprising the legislature and executive exhibited the requisite political will to combat the scourge of cybercrimes in Nigeria. That absence of political will on the part of the Nigerian government revealed the absence of genuine commitment aimed at combating the crimes in Nigeria.

5.3.4 Dearth of Trained Staff or Personnel with Necessary Technical Skills and Tools to Respond to Cyber Attacks

Besides, there is the dearth of trained staff or personnel with the necessary technical skills, know-how or resources for investigating and prosecuting offenders. Without trained personnel who have expertise on the collection of computerised evidence, important evidence may be lost or destroyed. The lack of an established knowledge base on computer crimes has created the potential for an ineffective response to the problem of cybercrimes. Cybercrimes are information and intelligence based activities as such cannot be fought with ignorance. It is noted that enforcement institutions will continue to lose cybercrime cases in the absence of requisite knowledge, skills and ethics of computer and internet technology.

5.3.5 Absence of Public Awareness and Enlightenment on the ills of Cybercrimes

The research further found that victims of cybercrimes, especially corporate personalities cover computer crime cases and report less. It is submitted that a thorough reporting system is necessary for prevention, investigation and prosecution of cybercrime cases. Awareness of risk associated with cybercrimes and how to mitigate them does not seem to be spreading quickly as the escalation in the use of cyber technology.[764]

[764] In 2006, for example, the African Information Security Association (AISA) was established to promote knowledge and create awareness about computer security and cybercrimes. The United Nations African Institute for the Prevention of Crime and Treatment of Offenders lunched the African Centre for Cyber Law and

5.3.6 Absence of Reliable System for Cooperation between and/or among the Enforcement Institutions within and without the Country

There is absence of reliable system for cooperation between and/or among the enforcement institutions within and without the country. Despite the effort made under the NCWG to encourage collaboration between and/or among the enforcement institutions that made up the body, the NCWG ended in disputes and/or crises as to which of the agencies should enforce the anti-cybercrimes legislation and as such ended without making any meaningful headways in their quest at combating cybercrimes in Nigeria.

5.3.7 Corruption, Poverty and Unemployment

Again, the increasing incidence of cybercrimes cannot be divorced from the high rate of corruption, poverty and unemployment bedevilling the Nigerian society. It is observed that it is poverty that has compromised the security situation of the nation.[765] It is what breeds criminality. And this poverty is engendered by the corrupt practices of those who govern the country.[766] In the United States, the internet has created a boom in its economy, but it was the government that did the initial hard work and the investment to create the internet in the first place that made it possible for entrepreneurs to create Ebay, Yahoo, Google and Facebook. Government should busy itself with how to make life easier for the people through policies and interventions that create jobs and eradicate poverty.[767] This point was noted by Ladan[768] and this researcher concedes to the same that more attention should be paid to solving the psycho-social, socio-economic and socio-cultural problems causing crimes in Nigeria.

5.4 Recommendations

Base on the findings above, the following recommendations are hereby made.

Cybercrime Prevention (ACCP) in Kampala, Uganda in August 2010 in response to mobile phone banking. The ACCP set itself the ambitious task of monitoring cyberspace abuses and the incidence of cybercrimes in Africa. However, not much of its activities can be seen or appreciated.

[765] Nda-Isiah, S. 'Did Jonathan know it was World Poverty Day?' *Leadership*. October 22, 2012

[766] *Ibid.*

[767] *Ibid.*

[768] Ladan M. T. (1995) *Op.cit.,* pp.456-458

5.4.1 Legislative Reform

Cybercrimes are major problems that have to be addressed. The National Assembly has enacted the anti-cybercrimes regime that would stop specific cybercrimes. Hitherto, the *Advance Fee Fraud Act 2006* was the predominant law for combating cybercrimes in Nigeria and as we have earlier noted above, it was inadequate to address the problem of specific cyber offences. Therefore, there is the need for further developments and amendments of the legislation to specifically address emerging cyber offences and to harmonise the same with global best practices.[769] Nigeria needs additional laws and systems that will not only reduce cybercrimes and criminality but to provide security and safety in cyberspace. Nigeria, like South Africa, should sign the European Convention on Cybercrimes so as to benefit from its cooperative and collaborative provisions, particularly with the more advanced countries in cyber technology. It is thus clear that amendment to the current legal regimes such as the *Advance Fee Fraud Act 2006* is needed in order to guarantee and protect the citizenry against cyber attacks and criminality. An amendment of the Nigerian *Advance Fee Fraud Act 2006* with the view to incorporate the similar provisions as contained in the *UK's Fraud Act 2006,*[770] though with necessary modifications to suit our peculiar circumstances may provide additional remedy to the situation. Recourse should be had to best practices in the United Kingdom such as its *Anti-Fraud Act 2005.* The United States cyber law provisions are not necessarily a positive model for Nigeria or any other country to follow. The United States provisions are vague and thus open to arbitrary enforcement and abuse than proper protection of individual liberties.[771]

---

[769] Aaunshi, S. and Srinidhi, R. (2012) *Op.cit.* identified 74 types of Cybercrimes and it is posited that new species are emerging. The *Cybercrimes Act, 2015* though passed and assented in May 2015, provides for only 29 types of offences.

[770] The UK's Fraud Act 2006 brought in a number of offences appropriate to tackle ICT fraud including dishonestly transferring funds electronically, phishing, using fake websites to obtain personal details such as bank account details, spyware and dishonest use of telecoms and information services. See Bainbridge, D.I. (2008) *Op.cit.*, p.433.

[771] Under the US *Patriot Act* for example, civil liberties, especially privacy rights have taken a severe blow. The law expands the ability of the state and the federal government to conduct surveillance on everybody including the US citizens. Government spying on suspects or individuals requires no court order. It eliminates government accountability by creating more secrecy for government activities, making it difficult to know about actions the government is taking. US *Patriot Act* allows law enforcement agents to enter private premises without the

5.4.2 Institutional Reform

Nigeria has been criticised for dealing inadequately with cybercrimes as its law enforcement agencies are inadequately equipped in terms of personnel, intelligence and infrastructure and the private sector is also lagging behind in curbing cybercrimes.[772] Cybercrimes cannot be fought by faulty means. Threat of arrest, detention and jail terms by the EFCC, the police and the courts do not seem to be effective enough. If a case of crime or alleged cybercrime will take 4 or 6 years from High Court to the Supreme Court,[773] how can anybody be deterred? There is need for quicker resolution of court cases and imposition of stiffer penalties for offenders. And the laws establishing these bodies are not only conflicting, duplicating and overlapping, the operation of the laws makes the enforcement not only faulty but ineffective. It is the view here that more international mutual legal and technical assistance should be rendered to African countries by corporate and individual entities to effectively combat cybercrimes.[774] Most importantly so because law enforcement agencies in Africa and Nigeria in particular are not adequately equipped with the necessary skills and manpower required to investigates and prosecute cybercrimes. The law enforcement personnel are not equipped with the requisite technological knowledge while most cyber criminals are expert in computer technology.

In combating these crimes there is the need for education and human capacity development which is one of the most viable strategies. Universities, schools of higher learning and academic institutions should device specific courses designed to allow the next generation of law enforcement agents, judges and lawyers become skilled in the area of

---

occupants permission or knowledge and without informing the occupant that such a search was conducted. For more information on the US *Patriot Act,* see 'Analysis of the Provisions of the US *Patriot Act* that Relates to Online Activities.' Retrieved from http://w2.eff.org//privacy/surveillance/terrorism/20011031-eff-usa-patriot-analysis.php on October 27, 2013.

[772] Ani, L. (nd) *Op.cit.*

[773] See for example the case of *Amadi vs. FRN (Supra),* which was commenced on 13th September, 2004 before the High Court of Lagos State, Ikeja Judicial Division, but was finally determined by the Supreme Court of Nigeria on 19th December, 2008 (more than 4 years).

[774] *Ibid.*

cybercrimes.[775] The *Cybercrimes Act 2015* empowers the Cybercrimes Advisory Council to promote graduate traineeship in cybersecurity, computer and network security research and development.[776] This, it is conceded, is a step in the right direction. It is hoped that the effort should not be paper based only, but practical steps be taken to actualize it.

It is clear that the existence of legislation which addresses specific type of criminal activity is not, in itself sufficient to tackle the problem of cybercrimes. It is essential to ensure that the law enforcement agencies understand the problem and have the resources to deal with it. Unfortunately, the law enforcement agencies in Nigeria have little knowledge and expertise to deal with cybercrimes. It may be necessary as such to increase the number of trained personnel in cybersecurity as well as create a dedicated agency to address the problem of cybercrimes in Nigeria.[777] Aptly put therefore, government in Nigeria should make a deliberate policy empower the enforcement institutions through ICT training and education.

Besides, it is the view that without enforcement tough laws have no effect on reducing crimes, and may foster general doubt about reform efforts. Enforcement institutions become ineffective because of their inability to tackle crimes and criminality in Nigeria. In Nigeria, all hope is not lost, there appears to be a light at the end of the tunnel. The EFCC, according to its Head of Cybercrimes Unit, Lagos office, has enjoyed international cooperation with respect to training from the Interpol, FBI, FATF and Microsoft organisation. The FBI for example, assigned an agent to work exclusively with Nigeria's EFCC. This trend is positive and should be encouraged and commended, however, with caution so as not to leak our sensitive security measures to our foreign trainers. Thus, enforcement institutions should

[775] *Ibid.*; This view seem to have been recognized and appreciated by the framers of the National Cybersecurity Policy and Strategy.
[776] Section 43(1)(e) of the Act.
[777] In response to the rising cases of cybercrimes in the United Kingdom, the United Kingdom government in April 2001 established a National Hi-Tech Crime Unit designed to provide coordinated response to cybercrimes. It worked closely with specialists from a range of agencies including National Crime Squad, Her Majestic's Revenue and Customs and The National Criminal Intelligence Service. The National Hi-Tech Crime Unit recorded some notable successes. These include the arrest of Russian hackers responsible for threatening online bookmakers with Distributed Denial of Service (DDOS) Attacks in a joint operation with Russian law enforcement agencies; and the arrest of those responsible for trying to steal money from the London branch of the Japanese *Sumitomo Mitsini* Bank in October 2004. See *The Register.* March 19, 2009.

strive towards keeping up with technological and security advancements through ICT training and education.

5.4.3 Need for Strategic Implementation and Enforcement of the Anti-Cybercrimes Legislation and the Support of the General Public

There is the need for strategic implementation and enforcement of the anti-cybercrimes legislation. Unless this becomes the culture, the current and prevalent culture of impunity will hinge and it will be difficult if not impossible to address the issue. The criminal law alone, it is argued, is not sufficient for the prevention and control of crime.[778] The moral tone of the society must be raised. Recourse should be heard to religious institution for coaching. If this is done members of the public would hopefully internalize these values and be more predisposed to obey the law.[779] The cultivation of such value standards, it is further observed, will hopefully reduce if not eradicate the commission of crimes against property and against the economy which have dishonesty or fraudulence as state of mind of the offenders.[780] It is evident from above that the issue of crime in Nigeria cannot be fought by legislation alone. Serious efforts should therefore be made to remove the socio economic injustices and inequalities which are some of the factors that facilitate and allow crime and criminality to flourish in Nigeria. The war against crimes generally should first be fought in the minds of the people with the leaders showing good example in probity and accountability.[781] The research supports the introduction of anti-cybercrimes studies in our educational institutions.[782]

5.4.4 Coalition and Collaborative Approach in Combating Cybercrimes

In countries that have successfully reduced the incidence of crime, one key lesson learned is the need to adopt a coalition and collaborative approach to the problem. The government takes the lead but must develop and nurture relationship with the anti-cybercrimes groups in the private and voluntary groups. The first step to coalition approach

[778] Ladan, M. T. (1998) *Op.cit.* p. 525.
[779] *Ibid.*
[780] *Ibid.*, p.526
[781] Omotunde, S. 'EFCC: Still chasing shadows' *Thisday*. November 26, 2004, p.14.
[782] Ani, L. (nd) *Op.cit.*, p.232

in fighting crime is the unified commitment from the three arms of government at both federal and state levels.

Institutional cooperation among the various enforcement agencies is equally critical in the fight against cyber related crimes. Absence of effective system of multi-lateral cooperation will hamper the fight against cybercrimes. Mechanisms are now in place that allows the law enforcement agency of one country to assist another to investigate and prosecute criminals and to freeze confiscated proceeds of crimes. To succeed in the fight against cybercrimes in Nigeria, enforcement institutions must cooperate by sharing information and intelligence among themselves and their foreign counterparts with the view to preventing the commission of crimes.[783]

It is instructive to note that lack of cooperation and duplication of efforts by the enforcement agencies is one of the factors militating against the successful war against cybercrimes.[784] There is therefore the need to harmonise the activities of the enforcement agencies with the view to making them more efficient. Under the *Cybercrimes Act, 2015*,[785] the Office of the National Security Adviser (ONSA) is empowered to coordinate all security and enforcement agencies under the Act and shall in the process provide support to all relevant security, intelligence, law enforcement agencies and military services to prevent and combat cybercrimes in Nigeria.

5.4.5 Role of Press, Civil Society Organizations and Workshops

It is has been identified that the absence of public awareness and enlightenment on the ills of cybercrimes are responsible for the escalation of the incidence of cybercrimes in Nigeria. The press plays very important role in creating awareness and mobilizing political will for reform. It is the view here that the press is the watch dog against all forms of abuses, crimes inclusive. In exposing criminal acts, the press elicits popular indignation about crimes

[783] This has been emphasized in section 43(1)(a) of the *Cybercrimes Act 2015* and Para. 4.3.2 (ix-x) of the Nigerian National Cybersecurity Policy.
[784] We have noted how the fight for supremacy and control by members of NCWG led to its failure to achieve its stated objectives of providing mechanism for effective fight against cybercrimes in Nigeria.
[785] Section 41(1) (a-h) of the Act

and put pressure on the government to change. It is this risk of exposure that motivates government to sometimes censor the press. It is therefore instructive to organize training for journalists about professional standards, and their role in creating public awareness against the risks involved in cybercrimes. This is necessary because more information is required on forms and trends of cybercrime. This, it is submitted might stimulates an improvement in cybercrime reports which will enable better databases to be compiled. It is our view that enhanced databases can support more pro-active investigation as well as the identification of crime networks. Thus, raising public awareness on ills of cybercrimes and methods of combating the same will go a long way in minimising the risks.

Given the rapid proliferation of smart phones, it is suggested that all users should be informed of the main risks and realities of cybercrimes. Besides, service providers should be required to secure all devices they distribute.[786]

Civil society organizations, where they are free to act can become partners on developing and strengthening ethical practices in the society. A number of civil society organizations have emerged to fight cybercrimes.[787] Most prominently, civil society organizations can be strong advocates for government reform and at the same time effective champions of moral and professional standards.

Workshops offer effective avenue for changing attitudes about ethics and moral behaviour and mobilizing political will for change. Workshops on cybercrimes strive to increase understanding of cybercrimes and to generate political strategies for reducing it. It is a tool for sustained public enlightenment campaign and education about the menace of cybercrimes and possible ways of checking same. Workshops could therefore be used to educate people on the ills of cybercrimes.

[786] See 'Predatory Cybercrime in South Africa: Current Risk and Realities.' Retrieved from www.isn.ethzch/ digital/detail… on March 4, 2014 at 5.12am

[787] See for example, the Nigeria 419 Coalition. A non-governmental organization whose mandates include creating awareness against cybercrime and campaigning for legislative reform with respect to cybercrimes.

5.5 Conclusion

It is clear that cybercrimes are not going to disappear. This should not surprise us because while cybercrimes are unwanted side effects of the internet age, they are also part of a broader crime landscape. If there is a use for something, someone will always find a way to abuse it and this includes computer technology and the connectivity provided by the internet. One must concede that crime and criminality can never be eliminated in the society, as such, tackling cybercrimes is about mitigating the risks associated with using the internet and not about completely winning the war against cybercrimes.[788] To manage the risk, Nigeria and the global society clearly needs a legal framework together with appropriate and effective law enforcement agencies.[789] In particular, the extension of international legislation beyond developed countries and the development of 'cyber-interpol' to pursue cyber criminals across geo-political borders would contribute immensely to the fight against cybercrimes. Law enforcement is only part of the problem, there is the need to ensure that individuals and businesses understands the risks and have the knowledge and tools to minimise their exposure to cybercrimes. This is important for individuals who are often technically inexperienced and have little understanding of the potential problems associated with online shopping, internet banking and social networking. The problem is exacerbated by the growing number of people accessing the internet for the first time. Nigeria must find ways of raising public awareness about cybercrimes and about methods which can be used to mitigate the risk. Simply put, we need a blend of appropriate legislation, effective enforcement and public awareness to succeed in the fight against cybercrimes in Nigeria.

[788] Crime is an inherent part of modern society and touches almost every aspect of life. It is hardly surprising, therefore that the use of computer technology is mirrored by abuse; they have developed in parallel. Besides, as more and more areas of human lives become dependent on computers, there is more scope for criminals to use technology. In response to any type of crime, society always attempt to find ways to prevent the crime and punish the perpetrators. In the first instance, this means creating legislation which makes specific activities illegal.

[789] Law enforcement agencies such as the FBI and the Interpol for example, have developed increasing expertise in dealing with hi-technology crimes, including joint policing operations across national borders. This must be further developed if we are to deal effectively with cybercrimes.

BIBLIOGRAPHY

BOOKS

Akinseye-Goerge, Y. (2000). *Legal System, Corruption and Good Governance in Nigeria.* New Century Law Publishing, Lagos

Ashaolu, D. D. and Oduwale, O. A. (2009). *Policing Cyberspace in Nigeria: A Publication in Honour of Col. Sani Bello (Rtd).* Life Gate Publishing Co. Ltd., Ibadan.

Babaji, B. "Cybercrimes under Nigerian Law" In: Chukkol, K. S. (2010). *The Law of Crimes in Nigeria*. A.B.U., Press Ltd., Zaria

Bali, O. (2002). *Information Technology and the Law: The Nigerian Perspective*. Legal Digest Publishing, Lagos

Brill, E. A. Baldwin, F. N. and Munro, R. J. (2001). *Cybercrimes and Security*. Oceana Publications Inc., U.S.A., Vols.1, 2 and 3.

Dambazzau, (1994). A.B. *Law and Criminality in Nigeria: An Analytical Discourse*. University Press Plc, Ibadan.

Genesis 2:16-17

Genesis 3:1-24.

Genesis 4:1-8

Haralambo, M. and Heald, R.M. (1983). *Sociology: Themes and Perspectives.* University Tutorial Press Ltd, Britain

Hon, S. T. (2013). *Law of Evidence in Nigeria.* Pearl Publishers, Port Harcourt, Rivers State.

Ladan, M.T. (1998). *Crime Prevention and Control and Human Rights in Nigeria*. Justice Watch, Abuja

Ladan, M.T. (2003). *Introduction to Jurisprudence: Classical and Islamic.* Faith Printers International, Zaria

Ladan, M.T. (2015). *Cyber Law and Policy on Information and Communications Technology in Nigeria and ECOWAS.* A.B.U. Press Ltd., Zaria.

Lawrence, L. (1999) *Code and other Laws of Cyperspace.* Basic Books, NewYork, U.S.A.

Nigeria's National Cybersecurity Policy. December, 2014.

Ocheme, P.A. (2006). *The Nigerian Criminal Law*. Liberty Publications Ltd, Kaduna, Cap. 4

Osinbajo, Y. (2001) *Cases and Materials on Nigerian Law of Evidence.* Macmillan Publishers, Lagos

Osinbajo, Y. Electronically Generated Evidence. In: Babalola, A. *Law and Practice of Evidence in Nigeria.* Sibon Books Limited, Ibadan

Paranjape, N.V. (2010). *Criminology and Penology*. 14th ed. Central Law Publications, Allahabad, India

Qadri, S.M.A. (2009). *Criminology and Penology.* 6th ed. Eastern Book Company, Lucknow, India.

Qur'an 5:27-37

Safra, J. E. *et al* (1998). *The New Encyclopaedia Britannica.* Vol. 3, 19th Ed. Encyclopaedia Inc. U.S.A.

Smith, J. C. (2002). *Smith and Hogan Criminal Law*. 10th Edition Butterworths LexisNexis, London

Tar, S. (2006) *Law of Evidence in Nigeria: Substantive and Procedural*. Pearl Publishers, Port Harcourt

William, G. (1983). *Textbook of Criminal Law*. 2nd ed. Stevens and Sons, London, Caps 3-7

UNPUBLISHED WORKS

Babaji, B. (2009). Admissibility of Documentary and Electronic Evidence under Nigerian Law. Ph.D Dissertation (unpublished), Faculty of Law, A.B.U., Zaria

Tokura, S. S. (2008). *The Legal Regime of Cyber Security and Crime: Challenges of Enforcement in Nigeria*. LL.M Thesis (Unpublished), Faculty of Law, A.B.U., Zaria.

ARTICLES/CONFERENCE/SEMINAR PAPERS/WEBSITES

Aaushi, S. and Srinidi, R. (2012) *A – Z of Cybercrimes.* Asian School of Cyber Laws. Retrieved from http://ensaiosjuridicos.files.wordpress.com

Abdullahi, I. *et al* (2016) "Cybercrimes (Prohibition, Prevention, etc) Act, 2015: Issues and Challenges in Nigeria." Paper Presented at Nigeria Association of Law Teachers (NALT) Conference, Nasarawa State University, Keffi

Adewale, K.S., Isiaka, R.M., and Olayemi, R.T. (2011) 'An Inquiry into the Awareness Level of Cyber Security Policy and Measures in Nigeria.' *International Journal of Science and Advanced Technology* (ISSN 2221-8386) Vol. 1 No. 7, September. Retrieved from http://www.ijsat.com

Agbajor, C. (2012) 'Senate set to Combat Cybercrimes.' Retrieved from www.Nigeriaob servernews.com

Agbonika, J. A. A. *et al* (2016) "Economic and Financial Crimes: Cybercrime, Money Laundering and Financial Terrorism in Nigeria." Paper presented by Faculty of Law, Kogi State University, Anyigba at the 49th Annual Conference of the Nigerian Law Teachers' Conference, Nasarawa State University Keffi.

Akinsuyi, F. F. (2011). 'Cybercrime Legislative Framework.' Proceedings at Stakeholders' Workshop on Cyber Security Legislation, held on October, 20, at International Conference Centre, Abuja.

Akintola, K. G. *et al* (2011). 'Appraising Nigeria Readiness for E-Commerce Towards Achieving Vision 20: 2020.' Retrieved from www.arpapres.com.../IJRRAS

Akonobi, J. (2008) "The Effect of Cybercrimes on National Economy." Being a Presentation at the National Conference on Cybercrimes and Cybersecurity. Nicon Luxury Hotel, Abuja, August 18-20.

Alexander, L. and Ferzan, K.K. (2009). *Crime and Culpability: A Theory of Criminal Law*. American Bar Association Section Report: Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet, 55 BUS. Law 1801 (2000)

An Appraisal of Legal, Regulatory and Institutional Frameworks in Combating Money Laundering and Terrorism Financing in Nigeria. Retrieved from http://ssrn.com/abstract2336025

Ani, L. (nd) 'Cybercrime and National Security: The Role of the Penal and Procedural Law.' Retrieved from www.nials-nigeria.org

Aseef, N. (2005) "Cyber Criminal Activity and Analysis." White Paper Fall. Retrieved from http://www.virus. Itn.com…xml.

Awomolo, A. (2013). 'Admissibility of Electronic Evidence.' Retrieved from www.awomolo& associates.com

Ayantokun, O. (2011) 'Fighting Cybercrimes in Nigeria.' Retrieved from http://www.tribune.com.ng

Brenner, S.W. and Koops, B. (2004) "Approaches to Cybercrimes Jurisdiction". In *Journal of High Technology Law.* Vol. 4. No.1, (2004) Retrieved from http://www.law.suffolk.edu/highlights/stuorgs/jhtt/docs/pdf/JHT4Brenner-koops-article.pdf

Burns, J.S. and Bales, R.A. (2001) 'Personal Jurisdiction and the Web.' 53 ME.L REV 29

Communique of the 1st West Africa Cybercrimes Summit. Retrieved from www.waccs.net

Cornish, P. (2011) 'The Vulnerabilities of Developed States to Economic Cyber warfare: Working Paper Produced by Chatham House, (2001). Retrieved from www.chataham house.org.uk on June 10, 2012

Crave, W., (2001) 'Legislative Updates: The World Wide Jurisdiction: An Analysis of Over-Inclusive Internet Jurisdictional Law and Attempt by Congress to fix it. J. ART & ENT. L 267

Cybercrimes National Crime Prevention Council. Retrieved from www.ncpc.org.pdf

EFCC Record of Conviction, 2013 at www.efccnigeria.org.

Emke, J. (2008) 'Trends and Shocks and the Impact of the Acquisition Community.' Defence AT & L, 37(1), 3.

Eric, J. S. and William, P. R. 'Cybercrimes: A Practical Approach to Application of Federal Computer Crime Laws.' Retrieved from http://www.law.cornell. edu/uscode/18/1030/htm/…

Esquibel, E. J. *et al* (2005) "Cyber Criminal Activity: Methods and Motivations." Paper Presented for Cyber Security and Homeland Security. University of Washington, CSEP 590TU.

European Commission (2007) "Towards a General Policy on the Fight against Cybercrimes."COM (2007) 267 Final. Retrieved from http://eu.lex.europa.eu/...

Fafinski, S. *et al* (2010) "Mapping and Measuring Cybercrime." Retrieved from www.oii.ox.ac.uk/publications/FD18.pdf

Finklea, K. and Theoary, C. A. (2015) *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement.* Congressional Research Service (CRS) Report Prepared for Members and Committee of U.S. Congress.

Finnie, T. *et al* (2010) "The Future Challenges of Cybercrimes." *Proceedings of the Future Working Group.* Vol. 5

Fox News "Master Card warns of possible security breach, Visa also reported affected" March 30, 2012. Retrieved from Foxnews.com

George-Maria Tyendezwa, T. G. (nd) 'Legislation on Cybercrime in Nigeria: Imperatives and Challenges.' Retrieved from www.ncc.gov.ng...

Gordon, S. and Ford, R. (2006) "On the Definition and Classification of Cybercrimes." *Journal of Computer Virology.* Vol. 2

Haack, S. (nd) "A Brief History of Artificial Intelligence." Retrieved from http://www.atariarchives.org/deli/ artificial_intelligence.php

Halder, D. and Jaishanker, K. (nd) "Cybercrime and Victimisation of Women: Laws, Rights and Regulations." Quoted in Somaiya, J. *et al* (2014) "A Survey of Web Based Cybercrimes and Prevention Techniques." *International Journal of Computer Applications.* Vol. 105.

Hassan, A. B. *et al* (2012) "Cybercrime in Nigeria: Causes, Effect and the Way Out." *ARPN Journal of Science and Technology.* Vol. 2, No. 7, ISSN 2225-7217.

Hassan, A. N. *et al* (2012). 'Cybercrime in Nigeria: Causes, Effects and the Way Out.' *ARPN Journal of Science and Technology*. Vol. 12, No. 7. Retrieved from www.ejournalofscience.org

Hoscheidt, M. M. and Eichner, E. F. (2014) "Legal and Political Measures to Address Cybercrime." World Summit on the Information Society Forum. UFRGS Model United Nations. Retrieved from http://www.ufrgs.br.ufrgsmun/2014/files/ws12.pdf

Internet World's Stats, Internet Usage Statistics: The Internet Big Picture-World Internet Users and Population Stats (2009). Retrieved from internetworldstats.com/stats.htm

Jeyabalan, R. 'Types of Cybercrimes.' Retrieved from http://cybercelimumbai.com/files

Ladan, M. T. (2004) 'The Effectiveness of Legal and Enforcement Framework in Fighting Advance Fee Fraud and Money Laundering Activities.' A paper presented at the 3rd National

Seminar on Economic Crimes, Abuja, June 27-29, Retrieved from www.dawodu.com /Ladan2.htm

Ladan, M.T. (2010) 'International Legal and Administrative Regimes for Combating Money Laundering and Terrorist Financing.' A paper presented at A-2 Day Workshop on Money Laundering Laws and Regulations. Organised by Lintol Resources Base Ltd., Lagos, March 1-2

Ladan, M.T. (2013). 'Recent Trends in Regulating Money Laundering and Terrorism Financing in the Banking, Insurance and Capital Market Sectors of the Financial Economy of Nigeria: Role of the Financial Regulators.' *A.B.U. Journal of Commercial Law (A.B.U.J.C.L.)*, Vol. 6, No. 1.

Longe, B. O. and Chiemeke, C. S. (2008). 'Crime and Criminality in Nigeria - What Roles are Internet Access Points Playing?' *European Journal of Social Sciences*. Vol. 6, No. 4

Longe, O. B. *et al* (2009). 'Internet Service Providers and Cybercrime in Nigeria-Balancing Services and ICT Development.' *Journal of Information, Law and Technology (JILT).* Vol. 7, No. 3. Retrieved from www.jiti.net

Mamandi, K. and Yari, S. (2014) 'A Global Perspective on Cybercrimes.' *Journal of Humanities and Social Science*. Retrieved from www.sciencepublishingroup.com/jhs.pdf.Vol2.No.2

Mamandi, K. and Yari, S. (2014) "A Global Perspective on Cybercrimes." *Humanities and Social Sciences Journal*. Vol. 2, No. 2. Retrieved from http://article.sciencepublishinggroup.com/pdf/...

Mamandi, K. and Yari, S. (2014) "A Global Perspective on Cybercrimes." *Journal of Humanities and Social Sciences.* Vol. 2, No. 2

Mbanaso, U. (2011). 'Technical Perspectives on Cyber Security.' Proceedings at Stakeholders' Workshop on Cyber Security Legislation, held on October, 20, at International Conference Centre, Abuja.

Mc Afee Virtual Criminology Report: North American Study into Organised Crime and the Internet. A Paper written for Council of Europe's Interface Conference. 10th-11th March, 2009, Strasbourg, France. Retrieved from www.mcafee.com/us/localcontent...report.pdf

McAfee Report (2013) "The Economic Impact of Cybercrimes and Cyber Espionage." Center for Strategic and International Studies.

McAfee Virtual Criminology Report. North American Study into Organised Crime and the Internet. Paper Written for Council of Europe's Octopus Interface Conference, Strasbourg, France. 10-11 March, 2009. Retrieved from www.mcafee.com/us/localcontent...report.pdf

McGuire, M, Dowling, S. (2013) "Cybercrimes: A Review of the Evidence." *Research Report 75.* Retrieved from https://www.gov.uk/...pdf

Morano, M. F. (1996). 'Legislating in the Face of New Technology: Copyright Laws for Digital Age.' *Fordham International Law Journal*. Vol. 20, Issue 4, Article 9. Retrieved from http://ir.lawnet.fordham.edu/ilj

Nagre, D. and Warade, P. (nd) 'Cyberterrorism, Vulnerabilities and Policy Issues: Facts behind the Myth.' Retrieved from http://www.andrew.cmu.edu/user/dnagre/cyberterrorism

National Information Technology Policy. Retrieved from http://www.nidta. govs.ng/document/nigeriaitpolicy.pdf

National Security Presidential Directive - 54/Homeland Security Presidential Directive - 23.

Nuredini, S. A. (2014) "Challenges in Combating Cybercrime." *Mediterranean Journal of Social Sciences.* MCSER Publishing, Rome, Italy, Vol. 5, No. 19.

Okpi, A. (nd) 'US Spies on Nigerian Security Agencies.' Retrieved from http://www.punchng.com/news/us-spies-on-nigeria-security-agencies

Olayemi, O. J. (2014) "A Socio-Technological Analysis of Cybercrime and Cyber Security in Nigeria:." *International Journal of Sociology and Anthropology.* Vol. 6 (3). Retrieved from www.academic journal.org/ijsa on October 17, 2016.

Oluwo, D. (2009). 'Cybercrimes and Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa.' *Journal of Information, Law and Technology (JILT).* Retrieved from http://go.warwick.ac.uk/jilt/2009_1oluwo

Oyesanya, F. (nd) 'A Performance Review of EFCC and the Nigerian Cybercrimes Working Group.' Retrieved from http://www.nigeriavillagesquare.com/articles/femi-oyesanya/...html

Oyesanya, F. 'Nigerian Internet 419 on the Loose.' Retrieved from www.nigeriavillagesquare.com/

Oyewume, A. O. (2012) 'The ICT Revolution and Commercial Sectors in Nigeria: Impact and Legal Interventions' *University of Ibadan Law Journal*, Vol.2, No.1

Pati, P. (nd) 'Cybercrimes.' Retrieved from www.naavi.org

Politt, M. M. 'Cyberterrorism Fact or Fancy?' Proceedings of the 20th National Information Systems Security Conference. October 1997

Rajaraman, V. (2014) "John McCathy - Father of Artificial Intelligence" in *General Article Resonance*

Recommendation No. R (89)9, adopted by the Committee of Ministers of the Council of Europe on September 13, 1989 and Report by the European Committee on Crime Problems: Computer-relatred crime. http://cm.cre.int/ta/rec/1989/89rg.htm

Recommendation No. R (95)13, approved by the European Committee on Crime Problems (CDPC) at its 44th Plenary Session, May 29-June 2, 1995: Concerning problems of criminal procedural law connected with information technology. http://cm/coe/int/ta/rec/1995/95r/13.htm

Regulator Shines Path to Cyber Security Challenges in Nigeria. Retrieved from http://www.worldcybersecurityconference.org/new-content php

Ribadu, N. (2007) 'Cybercrimes and Commercial Fraud: A Nigerian Perspective.' A presentation at the Modern Law for Global Commerce Congress to celebrate 40th Annual Session of UNCITRAL, Vienna, July 9-12. Retrieved from www.unicitral.org/pdf/english/congress/ribadu

Schjolberg, S. 'The History of Global Harmonization on Cybercrimes legislation: The Road to Geneva?' Retrieved from http://www.cybercrimeslaw-net/documents/cybercrimes-history.pdf

Schjolberg, S., (1986). Computers and Penal Legislation: A Study of the Legal Politics of a new Technology. Complex 3/86, Universite teforlaget

Sesan, G. *et al* (2012) Economic Cost of Cybercrime in Nigeria. Paradigm the Initiative Nigeria. Retrieved from www.pinigeria.org

Sesan, G. *et al* (2013) *Economic Cost of Cybercrime in Nigeria*, Paradigm Initiative in Nigeria. Report for Cyber Stewards Network Project of Citizen Lab, Munk School of Global Affairs, University of Toronto. Retrieved from www.pinigeria.org/download/ cybercrimecost.pdf

Shazali, I. (2014) "Nigeria Lost N6.2 Billion to Cybercrime." Retrieved from www.vanguardngr .com

Shinder, D. (nd) "What makes Cybercrimes Laws so Difficult to Enforce?" Retrieved from http://www.techrepublic.com/blog/it_security/

Shinder, D.L. (2002). 'Science of Cybercrimes: Jurisdictional Issues and other Special Problem in Enforcing and Prosecuting.' Paper presented at Dallasion Conference on Cyber terrorism

Shubhendu, S. S. and Vejay, J. (2013) "Applicability of AI in Different Fields of Life." *International Journal of Scientific Engineering and Research (IJSER).* Retrieved from www.ijser.in./archives/...

Singleton, T. (2013) AICPA. The Top 5 Cybercrimes. Retrieved from https://www.aicpa .org/...pdf

Singleton, T. *et al* (2013) The Top 5 Cybercrimes. American Institute of CPAS (AICPA), Dirham. AICPA Cybersource Corporation is worldwide e-commerce payment management company.

Smith, C. *et. al.* (2006) "The History of Artificial Intelligence." Retrieved from http://www.courses.cs.washington.edu/courses...

Snow, G.M. (2011) 'Cyber Security: Responding to the Threat of Cyber Criminals.' FBI Report to Chairman, White House Committee on Cyber security. Washington DC, April 2011. Retrieved from http://www.fbi.gov/news/cybersecurity

Susemani, M. A. (1999) "The Critical Challenges from International Hitech and Computer Related Crime at the Millennium." *Duke Journal of Comparative and International Law*. Vol. 9.

Tate, K. (2014) "History of Artificial Intelligence." Retrieved from http://www.livescience.com/...history-of-ai-artificial-intelligence

Tatera, K. (2015) "Using Artificial Intelligence to Take Down Cyber Criminals." Retrieved from http://thescienceexplorer.com/technology/usingartificial_intelligence

Thornburgh, 'Inside the Chinese Hack Attack,' *Times.* August 25, 2007. Retrieved from http://www.times.com/time/nation/printout/...

Traynor, 'Russia Accused of Unleashing Cyber War to Disable Estonia.' *The Guardian,* May 17, 2007. Retrieved from http://www.guardian.co.uk/russia/article/

Types and Incidence of Cybercrimes in Nigeria. Retrieved from http://martinslibrary. blogspot.com.ng

Udotai, B. (2011). 'A Legal Overview of the Draft Legislation on Cyber Security.' Proceedings at Stakeholders' Workshop on Cyber Security Legislation, held on October, 20, at International Conference Centre, Abuja.

United States Bureau of International Narcotics and Law Enforcement Affairs. Retrieved from www.travel.state.gov

Vijayan, J. (2011) "Albert Gonzalez Who is Serving a 20 Year Sentence Wants to Reverse His Guilty Plea." Retrieved from http://www.computerworld.com/...

Wada, F. and Odulaja, G. O. (2012). 'Assessing Cybercrimes and its Impact on E-Banking in Nigeria Using Social Theories.' *African Journal of Computing and ICT.* Vol. 5, No. 1. Retrieved from www.ajocict.net/uploads/wada_Odulaja...

Walden, I. '*Crime and Security in Cyber space.'* Retrieved from http://www.lawnet. Ik/docs/articles/cv47.htm

Wang, S. K. and Huang, W. (2011) "Evolutional View of the Types of Identity Thefts and Online Fraud in the Era of Internet." *Internet Journal of Criminology.* Retrieved from www.internetjournalofcriminology.com

Weil, N. (nd) "Gonzalez sentenced for Multi-million Dollar Credit Card Scam." Retrieved from https://www.pcworld.com...

Weil, N. (nd) "Gonzalez Sentenced for Multi-Million Dollar Credit Card Scam." Retrieved from http://www. pcworld.com/…

Wilson, C. (2008). 'Botnets, Cybercrimes, and Cyber terrorism: Vulnerabilities and Policy Issues for Congress.' Congressional Research Services (C. R. S.) Report for Congress

http://conventions/coe.int/treaty/en/treaties/honl/185.htm

http://eprints.qut.edu.au/43400/1/Ali_Alkaabi_Thesis.pdf

http://europa.en.int

http://fserrov.com/pdf/gonzalezindic timent.pdf.

http://leadership.ng/news/231013/vote-cyber-security-bill-2013

http://w2.eff.org//privacy/surveillance/terrorism/20011031-eff-usa-patriot-analysis.php

http://www.audioenglish.net.

http://www.bbc.co.uk/news/world-us-canada-24751821.

http://www.bbcnews.co.uk/.../technology

http://www.eff.org/Privacy/Surveillance/Terrorism/20011031...

http://www.fatf.gafi.org

http://www.fatf.org/...

http://www.hitechcj.com/computercrime/cyber_crime.html

http://www.hitechcj.comcomputercrime/cyber_crime.html

http://www.interpol.int/crime_area/cybercrime/crime

http://www.interpol.int/crime_areas/cybercrimes/crime

http://www.interpol.int/crime-areas/cybercrimes

http://www.interpol.int/crime-areas/cybercrimes

http://www.interpol.int/news…

http://www.nitda.govs.ng/

http://www.npf.govs.ng/departments/crime-investigation

http://www.reuters.com/article/.../us-usa-wikileaks-manning-idUSBRE97J0JI20130821

http://www.spamlaws.com/types_of_cybercrimes.html

http://www.spamlaws.com/typesofcybercrimes.html

http://www.voafanti.com/gate/big5/m.voanews.com/a/1780454.html

www.abcnews.go.com

www.bbcnews.co.uk

www.bbcnews.co.uk/hi/english/sci/tech/news

www.blackfriars.law.com

www.content.usatoday.com

www.cybercrimes.gove.ng/site/index.php

www.cybercrimesplanetindia.net/intro.htm

www.en.wikipedia.org/.wiki/cyberspace

www.hitechcj.com/computer/cyber _crime.html

www.hitechcj.com/computer_crime/cyber_crime.html

www.isn.ethzch/ digital/detail… on March 4, 2014

www.jidaw.com/security/.../nig

www.nairaland.com

www.nassnig.org/nars/legislation.php?.id...

www.nato.int/kosovo/press/...

www.ponemon.org

www.premiumtimesng.com

www.travel.state.gov

www.usatoday.com/stroy/news

www.waccs.net

www.zdnet.co.uk/story/o,1269./html

NEWS/NEWSPAPERS/MAGAZINES

Adibe, J. 'The Cynthia Osokogu's Case.' *Daily Trust*. August 30, 2012

Bashir, M. 'Defence Headquarters Website Hacked.' *Daily Trust.* September 19, 2012

Daily Trust. August 31, 2012

Daily Trust. February 14, 2011

Daily Trust. Friday, March 26, 2010.

Daily Trust. September 19, 2012

Daily Trust. Thursday, July 29, 2010

Daily Trust. Tuesday, November 10, 2009

Ladeinde, F., (2012) 'Formidable Cyber war Against Iran.' *Daily Trust.* June 4

Muhammad, H. 'Bank Customers Lose over N60,000,000 in ATM scam.' *Daily Trust*. Monday, June 15, 2009

Muhammed, H. 'NCC Clamps down on Illegal ISPs, Cyber Cafes.' *Daily Trust.* Monday, February 23, 2009

Nda-Isiah, S. 'Did Jonathan know it was World Poverty Day?' *Leadership*. October 22, 2012

Ocholi, D. (2010) 'The Internet Revolution.' *Newswatch Magazine.* August 2

Okeke, C. C. (2016) 'Nigeria loses N78 Billion Yearly to Cybercrimes.' *Daily Trust.* January 16,

Olusola, O. 'Yahoo Plus: The New Face of 419.' *The News Magazine*. July 26, 2010

Omotunde, S. 'EFCC: Still chasing shadows' *Thisday*. November 26, 2004

Somaiya, R. ‘Hackers shut Down Egyptian Government Site.’ *The New York Times.* February 3, 2011.

Subsidy Protest: EFCC Site hacked with false arrests of Oil Mogols’ P. M. News Nigeria. January 13, 2012.

The Nation. September 8, 2014

The Register. March 19, 2009.

Woodsome, K. ‘China Tighten Control on Internet Use’ *Voice of America (VOA)* News. December 28, 2013.