AN ANALYSIS OF LEGAL FRAMEWORK ON COMBATING CYBERCRIME IN NIGERIA

By

Eteya OGANA[2]

DEPARTMENT OF PUBLIC LAW,
AHMADU BELLO UNIVERSITY,
ZARIA

JANUARY, 2017

AN ANALYSIS OF LEGAL FRAMEWORK ON COMBATING CYBERCRIME IN NIGERIA

By

Eteya OGANA,
LLM/LAW/97832/2014-2015.

A DISSERTATION SUBMITTED TO THE SCHOOL OF POSTGRADUATE STUDIES, AHMADU BELLO UNIVERSITY, ZARIA IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF LAWS-LLM.

DEPARTMENT OF PUBLIC LAW,
AHMADU BELLO UNIVERSITY,
ZARIA

JANUARY, 2017.

DECLARATION

I, declare that the work in this dissertation titled:AnAnalysis of Legal Framework on Combating Cybercrime in Nigeria has been carried out by me in the Department of Public Law, Faculty of Law, Ahmadu Bello University, Zaria, Nigeria. The information derived from the literature has been duly acknowledged in the text and a list of references provided. No part of this thesis was previously presented for another degree or Diploma at this or any other institutions.

_____
___
Eteya, OGANA
January, 2017

CERTIFICATION

This Dissertation titled An Analysis of Legal Framework on Combating Cybercrime in Nigeria, by OGANA Eteya, meets the regulations governing the award of the degree of Master of Laws-(LLM)of the Ahmadu Bello University, and is approved for its contribution to knowledge and literary presentation.

Chairman, Supervisory Committee Prof., B. Babaji	(Signature)	(Date)
Member, Supervisory Committee Dr A.M Madaki	(Signature)	(Date)
Head of Department, Public Law Dr. K.M Danladi	**(**Signature**)**	(Date)
Dean, School of Postgraduate Studies Prof., S.Z Abubakar.	(Signature**)**	(Date)

DEDICATION

This dissertation is dedicated to God Almighty whom in His Divine providence, grace and favour saw me through my postgraduate studies, and to my late sister Kenah Ogana who always advised me to give thanks for what I am now and keep fighting for what I want to be tomorrow.

ACKNOWLEDGEMENT

I acknowledge first the grace of God for the guidance and protection throughout this array of perseverance.Special thanks to my caring and loving parent Mr & Mrs Madaki Ogana and my silings, for their combined prayers and admonition to make a responsible son out of me. Their encouragement and advice cannot be over-emphasized.

My profound gratitude goes to my amiable supervisors, Prof., B. Babaji and Dr. A.M. Madaki, erudite scholars who has distinguished themselves among their equals I appreciate them for guidance, directives and tremendous effort despite their tight schedules they saw to the success of this work, by also providing me with relevant materials which made this work a reality.

I appreciate the dedication of the following lecturers in the Faculty of Law, Ahmadu Bello University, Zaria Prof, M.T. Ladan, Dr. I.F. Akande,Dr A.A. Akume, Dr J.J Kur, Dr S.A Apeniga and Prof., A. Robert Agom for giving their best in impacting the knowledge of law in me, it is my prayer that God Almighty shall reward you mightily.

This work will not be complete without appreciating my friends and colleagues Mohammad Saleh, Mrs Fatimah Sa'id Ahmed, Barr, Salawu John Onipe, Barr. Dimson Dimas, Barr. S.S Osayi and Barr.Elisha Oloruntoba for their moral and materiel support towards the successful completion of this noble programme.

Mr Yusuf Agana's family, Justina Abimiku and Mr Ibrahim A.Azaki I appreciate you all,I am also indebted in gratitude to all who in diverse ways contributed to the success of this programme but their names are not mentioned owing to two cardinal reasons, some people preferred anonymity while others are excused for want of space.

Eteya, OGANA
A.B.U Zaria
January, 2017.

ABSTRACT

This research provides a conceptual discourse into the challenges of cybercrimes and the modes of curbing it. The modern society today faces with the greatest achievements of technical and technological development, associated by rapid expansion of information technology and automation of work activities in all social life spheres. Such development in modern society has brought a large number of facilities on one side while, on the other side the presence of deliberate misuse of this technological achievement has also created a number of problems and risks towards individuals and groups in the society in general and national safety in particular, the approach how criminals (offenders) commit crimes has changed. Digital general approach has opened new opportunities for unscrupulous behavior. Millions of Nairas/Euros have been lost by businesses and customers from the use of computers as part of the commission of the crime. In absence of technology and trained personnel to deal with this new threat known as cybercrime, the security agencies are challenged by specialized cyber offenders which are known as hackers because apart from managing to break into state institution websites they are able to have unauthorized access to information classified as state secret and top-secret. The research will be focusing majorly on the Nigeria perspective, the research will also focus on the variety of approaches from other jurisdictions, as well as the related problem of cybercrime from the perspective of governments, the private sector, academia and international organizations and how to combat cyber related crimes. Due to the global nature of computer crime, the general action in preventing and combating this type of crime, consists on building bridges of cooperation and coordinated action of all countries, and in this case of Nigeria in order to set international standards in the field of defense and security of information systems which standard would guarantee the success of a sustainable national perspective in combating threats from cybercrimes. In this thesis, among others we will present the global aspect of cybercrime, the legal infrastructure defining cybercrimes and their forms, in, the role of security institutions in combating crime in general with particular focus on tackling cyber challenges, current threats and future threats related to cybercrimes, the legal research methodology adopted in the collection of information is the doctrinal method. The findings of the research reveal essentially, that cybercrime legal responses are inadequate to fight cybercrime; those available could address cybercrime menace. It is therefore recommended that legislation needs to keep pace with e-crime, while some need reform to meet prevalent and sophisticated cyber challenges. Apart from awareness and culture, security measures (technical and non technical) will need to be put in place and enforced, as part of the solutions. This might involve raising penalties and increasing the seriousness of e-offences. The right culture should create a high level of awareness amongst stakeholders.

TABLE OF CONTENTS

Title Page- i

Declaration - ii

Certification- iii

Dedication- iv

Abstract - v

Acknowledgement- vi

Table of Contents vii

Table of Cases- ix

Table of Statutes- xvi

List of Abbreviation- xvii

CHAPTER ONE: GENERAL INTRODUCTION

1.1 Background to the Study -1

1.2 Problem of the Research -6

1.3 Aim and Objectives of the Study -8

1.4 Justification -10

1.5 Scope of the Study -10

1.6 Research Methodology -11

1.7 Literature Review - - - - - - - - -11
1.8 Organizational Layout - - - - - - - -18

CHAPTER TWO: THE CONCEPTUAL DISCOURSE/CLARIFICATION OF KEY TERMS

2.1 Introduction - - - - - - - - - -20
2.1.2 Meaning of Cybercrime - - - - - - - - -20
2.1.3 Types of Cybercrimes - - - - - - - - - -26
2.2 The Concept of Cybersecurity - - - - - - -38
2.2.1 Meaning of Cybersecurity - - - - - - - -39
2.2.2 Goals of Cyber Security - - - - - - - -41
2.2.3 Some Key Cyber Security Terminology - - - - - -41
2.2.4 Nigeria's Response to Terrorism - - - - - - -43
2.3 Concept of National Security - - - - - - - -45
2.3.1 Definition of NationalSecurity - - - - - - -45
2.3.2 National Security in Nigeria - - - - - - - -46

CHAPTER THREE: ANALYSIS OF LEGAL REGIME IN COMBATING CYBER CRIME

3.1 Introduction - - - - - -- - - - -51

3.2 Legal Framework Based on International Standards - - - - -51
3.2.1 United Nations and United Nations Office on Drugs and Crimes - - -51
3.2.2 International Telecommunication Union - - - - - -59
3.3 Legal Regime in Combating Cyber Crime at Regional Level - - -63
3.3.1 Council of Europe - - - - - - - - -64
3.3.2 Organisation for Economic Co-operation and Development - - - -71
3.3.3 Asia-Pacific Economic Cooperation - - - - - - -73
3.3.4 The Commonwealth - - - - - - - - -75
3.3.5 African Union- - - - - - - - - -76
3.3.6 Arab League and Gulf Cooperation Council - - - - - -79
3.3.7 Organization of American States - - - - - - -80
3.3.8 Caribbean - - - - - - - - - -82
3.3.9 Pacific - - - - - - - - - - -83
3.4 Legal Responses in Combating Cyber Crime at the National Level - - -84

CHAPTER FOUR: ISSUES AND CHALLENGES IN COMBATING CYBER CRIME

4.1 Introduction - - - - - - - - - -106
4.2 Law Enforcement in Combating Cyber Crime (Skills, Knowledge,Techniques

for Effective Investigation) - - - - - - - -106
4.3 The Role of Judiciary in the Admissibility of Electronic Evidence in Cyber Crime
Cases - - - - - - - - - - -118
4.4 Challenging Issues facing the Judiciary in Combating Cyber Crime - - -136
4.4.1 Legal Challenges in Tackling Cybercrime - - - - - -136
4.5 The Role of other Law Security and Intelligent Agencies in Curbing Cyber Crime -149

CHAPTER FIVE: SUMMARY RECOMMENDATIONAND CONCLUSION

5.1 Summary - - - - - - - - - -171
5.2 Findings - - - - - - - - -176
5.3 Recommendations - - - - - - - - -178
Bibliography - - - - - - - - - -181

TABLE OF CASES

Akingbola v FRN (2014) LPELR-24258 - - - - - 136

Amadi v FRN (2008) 18 NWLR(pt.119) 259- - - - - 156,157

Anyaebosi v. R. T. Briscoe Nig. Ltd (2000) 2 NWLR (pt 165) - - - 123

Aoko v Fagbemi(1961)ALL NLR 400 - - - - - 92

Asake v Nigerian Army Council (2007)ALL FWLR (pt.396) 737 - - 92

Attorney General of the Federation v Isong(1986)1 QLEN 75 - - 91

Austronic v Switzerland No:12726/87- - - - - - 148

Continental Sales Limited v. R. Shipping Inc (2013) 4 NWLR (pt 1343)- - 132

Kubor & Anor v. Dickson & Ors (2013) 4 NWLR (pt1345)- - - 133, 141

Esso WA Inc. v. Oyegbola (1969) NMLR 194- - - - - 123, 134, 153

Federal Republic of Nigeria v Ifegwu (2003) FWLR (pt.167) 703 - - 92

Federal Republic of Nigeria v Abdul (2007) EFCLR 204 at 228 - - 86

FRN v. Fani-Kayode (2010)14 NWLR (pt. 1214)481- - - - 122, 124

FRN v Amadi (2005) 2 QCCR 129.. - - - - - - 154, 156, 157

In Anvar v. P.K. V. Basheer, & Ors (2014) Supreme Court of India - - 134

In Navjot Sandhu V Afsan Guru (2005) Supreme Court of India- - - 134

Jagdeo Sigh v. The State & Ors (2015) Supreme Court of India- - - 135

King v. State ex. Rei Murdock Acceptance Corp- - - - - 127

Mehta v. J Pereira Femandes EWHC/Ch/2006/813- - - - - 130, 143

Oghoyone v. Oghoyone (2010)3 NWLR (pt. 1182)564 at 585.- - - 124

Okey Nwosu v FRN(2013) LPELR-22143.- - - - - - 136,

Olieh vsFederal Republic of Nigeria(2005) ALL FWLR (pt.281) 1746 - 91

P.A. Awolaha & Ors v. Seatrade Groningen B. V (2002) 4 NWLR (pt 758) 520- 132

State V. Mohd. Afzal & Ors (2003) Delhi High Court- - - - 134

Trade Bank Plc v. Chami (2003)13 NWLR (pt. 836) 158 at 213 -216- - 123, 126

U.S. v. Saccoccia, 18 F.3d 795 (9th Cir. 1994)- - - - - 138

UBA v. SAFPU & 3 ors (2004)3 NWLR (pt. 861) 516 at 541-543;- - 122
Udoro V. Governor, Akwa-Ibom State(2010)11 NWLR (pt. 1205)322- - 120

Yesufu v African Continental Bank Limited (2012) 1 BFLR 757.. - - 141
Yesufu vs. ACB (1976)4 SC1- - - - - - - 122

TABLE OF STATUTES

Advance Fee Fraud and Other Related Offences Act CAP A6 LFN 2006 - - - 86,154,157
Banks and Other Financial Institutions (BOFIA) Act CAP B3 LFN 2006 - - 87, 142
Constitution of Federal Republic of Nigeria 1999 (as amended)CAP. C23 L.F.N. 2004- 47,48,49,91,93,136,157
Criminal Code Act CAP. 77 L.F.N. 1990 Act CAP. C36 L.F.N. 2004 - 84
Cybercrimes (Prohibition, Prevention etc.) Act, 2015- - - 7,12,28,84,88,91,93,118,120,122,126,138,143

Evidence Act 2011- - - - - 120,122,133,140,141
Economic and Financial Crimes Commission (EFCC) Act CAP E1 2004 - - 84,153,157
Money Laundering (Prohibition) Act (MLA) 2011 (as amended)- - - 85
National Security Agency Act CAP 278 LFN 1990 - - -161
Nigeria Deposit Insurance Corporation (NDIC) Act CAP. L5 2006- - 87

National Information Technology Development Agency (NITDA) ACT 2007 - - 150
Nigerian Communications Act. *Cap.* N97 LFN 2004 - - - 151

LIST OF ABBREVIATION

ACPO	– Association of Chief Police Officers
APWG	– Anti Phishing Working Group
BKA	–Federal Criminal Police Office
BSI	– Federal Office for Information Security (DE)
CERT	– Computer Emergency Response Team
CII	– Critical Information Infrastructures
CIIP	– Critical Information Infrastructure Protection
CSIRT	– Computer Security Incident Response Team
CWG	– Conficker Working Group
DDoS	- Distributed Denial of Service
DHS	–Department of Homeland Security (US)
DIB pilot	– Defence Industrial Base (Information Exchange) pilot (US)
EC3	– European Cybercrime Centre
EG	–Expert Group
Europol	– European Police Office
f2f	– Face to face
FBI	– Federal Bureau of Investigation (US)
FIRST	– Forum of Incident Response and Security Teams
ICANN	– Internet Corporation for Assigned Names and Numbers
ICT	– Information Communications Technology
IETF	– Internet Engineering Task Force

Interpol	– International Police Office
IP	– Internet Protocol
ISP	– Internet Service Provider
ITU	– International Telecommunications Union
IT-ISAC	– Information Technology Information Sharing Analysis
Centre (US)	
JHA	– Justice and Home Affairs Council (EU)
LEA	– Law Enforcement Authority
MLAT	– Mutual Legal Assistance Treaty
MoU	– Memorandum of Understanding
MSSP	– Managed Security Service Provider
n/g CERT	– National/Governmental CERT
NHTCU	– National High Tech Crime Unit (NL)
NIS	– Network and Information Security
NWLR	- Nigerian Weekly Law Report
OCSIA	– Office for Cyber Security and Information Assurance (UK)
PCSIR T	– Product CSIRT
PPP	–Public Private Partnership
RAT	– Remote Access Tool
RfC	– Request for Comments
SC	- Supreme Court
SOCA	– Serious and Organised Crime Agency (UK)
SWITCH	– Swiss National Research Network
TF-CSIRT	– Task Force Computer Security Incident Response Team
(EU)	
TI	– Trusted Introducer program of the TF-CSIRT
TRANSITS	- Training programme for CERTs

CHAPTER ONE
GENERAL INTRODUCTION

1.1 Background to the Study

With the advent of the computer age, legislatures have been struggling to redefine the law to fit crimes perpetuated by computer criminals.[1] The crime is amongst the newest and most constantly evolving areas of the law in many jurisdictions. The rise of technology and online communication has not only produced a dramatic increase in the nature of criminal activities. Criminals are using cyberspace to commit numerous cyber crimes. Growing trends of complex distributed and Internet computing raise important questions about information security and privacy.[2]The Information Communication Technology (ICT) revolution has had impacts in almost every area of human endeavour, from business, industry, government to not-for-profit organization; ICT has simplified business process such as sorting, summarizing, coding, editing customized and generic report generation in a real-time proceeding mode. However, ICT has also brought unintended consequences such as criminal activities, spamming, credit card frauds, ATM frauds, phishing, identify theft and other related cyber crimes. Technology has integrated nations and the world has become a global village. The economy of most nations in the world is accessible through the aid of electronic via the internet. Since the electronic market is opened to everybody (which also includes eavesdroppers and criminals) the internet is a borderless regime[3]. The internet is one of the fastest-growing areas of technical infrastructure development.

[1] Ibikunle F., (2013) *Approach to Cyber Security Issues in Nigeria: Challenges and Solution,* Publication of Department of Electrical & Information Engineering, Covenant University Nigeria, Vol,1 No1 p1.
[2] Chen H., & Wang F.Y., (2005) "Guest Editors' Introduction: *Artificial Intelligence for Homeland Security*",IEEE intelligent systems, Vol. 20, No. 5, pp. 12–16.
[3] Okeshola F.B & Adeta A.K., (2013) The Nature, Cause and Consequences of Cybercrime in tertiary Institution in Zaria , Kaduna State, *American International Journal of Contemporary Research*, Vol3. No9, September P1.

Over the past decades, the growth of the internet and its use afforded everyone this opportunity[4]. However, information technology revolution associated with the internet has brought about two edge functions: that is on one hand, it has contributed positive values to the world. While on the other hand, it has produced so many maladies that threaten the order of the society and also producing a new wave of crime to the world. The internet online business services, which ordinarily suppose to be a blessing as it exposes one to a lot of opportunities in various field of life is fast becoming a source of discomfort and worry due to the atrocity being perpetrated through it. Based on the threatened menace the Nigeria government has come up with a legal framework of cybercrime which is discussed and x-rayed in this work on it effectiveness on combating cybercrimes.

Cyber infrastructures are highly vulnerable to intrusions and other threats. With the pace and amount of cyber attacks, human intervention is simply not sufficient for timely attack analysis and appropriate response. The fact is that the most network-centric cyber attacks are carried out by intelligent agents such as computer worms and viruses; hence, Combating them with intelligent semi-autonomous agents that can detect, evaluate, and respond to cyber attacks has become a requirement. These so called computer-generated forces will have to be able to manage the entire process of attack response in a timely manner, attack is occurring, what the targets are and what is the appropriate response, as well as how to prioritize and prevent secondary attacks[5]. Furthermore, cyber intrusions are not localized. They are a global menace that

[4] Ibikunle F., *Op Cit p.2*
[5] Selma Dilek, e,tal (2015) applications of artificial intelligence techniques to combating cyber crimes: a review, *International Journal of Artificial Intelligence & Applications* (IJAIA), Vol. 6, No. 1, January P.2

poses threat to any computer system in the world at a growing rate. There were times when only educated specialist could commit cyber crimes, but today with the expansion of the Internet, almost anyone has access to the knowledge and tools for committing these crimes. Conventional fixed algorithms (hard-wired logic on decision making level) have become ineffective against combating dynamically evolving cyber attacks. It has also resulted in the emergence of what appears to be some new varieties of criminal activities pose challenges for legal systems, as well as for law enforcement[6].

Cybercrimes are factor that has been a great threat to Information Communication and Technology, the operation of cyberspace transaction; other cyberspace related functions are the most wonderful means of communications and transactions in the field of internet. The Department of Justice ('Dos') defines computer crimes as any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation or prosecutions[7]. Cybercrime has been eluding factor in the cyberspace transactions in Nigeria, where cybercrimes and computer related crimes are endemic. The integration of computer technology as a global issue, with the opportunity opened to the general public in use for viable objectives, certain high-level of crimes are committed and some of the perpetrators of these menace crimes are referred to as "hackers" syndrome, they took advantage of cyberspace transactions available on the internet to defraud the unsuspected victims who are mostly foreign transactions in thousand and

[6] Laura A.(2015) Cybercrime and National Security; *the role of the penal and procedural Law,* Research Fellow, Nigerian Institute of Advance Legal Studies p.7. Accessed from http://nials-nigeria.org/pub/lauraani.pdf. On 4/8/15 at 9:45am.
[7] The Economic Times: September 11, (2004) p1.

millions of dollars[8]. These criminally minded individuals will have a discussion with the victims through the internet and they will pretend to be interesting and loving, before the victim realized, the criminals would have succeeded in luring them into sending some dollars to enable them facilitate traveling documents they falsify documents and tell all sort of lies to get money or that they are beneficiary to a thousand of dollars in a trust account but they need a little money to secure the services of a counsel to claim the trust fund[9].

Nigeria battles against cybercrime effort have been put in place by directing the sources and channel through which cybercrimes are perpetrated in Nigeria generally are targeted at individuals and not directly to computer systems, hence they require less technical expertise on the part of the criminals[10]. Recently, a report indicated that Nigeria is losing about 89 million dollars yearly to software piracy the report was the finding of a study conducted by institute of Digital Communication is a market research based in South Africa. Also the America national fraud information centre reported Nigeria money offers as the fastest online scam up to 90% in 2001. The centre also ranked Nigeria cybercrime, impact per capita as being exceptionally high[11].

In an attempt to fight the menace of cybercrime in Nigeria, Physical devices such as sensors and detectors are not sufficient for monitoring and protection of these infrastructures; hence, there is a need for more sophisticated IT that can model normal behaviors and detect abnormal ones. These cyber defense

[8] Ehimen O.R & Bola A., (2010) " Cybercrimes in Nigeria*" Business Intelligence Journal*, January, Vol.3, No.1 p.95
[9] Mu'azu A.S & Abubakar M.K., (2014) Cybercrime in Nigeria:*An Overview of Cybercrime Act 2013, Journal of Law, Policy and Globalization*, ISSN 2224-3240 (Paper) ISSN 2224 – 3259 (Online) Vol.32, p.23
[10] Ibid p 23.
[11] Ibid p 24.

systems need to be flexible, adaptable and robust, and able to detect a wide variety of threats and make intelligent real-time decisions[12]. There is need for Cyber law and Cyber security. Cyber laws prevent or reduce large scale damage from cybercriminal activities by protecting information access, privacy, communications, intellectual property and freedom of speech related to the use of the internet, websites, emails computers, cell phones, software and hardware, such as data storage devices[13]. The increase in internet traffic has led to a higher proportion of legal issues worldwide. Because cyber laws vary by jurisdiction and country, enforcement is challenging and restitution ranges from fines to imprisonment.

The term "Cyber law" has been defined by, the Black's law dictionary, as the field of law dealing with the internet, encompassing cases, Statutes, Regulations and disputes that affect people and businesses interacting through computers cyber law is at the heart of many legal and policy issues today, including jurisdictional questions, intellectual property rights, tort actions, privacy rights, e-commerce, cybercrimes, online speech. Since the internet is fluid and dynamic medium, cyberlaw is a field of law that changes rapidly and it is important to stay current with recent trends. In a related development, cyberlaw has been defined as the law governing cyber space[14].

For Nigeria, a nation in the process of saving her face regarding cybercrimes, efforts are now being directed at the sources and channels through which cybercrimes are perpetuated. The task of re-stigmatizing cybercrime and re-

[12] Dasgupta D., (2006) "Computational Intelligence in Cyber Security", *IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety* (CIHSPS 2006), pp. 2–3

[13] Ladan M.T, (2015) *Cyberlaw and Policy on Information and Communications Technology in Nigeria* Ahmadu Bello University Press Limited p 104.

[14] Garner A. B., (2009) *Black's Law Dictionary*, Thomson West, United State of American, 8th ed p 414.

dignifying honest is not as easy as that of institutionalizing a deterrence mechanism and the legal framework in combating cyber crime like Cybercrimes Act, Code of Conduct Bureau, Independent Corrupt Practices Commission (ICPC), Economic and Financial Crime Commission (EFCC) and many more[15].

1.2 Problem of the Research

The contribution of internet to the development of nation has been marred by the evolution of new waves of crime. The internet has also become an environment where the most lucrative and safest crime thrives. Cyber has become a global threat from Europe to America, African to Asia. The rate of Electronic-crime in Nigeria has outgrown the rate of internet usage in the country because it is an easy way of communication. In this research work, we proffer an answer as to why there is such an upsurge of electronic crimes in Nigeria, what are the factors that made Nigerians so vulnerable to Electronic-crime[16].

First, the cyberspace is borderless which poses fundamental problem for courts whose jurisdiction is based on geography, the problems of cyber system in Nigeria is not unconnected with the porous nature of the internet, the internet is free for all with no central control, hence, the state of anarchy presently experienced. Proliferation of an unauthorized cybercafé is another problem in the cyber regime, and many entrepreneurs have taken to

[15] Ladan M.T., *op cit* p.105

[16] Olayemi O.J.,(2014)A Socio – Technological Analysis of Cybercrime and Cyber security in Nigeria, *International Journal of Sociology and Anthropology* Vol 6 (3) March, p.117 Http://www.academic journals.org/ijsa accessed on 03/08/15 at 04:34 pm.

establishment of cybercafés that serve as blissful havens for the syndicates to practice their act.

Secondly, lack of national functional data base, lack of infrastructure, lack of standards and national central control, corruption, poverty rate, and unemployment is an impediment to the curbing of cybercrimes in Nigeria.[17] It is very difficult to fix the identity to the perpetrator in Cyber-space as it is very easy to mask a fake identity. You can have a mask of famous hero, heroin, politician or even policeman with photo-identify in the Cyber-space. It is difficult to see the person actually sitting in front of terminals and only the manifested identity is only source in Cyberspace.[18]

Thirdly, this relates to the constitutionality of the requirement for personal information under the Know Your Customer (KYC) and Bank Verification Number BVN initiatives. This requirement might be considered intrusive and a breach of the constitutionally guaranteed right to privacy, as the provision of S. 38 Cybercrime Act conflicts with the constitution, it triggers the inherent risk of leaving bank customers vulnerable to cybercrime attacks, particularly given the multiplicity of biometric data requests by various regulators in Nigeria.[19]

Lastly, Cybercrime cut across territorial borders, creating a new realm of illegal human activity and undermining the feasibility--and legitimacy--of applying laws based on geographic boundaries. Territorially-based law-making and law-enforcing authorities find cybercrime deeply threatening. It

[17] Ibikunle F, Op Cit p3. www.ijcrees.com/index.php/ijcrsee/article/view/11/114 accessed on 03/08/15 at 8:00am
[18] Jain Atul (1999): *Cyber Crime - Issues Threats and Management* Vol. 1, Isha Books Delhi, pg. 4

[19] Olanipekun O., (2015) *Cybercrimes in the Banking Sector*: Facing the new wave of criminals legally p 16

has subjected the nation-State to unprecedented challenges with regard to its efficacy, compliance and enforcement. However, established territorial authorities may yet learn to defer to the self-regulatory efforts of Cyberspace participants who care most deeply about this new digital trade in ideas, information, and services. Separated from doctrine tied to territorial jurisdictions, new legislations will emerge, in a variety of online spaces, to deal with a wide range of new phenomena that have no clear parallel in the real world.

The above issues clearly represent the special legal problems which confront cybercrimes regime. The following questions form the basis for the research work thus:

Whether a comparative and critical analysis of the existing laws or the regulatory/institutional framework and their control measures in place, adequately combat cybercrime in Nigeria is there established institutional framework for coordination and the implementation of cyber law? Whether these legal frameworks that regulate cyber crimes, law enforcement agencies and the judiciary are up to the task? Accordingly, this work seeks to address and analyse the following issues:

a) Firstly, is to examine how cybercrime is being addressed at the International, Regional and National levels.
b) Secondly, it reviews the state of the existing legislative and regulatory framework and their efficiency in combating this form of cross-border organised crime, taking the Nigeria as a case study.
c) Finally, the research work will conclude by discussing the steps nations should take in their battle against the cybercrimes.

1.3 Aim and Objectives

The cardinal objective of the research work is to

(a) Find answers, or solutions to the problems as highlighted under paragraph 1.2 above, this will be done by assessing and analyzing the regulatory frameworks role in combating cyber crime computer related acts including physical damage to computer systems stored data, unauthorized use of computer system and the manipulation of electronic data computed related fraud, and software piracy which have been recognized as criminal offences. This study sought to assess cyber crime and its impact in Nigeria. It also examined the existing policy framework and assessed the success of the institutional counter measures in combating cybercrime in Nigeria[20].

(b) To examine and appraise selected court decisions with a view to understanding better, the critical role of the judiciary (Courts), and analyze the efficiency of the law enforcement agencies and other administrative machinery in dealing with, and prevention of cybercrime offences and proffer necessary recommendation for the proper enforcement and implementation of the penalties on the cybercrime offenders.

(c) The research attempts to provide an overview of cybercrime, cyber security, and Concept of National Security. It define the concept of cybercrimes, identify reasons for cybercrime and it eradication. It looks at those involved and the reasons for their involvement methods of stepping up cyber security in Nigeria. In the light of the above, the

[20] Wada F. & Oduloja G.O., (2012) E-banking and Cybercrime in Nigeria: *A Theoretical Policy Perspective on Causation*, Afr J. of Comp & ICTs, Vol5, No1 P 69.

research would conduct an x-ray of the Cyber Crime Act 2015 enacted by the 7th National Assembly, which provided a legal framework for the prohibition, prosecution, prevention and punishment of electronic fraud and cybercrimes, with a view to preparing the minds of stakeholders in the ICT regime and general public on the content of the Act[21].

(d) Finally to make a survey into other possible ways which may most likely present appreciable mode of curbing computer related offences in Nigeria by concluding with some findings and recommendations.

1.4 Justification

This research work will be of immense important to all stakeholders involved, particularly in Nigeria. The knowledge provided in this study will demonstrate the impact to current realities, global competitiveness and relevance to the Nigerian economy and sustainable development. It shall also produce legal expert/researchers, academicians, students of law and users of information, with the necessary competencies and skills to function effectively in institutions of higher learning and in both the public private sectors of the Nigerian economy. It would also broaden the knowledge of the legislature to provide possible amendments of the existing law on the subject.

Finally, this research work would add to the prevailing knowledge and serve as useful and reference materials for further study in the area of Information Communication Technology. (Cyber Crime Act).

[21] Cyber Crime Act, 2015

1.5 Scope of the Research

The research focuses majorly on the national approach of the legal framework in addressing cybercrimes in Nigeria, the research has also looked on the variety of approaches from other jurisdictions, as well as the related problems, demonstrates that there are considerable difficulties in defining the terms "computer crime" and "cybercrime"[22].

The term "cybercrime" is used to describe a range of offence including traditional computer crimes, as well as network crimes. As these crimes differ in many ways there is no single criterion that could include all acts mentioned in the different regional and international legal approaches to address the issue whilst excluding traditional crimes that are just facilitated by using hardware[23].

The study analyses the problem of cybercrime from the perspective of governments, the private sector, academia and international organizations and how to combat cyber related offences. References will however be made to the global cybercrime picture, cybercrime legislation and frameworks.

1.6 Research Methodology

This research utilizes the use of doctrinal method on the basis of existing literature and articles on the field of research. This research examined the Nigerian Laws, statutes as well as cases and judicial precedent on the subject matter vis-à-vis international treaties to which Nigeria is a signatory were also relied on.

---

[22] Laura A. Op Cit p.4

[23] For difficulty related to the application of a Cyber crime definition to real-world crimes, see: Brenner, (2004) Cybercrime Metrics: *Old Wine Bottles? Virginia Journal of Law and Technology* Vol.9, available at www.vjolt.net/Vol9/issue4/v9i4 - a13 -Brenner.pdf.

1.7 Literature Review

This area of research work is new and a developing sphere for academic exploitation, though there are few scholars and researchers who delved into various aspects of computer related offences (cyber crimes) the research shall assess legislation, cases, books etc. in self-assessment in other to facilitate further research in the subject.

In Nigeria today, numerous internet assisted crimes are committed daily in various forms such as identify theft, desktop counterfeiting, internet chat room, cyber harassment fraudulent electronic mails, Automated Teller Machine spoofing, pornography, piracy, hacking, phishing and spamming. Usually these crimes are committed in forms like sending of fraudulent and bogus financial proposals from cyber criminal to innocent internet users. Due to the prevalent rates of cyber crime, which have become strong threats to Nigeria[24]. The National Assembly of the Federal Republic of Nigeria enacted an Act known as Cyber Crimes (Prohibition, Prevention etc) Act, 2015. The Act provides for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria.

This Act also ensures the protection of critical national information infrastructure and promotes cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights[25] Some of the cases of cybercrimes and computer related offence tried and those pending by the Anti-grafting agencies such as the Economic and Financial Crime Commission

[24] Ladan M.T., *Op Cit p.34*
[25] Cybercrime (Prohibition, Prevention, etc) Act, 2015, Explanatory Memorandum.

(EFCC), Independent Corrupt Practices Commission (ICPC) shall be assessed in this research study. However, it is the considered view of the researcher that the Act did cover the field there lacuna in the area of prescription of punishment under S.7 of the Cybercrime Act as well as the issue of electronically generated evidence was not contemplated in the Act, which shall be discussed comprehensively in our next chapter

According to Vladimir[26], internet is a global network which unites millions of computer located in different countries and open broad opportunities to obtain and exchange information, but it is now been used for criminal purposes due to the economic factors. Nigeria a third world country is faced with so many economic challenges such as poverty, corruption, unemployment amongst others, thereby making this crime thrive.[27]

Ladan M.T.[28] an erudite scholar postulated that with the growing sophistication and use of information, the past decade has seen a major growth in cybercrime. The fight against cybercrime require a cohesive and coordinated approach, but in African bad governance, high rate of educated youth unemployment, weak or non-existent legal and regulatory frameworks on cybercrime and cyber security, poverty underdevelopment are the major causes for growth of cybercrime in the region. The potential for internet abuse in Africa is also high, this is due to the lack of security awareness programmes or specialized training for the law enforcement agencies[29]. In the considered view of the writer however, it will be inconclusive to base it only on economic

[26] Vladimir, G. . (2005) *International Cooperation in Fighting Cyber crime*. p5. www.crimeresearch.org
[27] Folashade B.O. etal, (2013) The Nature, Causes and Consequence of Cyber Crime in Tertiary institution in Zaria-Kaduna state, *American International Journal of Contemporary Research*, Vol. 3, No. 9, September, p.98
[28] Ladan M.T., *op cit p.1*
[29] *Ibid* p.1

challenges as the cause of cyber-crime in Nigeria there are other causes too such as political factors.

According to Sieber, the Internet is not only used for direct attacks, but also as a forum for soliciting, offers and incitement to commit crimes unlawful sale of products and providing information and instructions for illegal acts (e.g. how to build explosives). Many countries have put in place regulations on the trade of certain products. Different countries apply different national regulations and trade restrictions to various products such as military equipment. A similar situation exists for medicines – medicines which are available without restriction in some countries may need prescription in others. Cross-border trade may make it difficult to ensure that access to certain products is restricted within a territory. Given the popularity of the Internet, this problem has grown. Webshops operating in countries with no restrictions can sell products to customers in other countries with restrictions, undermining these limitations. Prior to the Internet, it was difficult for most people to access instructions on how to build weapons. The necessary information was available (e.g. in books dealing with chemical aspects of explosives), but time consuming to find. Today, information on how to build explosives is available over the Internet and ease of access to information increases the likelihood of attacks.[30]

Agba.,[31] is of the view that internet is the most technologically advanced medium of interaction, it is the information revolution that has turned the

[30] Sieber, (2004) Council of Europe Organised Crime Report , page 140.

[31] Agba P.C., (2003) International Communication Principles, Concepts and Issues: In Okunna C.S. (ed) *Techniques of Mass Communication: A multi – Dimensional Approach*. Enugu: New Generation Books p.9

world into a global village[32]. Igwe posited that the internet is multi-jurisdictional because of it borderless nature, which makes it easily accessible from any place. The packet-switching technology and complex weave of digital networks and telecommunication infrastructure, digitized information may travel though various countries and jurisdictions, each with its own destinations.[33]the following arise in the context of private international law; namely jurisdiction to adjudicate dispute, also referred to as choice of law or conflict of laws, and the recognition and enforcement of judgments in courts in foreign jurisdictions. There are situations where one or more parties are involved in commercial activities, internet users, service and content providers, buyers, sellers, businesses technology systems and computer servers are located in different countries. In the process, the uncertainties may arise as to where the activities are taken place. The effect of such activities could be felt all over the world. This result to the question of jurisdiction such as country who has the jurisdiction to entertain and or address the issue, enforcement and probably resolution through amicable means. Every country determines its own rules of private international law, some regions are harmonized by treaty. Jurisdiction has been posing lots of setback in an attempt to curb the scourge of cybercrimes in our courts system especially when the parties are located in different countries and the offence is felt in another country and Nigeria is not an exception.[34] Shinder.,[35] viewed cybercrime as any criminal offences committed using the internet or another computer network as a component of the crime. Cybercrimes are offences that

[32] Folashade B.O.Op Cit p.99

[33] Rodney, D.R., (2002) Intellectual Property are the internet, Butterworths, New Delhi. P. 111

[34] Igwe, E.K., (2016) An Exposition on the Jurisdictional Issues in Cybercrimes in Nigeria, *Benue State University Law Journal*, Vol. 7 NO. 1 P.281-282

[35] Shinder, D.L.,(2002) *Scene of the Cyber Crime; Computer Forensics handbook*, Syngress Publishing Inc. 88 Hingham street, USA. p.1

area committed against individual or group of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly using modern telecommunication networks such as internet and mobile phones.

Akomolede T.I., et al., postulated thus, that the growing functionality and ease of computerized network, perhaps the most important characteristic of the impact of internet to terrorist is the ubiquity of the internet. This means that internet connectivity is everywhere and accessible by or to almost everyone. As the internet serves, private business, governmental and international needs, it also serves criminals. It essentially allows terrorist organizations to operate on a global basis without the added requirement for physical infrastructures and personnel. This is actually the biggest advantage terrorist organizations currently have since it allows them to communicate their massages to decentralized cells around the world in efforts to ensure terrorist operations are conducted in support of the greater intent. It also allows them to establish successful information operation campaign against countries on attack and its allies through the publishing of tightly controlled information on various web pages.

It appears most terrorist organizations are not interested in cyber terrorism. This is because known terrorist organizations like Al-Qeada are reported to prefer leveraging cyber technologies such as the internet to enable terrorist operation in the physical domain. They also opined that there are eight ways to which terrorist use internet viz, psychological warfare, publicity and

propaganda, data mining, fundraising, recruitment and mobilization, networking, information sharing and planning and coordination.[36]

Chiesa.,[37] he opined that another cause of cyber crime in Nigeria is the quest for wealth, there exist a large gap between the rich and the average, as such many strive to level up using the quickest means possible, since for any business to thrive well, the rate of return in the investment must be growing at a geometric rate with a minimal risk.

Anahet'al.,[38] weak/fragile laws regulating cybercriminals exist in Nigeria unlike in the real world where criminals, such as armed robbers are treated with maximum penalties. Unfortunately, the nation is not well equipped with sophisticated hardware to track down the virtual forensic criminals. Meke.,[39] in his article, he opined that urbanization is one of the major causes of cybercrimes in Nigeria and urbanization will be beneficial if and only if good jobs can be created in the cities where population growth is increasing, he emphasised that urbanization without crime is really impossible.

According to Sutherland,[40] criminal behaviour is learned. Criminal behaviour is learned in interaction with other persons in a process of communication. This would mean an individual is influenced to participate in criminal behaviour through watching and interacting with other individuals who are engaging in the criminal behaviour. The principal part of the learning of

[36] Akomolede T.I., Et al., (2016) *Cybercrime and Cybersecurity as challenges to the fight against Global Terrorism:* Paper Presented at the 47th Conference of the Nigerian Association of Law Teachers 22nd -27th May, Nasarawa State University, Keffi, Nigeria.
[37] Chiesa, R.,(2011)*'Auditing the Hacker's Mind: The Hacker's Profiling Project*. A Presentation by Chiesa Raoul at WINS International Best Practice Conference, Vienna, Austria.
[38] Anah,B.H., Funmi, D.L., & Julius, M., (2012) Cyber Crime in Nigeria: Causes, effects and the way out. *ARPN Journal of Science and Technology,* 2 (8) 626, http:/www.ejournalofscience.org
[39] Meke E.S.N. (2012), Urbanization and cybercrime in Nigeria : Causes and Consequences: *ARPN Journal of Science and Technology,* 2 (8) 631, http:/www.ejournalofscience.org.
[40] Sutherland, E.(1939), Principles of Criminology. Fourth edition.

criminal behaviour occurs within intimate personal groups. When criminal behaviour is learned, the learning includes techniques of committing the crime, which are sometimes very complicated, sometimes simple and they learn the specific direction of motives, drives, rationalizations and attitudes for committing a crime. This means that an individual will be influenced into believing that the behaviour which they may have previously believed was wrong, into believing that it is right through rationalization of their action.[41]

Furthermore, an individual will be pushed into deviant behaviour depending on their view of the legal code as being favourable or unfavourable. A person becomes delinquent because of an excess of definitions favourable to violation of law over definitions unfavourable to violation of the law. Therefore, an individual will break a law if they see more reasons to break it than to stay in compliance with it. Differential Associations may also vary in frequency, duration, priority and intensity.[42] The process of learning criminal behaviour by association with criminal and anti-criminal patterns involves all of the mechanisms that are involved in any other learning. This means that individuals learn criminal actions and legal through the same way. This theory states that while criminal behaviour is an expression of general needs and values, it is not necessarily the fulfilment of these needs and values which causes deviant behaviour since non-criminal behaviour is an expression of these same needs and values.[43]

From the foregoing, the authors and researchers on this topic made effort to define the concept cybercrime and also state the cause of cybercrime by

[41] *Ibid*
[42] *Ibid*
[43] *ibid*

relying on economic perspective but living the socio-political effect of computer related offence, the recent trend of the legal, regulatory and institutional framework on cybercrime was not addressed by the scholars, based on the gap created this work shall fill in the gap by addressing the above mentioned issues. The internet creates unlimited opportunities for commercial social and educational activities. However, it has introduced its own peculiar risk that poses danger to the economy. The danger could affect many sectors of the society and put the development of the country into peril. Some of these possible adverse effects could include the destruction of the country's image both at home and abroad, insecurity of both life and properties, fear of doing business with Nigerian citizens, economic loss of spending substantial amount of money on the prevention and control of cyber crime amongst others.

1.8 Organizational Layout

This work is structured into five chapters. Chapter one contains issue such as the general introduction, the background to the study, aims and objective of the study, research methodology, the scope of the research, literature review, justification as well as the organizational layout of the research. The chapter two which is the literature review and theoretical framework would deal with the conceptual exploration of the topic. Chapter three, deals on analysis of legal regime in combating cyber crime.

The fourth chapter analysis issues and challenges in combating cyber crimes, by identifying the problems associated with cyber crimes in Nigeria. The last chapter contains summary, observation, conclusion and recommendation to the research.

CHAPTER TWO
THE CONCEPT OF CYBERCRIME

2.1 INTRODUCTION

Today's world is a world of information explosion. This information explosion is taking place in such a fast speed that even a literate person is feeling as if he or she is illiterate being not able to cope up with such an information explosion. Here the question arises how is one to cope up with it? The answer is, Information Technology (IT) that can help in coping with the information explosion, by the use of internet to source for information[44]. The concept of cybercrime is historical with the advent of information and communication technology, massive digitalization and unprecedented interconnectivity provided by the internet has been a boon to students, doctors, teachers, lawyers, businessmen and criminals. Historical antecedent shows that unauthorized access, damage to property, theft and distribution of obscene and indecent materials are all considered as familiar cybercrimes[45]. This chapter shall be focusing on the clarification of the concept of cybercrime, concept of cyber security and concept of National security.

2.1.2 Meaning of Cybercrime

Technical experts, police, lawyers, criminologists, and national security experts understand the concept of 'cyber crime' differently, in order to understand the Cyber crime at conceptual level, it is essential to scrutinize the definitional aspects of the word 'Cybercrime'. In this portion, some of the

[44] Ladan M.T op cit p12.
[45] The communicator Magazine, A summary of the legislation on cybercrime in Nigeria, by legislative & Government Relation Unit, Public Affairs Department, the communicator Magazine (2015) Nigerian Communications Commission (2015) p.1 www.ncc.gov.ng/thecommunicator/index//php/option=com-content&iew=article&id=899:9-summary-of-thelegislation-on-cybercrime-in-nigeria&catid-132:features&itemid=68 Retrieved on 22/09/2015, by 21:59 am.

definitions are verified. Cybercrime must be a terminology that crept into the lexicon of our criminal jurisprudence at the advent of the internet as observed earlier.[46] However, cybercrimes could mean the terms "Computer Crimes" and "Cybercrime"[47]. Computer crime or cybercrime is any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target net crime of criminal exploitation of the internet, inherently a cybercrime. Cybercrime uses the unique features of the net–sending of e-mails in seconds, speedy publications/disseminations of information through the web to anyone on the planet. Computer attacks can be generated by the criminals from anywhere in the world, and executed in other areas, irrespective of geopolitical location. Often, these criminal activities can be faster, easier and more damaging with the use of internet[48].

The 10th United Nation Conference on the punishment of offences, cybercrime was broken into two categories and thus defined as;

1. in a narrow sense, as any illegal behaviour directed by means of electronic operations that target the security of computer system and data processing by them and
2. In a broader sense, as any illegal behaviour committed by means of or in relation to a computer system or network including such crimes as illegal possession and offering or distributing information by means of a computer system or networks[49].

[46] For history of computer crime, see M Wasik, *Crime and the Computer* Oxford University Press (1991).
[47] Ladan M.T op cit p.30
[48] The communicator Magazine op cit p.2 available at: www.ncc.gov.ng/thecommunicator.
[49] Crimes related to computer networks, background paper for the workshop on crimes related to computer networks, *10th UN Conference on the prevention of crimes and to treatment of offenders*, 2000, A/CONF/87/10, page5:available at:www.uncjin.org/documents/confr10/10e.pdf.

Cybercrime, is a broad notion, in literature all kind of definition can be found of computer crime, computer-related crime, internet, etc., including discussions what about which specific crimes should be considered as such, modern definitions of cybercrime describe cybercrime as concerning any crime for the commission of which the use of the internet was essential. This implies that even offences that do not include an explicit reference to information communications technology (ICT) or to the electronic environment, can nevertheless be considered as such if the criminal conduct was directed against other computers or where the facilities of the internet were used to disseminate or retrieved information "essential" means that ICT or the electronic environment is an essential element of the criminal conduct A murder in the computer room would not qualify as such.[50]

Under the notion of cybercrime, all kind of subcategories can be distinguished, including their refinement and details. The cybercrime Convention 2001, that adopted the notion of cybercrime, does not provide a definition but distinguished in its substantive law part four categories of the cybercrime;

1) CIA offences: dealing with conduct that is directed against computer systems (and networks) and the data processed, stored or transferred by it;
2) Computer-related offences, property crime committed by means of computer system.

[50] Kaspersen Henrik W.K., *Cybercrime and internet jurisdiction Vrrje Universiteit Amsterdam*, Economic crime Division, Directorate General of Human Rights and Legal Affairs, Strasbourg, France Version 5 March (2009) p.12 available at: www.coe.int/cybercrime.

3) Content-related offences, concerning the disclosure or making available by means of a computer system of illegal content; and as a separate category.

4) Offences related to intellectual property.[51]

According to *Osborn*, cybercrime are crimes committed on the internet using computer as either a tool or a targeted victim,[52] cybercrimes involves both the computer and the person behind it as victim, depending on which of the two is the target. Hence, the computer could be looked at as either a target or a tool.[53] *Folashade,* defined cybercrime as follows; "cybercrime is derived from two words "Cyber" and "Crime" cyber refer to any activities either sales or transaction of services in the cyber space while crime are unacceptable activities, when join together, it means all fraudulent, illicit and unacceptable activities related to cyber"[54]

The OECD Recommendation of 1986[55] gave a working definition of cybercrime as: "computer related crime is considered as any illegal, unethical or unauthorized behaviour relating to the automatic processing and transmission of data."

The Commission of the European Union in 2001, define cyber crime or computer related crime as any crime that in some way or the other involves

[51] Ibid.
[52] The Indian Law Institute; Introduction to the cyber world and Cyber law (2010) p.10
[53] Osborn H.Q., e tal, .(2012) Fighting Cybercrime in Africa; *Computer science and Engineering*, 2(6) 118-100 Doi 1-.5923/j computer20/20206.03. p.2Published online at:http://Journalsapub.org/computer.scientific&Academic publishing 2012.
[54] Folashade B.O., *op cit* p.103
[55] Computer Related Criminality:Analysis of Legal politics in the OECD Area (1986)

the use of information technology.[56] Cybercrime must be a terminology that crept into the lexicon of our criminal jurisprudence at the advent of the internet as observed earlier most products and services are now being offered and delivered across these platforms, the reinvention has created a new form of contactless transactions. Ironically, it has also witnessed the emergence of the invisible criminal as the internet has also provided a platform for criminals to ply their trade.

According to the website of Crime Investigation Department, Andhra Pradesh State Police, who said "Cyber crime means unlawful acts wherein the computer is either a tool or a target or both."[57] According to the definition, the Cyber crime consist crimes

a. Where the computer is a tool for an unlawful act - and;

b. Where the computer is the target for an unlawful act.

c. Where computer is both tool and target for/of unlawful act.

However, the present definition considers Cyber-crime and computer crime as one of the same thing, which though having some common premises, differ on several account. Again, this definition have rider like 'unethical' which, too great extent, fall outside the purview of law. Ethics is not basis for imposing legal liability.

According to Pavan Duggal, an advocate of Supreme Court and Cyber law expert, he defined cybercrime as, “Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes

[56] The European Parliament, the Economic and Social Committee and the Committee of Regions, 26th January, 2001. *http://www.europe.en.int.retrieved* on the13/09/2015 by 2:00pm

[57] *http://www.cidap.gov.in/mainwccrime.aspx* See also, same definition appeared on the web site of Cyber Crime Police Station, Banglore, Karnataka, *http://www.Cyberpolicebangalore.nic.in/Cybercrimes.htm*

comes within the ambit of Cyber crime."[58] The term 'cybercrime' also poses a significant challenge in definition. Literally, it means crime committed in cyberspace or with the use of the internet. This definition raises questions whether a criminal activity conducted via non-internet-based computer or other electronic devices constitutes cybercrime. Hence, others have opted for alternative terms such as 'e-crime,' 'computer crime,' 'hi-tech crime' or 'digital crime.' While each of these alternative terminologies might not necessarily involve the use of the internet, it is clear that they refer to criminal activities on a far broader spectrum. Thus, the term, cybercrime, literally speaking, should be referring to a narrower set of criminal activities.[59] It is arguable whether the consideration of the use of the internet in the commission of crime should remain a function of the definition of cybercrime. Given the extant state of technology advancement, there is hardly any electronic or digital device that is not now connected to the internet, whether remotely or directly. The duration of the connection, or whether the internet connectivity function of the device was enabled at the time the crime was committed, is a question of fact. For the present purposes, it is pertinent to adopt a working definition of cybercrime. Hence, cybercrime is defined as a financial crime involving the use of internet-enabled electronic or other devices and platforms. Therefore, for the present purposes, the scope of cybercrime is narrowed down to a subset of financial crime. The cybercrime could also refer to all type of crimes that exploit telecommunications network in computers or computer network are used for criminal activities. E,g

[58] http://www.rediff.com/netguide/index.html accessed on 01.12.2015.
[59] See A Gillespie, (2007) *Cybercrime: Key Issues and Debates* (Routledge 2016) Chapter 1; I Walden, *Computer Crimes and Digital Investigations* (Oxford University Press).

designing a fake receipt on a computer system to extort funds from the government desk.

It has been aptly observed that computers play any or all of four roles in crime. They serve as objects, subjects, tools and symbols.[60] These roles of computers have been analysed further:

> Computers are the objects of crime when they are sabotaged or stolen … computers play the role of subjects when they are the environment in which technologies commit crimes. Computer virus attacks fall into this category. When automated crimes take place, computers will be the subject of attacks. The third role of computers in crime is as tools, enabling criminals to produce false information or plan and control crimes. Finally, computers are also used as symbols to deceive victims …
>
> When speaking about cybercrime, we usually speak about two major categories of offence: in the first, a computer connected to a network is a target of the offence; this is the case of attacks on network confidentiality, integrity and/or availability. The other category consists of traditional offences such as theft, fraud, and forgery which are committed with the assistance of/or by means of computers connected to a network, computer networks and related information and communications technology.[61]

From this exposition, the working definition of cybercrime can further be expounded as financial crime where internet-based computer or other devices and platforms serve as objects, subjects, tools and/or symbols. The peculiar challenge posed by cybercrime must form the backdrop of any analysis of this scourge. While the advancement in technology has aided legitimate activities and transactions, criminals have also taken it as a free ride to carry out criminal activities ubiquitously and anonymously.

[60] D Parker, *Fighting Computer Crime: For Protecting Information* (Wiley 1998).
[61] Olanipekun O. (2015) Cybercrimes in the Banking Sector: Facing the new wave of criminals legally, p 10.

The attempt to define cybercrime here is merely notional. For the sake of emphasis, it is reiterated that crime is what the law says it is. Thus, cybercrimes that are expressly established by statute will be considered subsequently.

2.1.3 TYPES OF CYBERCRIMES

The term "cybercrime" is used to cover a wide variety of criminal conduct.[62] As recognized crimes include a broad range of different offences, it is difficult to develop a typology or classification system for cybercrime.[63] One approach can be found in the Convention on Cybercrime,[64] which distinguishes between four different types of offences[65]:

1. offences against the confidentiality, integrity and availability of computer data and systems;[66]
2. computer-related offences;[67]

---

[62] Some of the most well-known cybercrime offences are illegal access, illegal interception of computer data, data interference, computer-related fraud, computer-related forgery, dissemination of child pornography. For an overview see: *Sieber*, Council of Europe Organised Crime Report 2004; ABA International Guide to Combating Cybercrime, 2002; *Williams*, Cybercrime, 2005, in Miller, Encyclopaedia of Criminology.

[63] Gordon/Ford,(2006) On the Definition and Classification of Cybercrime, *Journal in Computer Virology*, Vol. 2, No. 1, page 13-20; Chawki, Cybercrime in France: An Overview, 2005, available at: www.crimeresearch.org/articles/cybercrime-in-france-overview; Gordon/Hosmer/Siedsma/Rebovich, (2003) *Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime*, available at: www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf.

[64] Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. Regarding the Convention on Cybercrime see: Sofaer, Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; Jones, (2005) The Council of Europe Convention on Cybercrime, Themes and Critiques, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; Broadhurst, Development in the global law enforcement of cyber-crime, in Policing: *An International Journal of Police Strategies and Management*, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No.4,2001, page 889 *et seq.*

[65] The same typology is used by the ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008. The report is available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[66] Art. 2 (Illegal access), Art. 3 (Illegal interception), Art. 4 (Data interference), Art. 5 (System interference), Art. 6 (Misuse of devices). For more information about the offences.

3. content-related offences;[68] and

4. copyright-related offences.[69]

This typology is not wholly consistent, as it is not based on a sole criterion to differentiate between categories. Three categories focus on the object of legal protection: "offences against the confidentiality, integrity and availability of computer data and systems"; content-related offences; and copyright related offences. The fourth category of "computer-related offences" does not focus on the object of legal protection, but on the method used to commit the crime. This inconsistency leads to some overlap between categories. In addition, some terms that are used to describe criminal acts (such as "cyberterrorism" or "phishing") cover acts that fall within several categories. Nonetheless, the four categories can serve as a useful basis for discussing the phenomena of cybercrime.[70]However, the most prevalent cybercrime in Nigeria are:

Hacking:[71] Software Piracy:.[72] Pornography: Credit Card or ATM Fraud:. Denial of Service Attack: Virus Dissemination:[73] Phishing:[74] Cyber Plagiarism:[75]. Cyber Stalking:[76] Cyber Defamation:[77] Cyber Terrorism:.[78] These are codified into our law known as Cybercrime Act 2015.

---

[67] Art. 7 (Computer-related forgery), Art. 8 (Computer-related fraud). For more information about the offences.
[68] Art. 9 (Offences related to child pornography). For more information about the offences,
[69] Art. 10 (Offences related to infringements of copyright and related rights). For more information about the offences,
[70] Marco Gercke, (2013) *Understanding cybercrime: phenomena, challenges and legal response* a new edition of a report previously entitled *Understanding Cybercrime: A Guide for Developing Countries*. The author wishes to thank the Infrastructure Enabling Environment and E-Application Department, ITU Telecommunication Development Bureau. September, P.12
This publication is available online at: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html
[71] Maitanmi Olusola et tal, 'Impact of Cyber Crimes on Nigerian Economy', *the International Journal of Engineering and Sciences (*IJES) Volume 2, Issue 4, p. 47. ISSN 2319-1813. Available at .
http://www.theijes.com/papers/v2-i4/part.%20%284%29/H0244045051.pdf. Accessed on 23/12/2015.
[72] *Ibid.*
[73]*Ibid.*
[74] *Ibid.*
[75] *Ibid.*
[76] *Ibid.*
[77] *Ibid.*
[78] *Ibid.*

Cybercrimes offence under the Act[79] include: offences against critical national information infrastructure; unlawful access to a computer system or net work; perpetration of electronic fraud or online fraud; system interference; interception electronic messages or processes; tampering with critical infrastructure; and the wilful misdirection of electronic messages. Unlawful interceptions; computer related forgery; computer related fraud; theft of electronic devices; unauthorized modification of computer systems, network data and system interference; forgery of electronic signatures are all offences under the Act.[80]

Other offences under the Act include: fraudulent issuance of e-instruction; identity theft and impersonations; child pornography; cyberstalking; cybersquatting; racist and xenophobic offences; unlawful importation and fabrication of e-tools; manipulation of Automated Teller Machine (ATM) or point of Sale (POS) terminals; phishing, spanning and spreading of computer virus; electronic cards related fraud; dealing in card of another; purchase or sale of card of another; and use of fraudulent device or attached e-mails and websites.[81]

This study presents the types of cyber crimes that have economic impact either directly or indirectly on the financial system of a nation or having cross border ripple effects. Longe & Chiemeke simplified the list of unintended consequences of ICT to include acts such as Phishing, cyber terrorism, electronic spam mails, cyber-stalking, and fake copy -cat websites. While

[79] Cybercrimes Act 2015.
[80] See Section 5-36. Ibid
[81] Ladan M.T., (2015) *Overview of the 2015 Legal and Policy Strategy on Cybercrime and Cybersecurity in Nigeria,* M.T Ladan's Law and Policy Review Research working Paper, May – August, p.10.

some types of cyber crimes are specific to Nigeria, other types, such as identity theft and false statements, cut across all countries.

i. PHISHING

According to Roger[82], phishing is simply a high-tech identity theft that does not only steal personal information and identity from unsuspecting consumers, but also an act of fraud against the legitimate businesses and financial institutions that are victimized by phishing. Phishing is usually a social engineering crime pervasive in attacking organisations' or individuals' (customers') information systems (IS) in order to gather private information to be used against organisations to extract some benefit for the perpetrator through the anonymity of identity theft or identity deception acts. According to recent estimates from the Anti- Phishing Working group[83] phishing scams remain a relatively small percentage of spam sent worldwide today. Phishing attempts to pose significant dangers for unsuspecting victims. It has become one of the fastest-growing worldwide threats on the Internet. This rapid growth has made combating it a huge priority for electronic mail service providers, since phishing impacts every aspect of the Internet and computing and there is no single action from any one company or organization to solve the problem. Data suggest that some phishing attacks have convinced up to 5% of their recipients to provide sensitive information to spoofed websites[84]. About two million users gave information to spoofed websites resulting in

[82] Roger, E.S. (2008) Rogers Communications Inc, *2008 Annual Report* . P12

[83] APWG (2004) *(Anti-Phishing Working Group). Phishing Activity Trends* Report. Available: http://www.antiphishing.org accessed on 19/12/2015 at 3:45 am

[84] Loftness, S. (2004) Responding to*"Phishing" Attacks.* Glenbrook Partners

direct losses of $1.2 billion for U.S. banks and card issuers in 2003[85]. Perpetrators target both document categories to secure personal identifying information. Often they obtain a 'set' of point of information documents in order to present themselves as 'legitimate customers' to deceive the target organisation's authentication and verification processes to commit identity fraud[86]. For example, 77% of United States (US) adults were online in May 2006, up from 74% in 2005, 66% in 2002, 64% in 2001, and 57% in 2000, according to e-Marketer[87]. In phishing e-mail messages, the senders must gain the trust of the recipients to convince them to divulge their personal information. To gain this trust, fraudsters "spoof," or mimic, a reputable company. The companies spoofed most often are financial services- Internet organizations such as the Bank of America, Citibank, eBay, PayPal, etc. Retailers and Internet service providers are also targeted[88] these phishing e-mails are usually mass mailed (Warner, 2004). Fraudsters rely on the responses from the few recipients who are customers of the spoofed company and who fall victim to the scam.

According to Longe, Mbarika, Korouma, Wada, & Isabalija[89], the scammers claim to be from reputable companies and go to great lengths to emulate the company's visible branding. Their fraudulent e-mails often contain the company's logo and use similar fonts and color schemes as those used on the company's web site. Some of the fraudulent e-mails simply reference images

[85] Litan, A. (2004). *Phising attack victims likely targets for identity theft*. Available: http://www.gartner.com/DisplayDocument?doc_cd=120804
[86] Kochems, A. & Keith, L (2006).*Successfully Securing Identity Documents: A Primer on Preventive Technologies and ID Theft*
[87] E-Marketer (2006) estimate and projections. http://www.emarketer.com/docs/emar_whitepaper.pdf. accessed on 20/12/2015 at 7.00pm
[88] Litan., A *op cit.*
[89] Longe,O.B, Mbarika, V, Kourouma, M, Wada, F & Isabalija, R., (2009) Seeing Beyond the Surface: Understanding and Tracking Fraudulent Cyber Activities. *International Journal of Computer Science and Information Security*. Vol. 6 (3) pp. 124-135.

from the legitimate company's site. The main link in a fraudulent e-mail sends the recipient to the fraudulent phishing web site, but many fraudulent e-mails include other links that send the recipient to sections of the real company's web site. To further convince the recipient that the e-mail originated from the reputable company, the scammers use a "from" e-mail address that appears to be from the company by using the company's domain name (e.g., @ebay.com, @paypal.com)[90]. Phishing e-mails also try to assure the recipient that the transaction is secure in hopes of gaining the recipient's trust. The following are assurances that were included in fraudulent e-mails *"Remember: eBay will not ask you for sensitive personal information (such as your password, credit card, bank account numbers, social security number, etc.) in an e-mail."* This e-mail then sends users to a fraudulent web site that asks for personal and account information while promising that the information is submitted via a secure server. The phishing perpetrators could then notify the victim of a "security threat." Such a message may be welcomed or expected by the victim, who would then be easily induced into disclosing personal information[91]. The number of unique phishing websites detected by APWG during the second half of 2008[92] saw a constant increase from July to October with a high of 27,739[93]

In Nigeria, the most recent phishing attacks were on the customers of Inter-switch, which remains the organization with the highest customer base in

[90] *Ibid.*
[91] Jaishankar K., (2008) *Space Transition Theory of Cyber Crimes, Crimes of the Internet*, Pearson, ISBN-13:978-0-13-231886-0, pp.283.
[92] APWG (Anti-Phishing Working Group) (2008). *Phishing Activity Trends Report*. Available: http://www.antiphishing.org accessed on 18/12/15 at 10:30pm.
[93] Atherton, M. (2010) *Criminals switch attention from Cheques and plastic to internet transactions.* The Sunday Times of March 10, 2010

electronic transactions. The Nigeria Deposit Insurance Corporation (NDIC) disclosed in its 2007 annual report and statement of account that underhand deals by bank staff, among others, resulted in attempted fraud cases totalling over N10.01 billion (over 65 million USD) and actual losses of N2.76 billion (13 million USD) in 2007[94]. With the present situation in the world economy and the appropriate technology, fraudulent action is most likely to increase and phishing remains one of the main means of performing "fraud without borders." The extent of readiness to stem phishing in Nigeria needs to be determined because fraudulent activities emanating from these nations have far-reaching consequences beyond her borders.[95]

ii. Cyber Terrorism

According to the U.S. Federal Bureau of Investigation, cyber terrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents"[96]. Unlike a nuisance virus or computer attack that result in a denial of service, a cyber terrorist attack is designed to cause physical violence or extreme financial harm. According to the U.S. Commission of Critical Infrastructure Protection, possible cyber terrorist targets include the banking industry, military installations, power plants, air traffic control centers, and water systems. Apart from that, there is another dimension to cyber terrorism – the use of cyber infrastructure to launder money for financing physical terrorism. In 2005, FBI

[94] Ahmed, I.(2008) Nigeria: N10 Billion Lost to Bank Fraud in 2007 – *NDIC, Daily Trust*, 28 October 2008
[95] *Ibid*
[96] See Search security (2009), *Information Security magazine*

officials reported that Al Qaeda terrorist cells in Spain used stolen credit card information to make numerous purchases[97].

According to Wilson, cyber terrorism is said to have taken place when the effects of a widespread computer network attack is unpredictable and might cause enough economic disruption, fear, and civilian deaths, to qualify as terrorism. At least two views exist for defining the term cyber terrorism[98].[99] These are (1) Cyber terrorism exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals. (2) Cyber terrorism exists when unlawful or politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage. The terrorist's use of the Internet and other telecommunications devices is growing both in terms of reliance for supporting organizational activities and for gaining expertise to achieve operational goals. Tighter physical and border security may also encourage terrorists and extremists to try to use other types of weapons to attack the United States. Persistent Internet and computer security vulnerabilities, which have been widely publicized, may gradually encourage terrorists to continue to enhance their computer skills, or develop alliances with criminal organizations. They will also probably consider attempting a cyber attack against the U.S. critical infrastructure[100]. Cybercrime has increased

[97] Tudor J.K., *(2001) IS security Architecture, An Integrated Approach to Security in the* Organization. Auerbach Publications, USA

[98]Collin, B.C. The Future of Cyber Terrorism: *Where the Physical and Virtual Worlds Converge,* 11th Annul International Symposium on Criminal Justice Issues .(1996)

[99] Denning DE (1999) Information Warfare and Security. ACM Press, USA

[100]Longe, O.B & Chiemeke, S.C.(2007). Beyond Web Intermediaries: *Framework for Protecting Web Contents on Clients Systems.* Paper Presented at the International Conference of the International Association of Engineers (IAENG) Imperial

dramatically in past years, and several recent terrorists events appear to have been funded partially through online credit card fraud. Reports indicate that terrorists and extremists in the Middle East and South Asia may be increasingly collaborating with cybercriminals for the international movement of money and for the smuggling of arms and illegal drugs[101]. These links with hackers and cybercriminals may be examples of the terrorists' desire to continue to refine their computer skills, and the relationships forged through collaborative drug trafficking efforts may also provide terrorists with access to highly skilled computer programmers.

iii. Electronic Spam Mails

These are unsolicited bulk e-mail to multiple recipients. They can be commercial, political, or religious. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, web search engines, and blogs. Spamming is popular because the advertisers have no operating costs beyond the management of their mailing lists and it is difficult to hold senders accountable for their mass mailings. As a result, costs such as lost productivity and fraud are borne by the public and by Internet service providers that have been forced to add extra capacity to cope with the deluge[102] A good example is 419 mails or the Nigerian advance fee frauds which in 1996 was estimated to have cost unsuspecting clientele over five billion dollars[103]. These mails emanate in a triangle called the "The Nigerian Connection" mostly in Europe and in some

[101] Dennings D.E op cit.
[102] Longe, O.B.& Chiemeke, S.C. (2008): Cybercrime and Criminality in Nigeria- What roles are internet Access Points in Playing. *European Journal of Social Sciences,* Volume 6 No 4.
[103] Smith, R.G., Holmes, M.N. & Kaufmann, P. (1999): *Nigerian advance fee fraud. Trends and Issues in Crime and Criminal Justice,* No. 121. Australian Institute of Criminology, Canberra. Available online at *http://www.aic.gov.au* accessed on 20/12/15 at 10:00am.

parts of Africa, "The 419 Coalition, 2005." The Nigerian Scam, according to published reports, is the third to fifth largest industry in Nigeria. It is the 419 Coalition view that, in effect, the elites from which successive governments of Nigeria have been drawn are the scammers. Therefore, victims have little recourse in this matter. Monies stolen by 419 operations are almost never recovered from Nigeria. Most 419 letters and e-mails originate from or are traceable back to Nigeria. However, some originate from other nations, mostly also West African nations such as Ghana, Cameroon, Togo, Liberia, Sierra Leone, Ivory Coast (Cote D'Ivoire), etc.

The effects of such scams have immense effects with confirmed losses of millions of dollars annually (Herald Tribute, 2007). According to Longe and Longe[104], governments have tried to come up with policies to try to curtail this menace. Nigeria, through the EFCC, banned night browsing. This is because most fraudulent activities are perpetrated at cyber cafés at nights. For now, there are no quantitative data to measure the effect of this action on the reduction or otherwise of cybercrime in Nigeria.

iv. Cyber Stalking

Stalking in the physical sense generally involves harassing or threatening behavior in which an individual engages repeatedly, such as following a person, appearing at a person's home or place of business, making harassing telephone calls, leaving written messages or objects, or vandalizing a person's property. According to,[105] cyber stalking refers to the use of the Internet, e-mail, or other electronic communications devices to stalk another person this

[104] Longe, O.B & Longe, F.A. (2005). The Nigerian Web Content: *Combating the Pornographic Malaise Using Web Filters. Journal of Information Technology Impact*. Vol. 5, No. 2 Loyola University, United States of America. www.jiti.net

[105] Ellison, L., & Akdeniz, Y.,(1998) "*Cyberstalking: the Regulation of Harassment on the Internet,"* Criminal Law Review, December Special Edition: Crime, Criminal Justice and the Internet, pp 29-48.

term is used interchangeably with online harassment and online abuse. Cyber stalking is becoming a common tactic in racism and other expressions of hate. Cyber stalkers target and harass their victims via websites, chatrooms, discussion forums, open publishing website (e.g., blogs) and e-mail. The availability of free email and website space, as well as the anonymity provided by these chat rooms and forums, has contributed to the increase of cyber stalking as a form of harassment[106].

Most stalking laws require that the perpetrator make a credible threat of violence against the victim; others include threats against the victim's immediate family; and still others require only that the alleged stalker's course of conduct constitute an implied threat[107]. While some conduct involving annoying or menacing behavior might fall short of illegal stalking, such behavior may be a prelude to stalking and violence and should be treated seriously. The nature and extent of the cyber stalking problem is difficult to quantify. Indeed, current trends and evidence suggest that cyber stalking is a serious problem that will grow in scope and complexity as more people take advantage of the internet and other telecommunications technologies[108]. Physical stalking, online harassment, and threats may be a prelude to more serious behavior, including physical violence. For example, the first U.S. cyber stalking law went into effect in 1999 in California. Other states include prohibition against cyber stalking in their harassment or stalking legislation. In Florida, HB 479 was introduced in 2003 to ban cyber stalking. This was signed into law in October 2003. The crime of cyber stalking is defined in

[106] Ibid
[107] See US Attorney General (1999) Cyberstalking: *A New Challenge for Law Enforcement and Industry*.A Report from the Attorney General to the Vice President August 1999.
[108] CCIPS, (1999) Cyber stalking*: A New Challenge for Law Enforcement and Industry. Workshop on the economics of information security*

Florida Statutes 784.048(1) (d) which is one of the strictest such laws in the United States.[109]

v. Fake Copy-Cat Web Sites

One recent trend in on-line fraud is the emergence of fake 'copy-cat' web sites that take advantage of consumers who are unfamiliar with the Internet or who do not know the exact web address of the legitimate company that they wish to visit. The consumer, believing that they are entering credit details in order to purchase goods from the intended company, is instead unwittingly entering details into a fraudster's personal database. The fraudster is then able to make use of this information at a later stage, either for his own purposes or to sell on to others interested in perpetrating credit card fraud

vi. Malware:

Malware, short for malicious software, (sometimes referred to as pestware) is a software designed to secretly access a computer system without the owner's informed consent

vii. **Spoofing** Spoofing or decoying is the practice of inundating online networks with bogus or incomplete files of the same name in an effort to frustrate the user.

viii. **Cyber Contraband:** This is transferring illegal items through the internet (such as encryption technology) that is banned in some locations.

ix. **Child Pornography:** This is the use of computer networks to create, distribute, or access materials that sexually exploit underage children.

[109] Smith, M. (2004) Cyberstalking and the Law

x. **Cyberlaundering:** Is an electronic transfer of illegally-obtained monies with the goal of hiding its source and possibly its destination.

xi. **Cybertheft:** This is an act of using a computer to steal. This includes activities related to; breaking and entering, embezzlement and unlawful appropriation, espionage, identity theft, fraud, malicious hacking, plagiarism, and piracy.

xii. **Cybervandalism:** Damaging or destroying data rather than stealing or misusing them (as with cybertheft) is called cybervandalism.

xiii. **Keylogging:** Keystroke logging (often called keylogging) is the practice of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.

2.2 The Concept of Cybersecurity

A secure cyberspace will hamper the continuous boom and smooth running of terrorist activities. In other words, a secure cyberspace is an effective anti-terrorism measure. Cybersecurity is the offensive way (otherwise known as a preventive measure) of combating terrorism. The security of the cyberspace is as crucial more than ever to the survival of mankind as the physical space is. This simply translates to the fact that the security of the cyberspace is not only necessary for the prevention of cyber attacks, but also physical and other forms of attacks that can be organized or coordinated via the cyberspace. From a counter-terrorism point of view, cybersecurity, as a tool, is necessary for intelligence gathering.

2.2.1 Meaning of Cybersecurity

There are many definition of the term "Cybersecurity" in use; however, we would present a couple of these: - first, Cyber security, referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.[110] Second, cybersecurity is "the state of being protected against the criminal or unauthorized use of electronic data, or measure taken to achieve this."[111]

Third, from International Telecommunications Union (ITU) Point, Cybersecurity is the collection of tools, policies, security concepts security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's of assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems and the totality of transmitted and/or stored information in the cyber environment cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the environment.[112]

---

[110] UMUC has been designated as a National Center of Academic Excellence in Information Assurance and Cyber Defense Education by the National Security Agency and the Department of Homeland Security.© 2015 University of Maryland University College

[111] Oxford Dictionaries (2013, June) online available *at* *http://oxforddictionaries.com*.

[112] www.itu.int/en/ITU-T/studygroups/com17/pages/cybersecurity.aspx. accessed on 19/12/2015 at 2:04pm.

Fourth, "Cybersecurity" is the sum efforts invested in addressing cyber risk, much of which was, until recently, considered so improbable that it hardly required our attention.[113] Cyber-security is the body of rules put in place for the protection of the cyber space. But as we become more dependent on cyberspace, we undoubtedly face new risks. Cyber-crime refers to the series of organized crime attacking both cyber space and cyber security. Sophisticated cyber criminals and nation-states, among others, present risks to our economy and national security. Nigeria's economic vitality and national security depend on a vast array of interdependent and critical networks, systems, services, and resources known as cyberspace. Cyber-space has transformed the ways we communicate, travel, power our homes, run our economy, and obtains government services. Cyber-security is the body of technology, processes and practices designed to protect networks, computers, programs and data from attacks, damage, or authorized access. In the computing or cyber context, the word security simply implies Cyber-security. Ensuring cyber-security requires coordinated efforts from both the citizens of the country and the country's information system.

The threat posed by breaches in our cyber-security is advancing faster than we can keep up with it. It is not possible to concentrate efforts on only one aspect of the breach as it means negligence and allowance of growth for other aspects of the breach. This leads us to conclude that we have to attack cyber security breaches as a whole. What then are these breaches? Cyber-crime refers to criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars

[113] Ladan M.T *op cit* p.81

from online bank accounts. Cybercrime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet. Perhaps the most prominent form of cybercrime is identity theft, in which criminals use the Internet to steal personal information from other users.[114] Perhaps the most complete definition of Cyber-crime is as given in our discussion under the concept of cybercrime.

2.2.2 Goals of Cyber Security

The following are the objectives of Cyber-security.

a. To help people reduce the vulnerability of their Information and Communication Technology (ICT) systems and networks.

b. To help individuals and institutions develop and nurture a culture of cyber security.

c. To work collaboratively with public, private and international entities to secure cyberspace.

d. To help understand the current trends in IT/cybercrime, and develop effective solutions.

e. Availability.

f. Integrity, which may include authenticity and non-repudiation.

g. Confidentiality.[115]

2.2.3 Some Key Cyber Security Terminology.[1]

"***Access***" means the making available of communications facilities and communications services one licensee to another for the purpose of providing services, and includes the connection of equipment by wire or wireless means,

[114] IbikunleF.,*opcitp.6*http://covenantuniversity.edu.ng/

[115] Ibid

access to physical infrastructure including but not limited to buildings, ducts and masts, access to mobile networks, in particular for roaming, and access to number translation or systems offering equivalent functionality;[116]

Active Attack: An actual assault perpetrated by an intentional threat source that attempts to alter a system, its resources, its data or its operations.

Blacklist: A list of entities that are blocked or denied privileges or access.

Bot: A computer connected to the Internet that has been surreptitiously/secretly compromised with malicious logic to perform activities under the remote command and control of a remote administrator.

Penetration Testing :An evaluation methodology whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system.

Root: A set of software tools with administrator-level access privileges installed on an information system and designed to hide the presence of the tools, maintain the access privileges and conceal the activities conducted by the tools.

Software Assurance: The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its lifecycle, and that the software functions in the intended manner.

Virus: A computer program that can replicate itself, infect a computer without permission or knowledge of the user and then spread or propagate to another computer.

[116]See, *Section 157* of Nigerian Communications Commission Act.

Whitelist: A list of entities that are considered trustworthy and are granted access or privileges.

2.2.4 Nigeria's Response to Terrorism

Nigeria is weak and fall short when it comes to emergency response. Taking proactive measures to forestall unwanted events is alien to the county. Signals are often ignored, warnings not paid due attention to. In the case of response to terrorism, unfortunately, it has been through vicious suppression of opposition through the Combating Terrorism with Cybersecurity: The Nigerian Perspective use of force. In spite of this, the frequency of attacks, including suicide bombings has ceased to abate[117]. Rather, it has been on the increase. There have even been reports of extra-judicial killings by the military and other security agencies, all in their bid to quench insurgence.[118] Challenges including lack of capacity for quality operational intelligence gathering, lack of cooperation from local population, and lack of trust between government and its citizens[119] have all being hampering the prospect of success. Generally speaking, the response to terrorism in Nigeria to a large extent has been on the defensive side, and mostly non-cyber in nature. No doubt, terrorists form a chunk, however small, of the country's population, and thus, a percentage of her cyberspace users. From

[117] "Respondingto Terrorism inNigeria."Retrievedfrom http://234next.com/csp/cms/sites/Next/News/National/5743941-146/responding_to_terrorism_in_nigeria.csp

[118] Human Rights Watch (2011), "A Human Rights Agenda for Candidates in Nigeria's 2011 Elections." Retrieved from http://www.hrw.org

[119] Forest, J. J. F. (2012). Confronting the Terrorism of Boko Haram in Nigeria. Retrieved on October 24, *2013 from http://www.jamesforest.com/wp-content/uploads/2012/06/Boko_Haram_JSOU-Report-2012.pdf*

observations, most of the activities of terrorists in the country are purely traditional terrorism. However, there were sparse occurrences of cyber terrorism activities where the telecommunication masts of some mobile network providers were attacked in some states[120]. Terrorists in Nigeria utilize the cyberspace for their activities, albeit not at an advanced level. Majorly, their exploitation has been limited to the usage of mobile technology for communicating between themselves and to media, and for planning, preparation, and coordination of attacks; and internet for propagating and communicating messages to the public. While terrorism seems to have become a reality the country may continue to live with, it is unwise to remain on the defensive side of this menace – reacting only after every attack. An evidence of the federal government's lack of capacity to appropriately respond offensively to the abuse of cyberspace by terrorists is the ban of mobile networks in the most affected areas.[121] No doubt, this would have had negative effects on innocent people's ability to communicate online. Businesses in these areas too must have felt these effects. On the part of the law making arm of the government, legislature, it has been a combination of lack of experience on general legislation, incapability of the part of some members, and lack of political will. These, and other reasons, explain why bills like the Cybersecurity and Information Protection Agency Bill was rejected by the House of Representative on the ground that it duplicated the efforts of some existing law enforcement agencies of the

[120] Adeyemi, K., Joel, D., Tsenzughul, A. (2012). Gunmen Attack MTN, Airtel masts in Kano, Borno, Bauchi, Yobe. The Nation Newspaper. Retrieved September 6, 2012. Retrieved from http://www.thenationonlineng.net/2011/news/60494-gunmen-attack-mtn-airtel-masts-in-kano-borno-bauchi-yobe.html, published in September, 2012.
[121] Abdullahi T.A *et al*, *op cit*

country.[122] It is surprising to know that the national security policy does not reflect present realities. The last review done was under the military regime in 1986, which led to the National Security Agencies Act.[123]

In this present age, considering the rapidity of development in every facet of human endeavor, a 27 years old document, enacted by the military, would hardly be relevant to tackle present challenges in a democratic setting. Also, Nigeria presently lacks capacities for digital forensics, internet filtering, to mention but few. There is also a lack of synergy among the security agencies. For instance, from videos posted online by some terrorist groups, using a voice recognition mechanism, the voice pattern of the speaker could be captured, and used to track the terrorist when next his voice traverses the cyberspace, say, through a phone call. Unfortunately, Nigeria lacks this capacity and required personnel.

Nigerian law enforcement agencies some are basically technology illiterate; they lack computer forensics training and often result to conducting police raids on Internet service site mainly for the purpose of extortion.

2.3 CONCEPT OF NATIONAL SECURITY

The issue of national security is one that has been on the top list of the Nigerian government in recent years. It has become a matter of concern, not

[122] Daily Champion Newspaper, *"Nigeria: Representatives Reject Cyber Bill."* Retrieved fromhttp://allafrica.com/stories/201103020802.html, published on March 2, 2011.

[123] Responding to Terrorism in Nigeria. "Retrieved from ttp://234next.com/csp/cms/sites/Next/News/National/5743941-146/responding_to_terrorism_in_nigeria.csp

only domestically, but also on the international plane. It is therefore commendable that this conference is being put together at such a time to discuss the issue of our national security and how it affects the development of the nation and also to chart a way forward.

2.3.1 DEFINITION OF NATIONAL SECURITY*:*

There is no single universally accepted definition of "National Security". The variety of definitions provides an overview of the many usages of this concept. The concept still remains ambiguous, having originated from simpler definitions, which initially emphasised the freedom from military threat and political coercion to later increase in sophistication and include other forms of non-military security as suited the circumstances of the time. The National Defence College of India defined National Security as "an appropriate and aggressive blend of political resilience and maturity, human resources, economic structure and capacity, technological competence, industrial base and availability of natural resources and finally the military might"[124] National security has been defined as freedom from hunger, or from threat to a nation's ability to protect and defend itself, progmote its cherished values and interests, and enhance the well-being of its people.[125] National security is a state or condition where our most cherished values and beliefs, our democratic way of life, our institutions of governance and our unity, welfare and well-being as a nation and people are permanently protected and continuously enhanced.[126]

[124] "Proceedings of Seminar on *"A Maritime Strategy for India" National Defence College"* Tees January .(1996) Marg, New Delhi, India. p.8
[125] Gwarzo I (1998) "Meeting the Current Challenges of National Security".
[126] http://www.dlsu.edu.ph/offices/osa/rotc/pdf/msl/threat-NatlSecurity. Retrieved on 03/01/2016 at 10:23am.

In the considered view of the writer, National security question involves a lot of issues. It practically touches on all spheres of human existence. The best way to approach it is from the systems theory perspective where a dislocation in any particular area of the system is bound to have an overlapping effect on other areas. It ranges from food security to issues of environmental degradation. It touches on health matters. It encompasses psychological security as well as arms security.[127]

2.3.2 National Security in Nigeria

It becomes clear that protecting the lives and property of citizens as well as improving their welfare and standard of living is at the heart of government's responsibility. This makes national security a part of, if not the most important element of national interest, and the provision of same is the main essence of government.

The importance attached to national security as an element of national interest and essence of government is not lost to Nigeria. Section14 **(2) (a)** of the Constitution of The Federal Republic of Nigeria[128]provides thus:

It is hereby, accordingly, declared that:

(b) the security and welfare of the people shall be the primary purpose of government; and

(c) the participation by the people in their government shall be ensured in accordance with the provisions of this Constitution."

Section 16(1)[129] provides as follows: "The state shall, within the context of the ideals and objectives for which provisions are made in this Constitution:

[127] Ebeh J.I., National Security and National Development*: A critique International Journal of Arts and Humanities* (IJAH) Bahir Dar- Ethiopia Vol.4(2) S/No 14, April, 2015; 1-14 ISSN: 2225-8590(Print) ISSN 2227-5452(online). www.afrrevjo.net/ijah.

[128] . CAP C20 Laws of the Federation of Nigeria 2004.

(a) harness the resources of the nation and promote national prosperity and an efficient, a dynamic and self reliant economy;

(b) control the national economy in such manner as to secure the maximum welfare, freedom and happiness of every citizen on the basis of social justice and equality of status and opportunity

(c) that suitable and adequate shelter, suitable and adequate food, reasonable national minimum living wage, old age care and pensions, and unemployment, sick benefits and welfare of the disabled are provided for all citizens."

Section 17(1) provides thus: "The State social order is founded on ideals of Freedom, Equality and Justice.

(2) In furtherance of the social order:

(a) every citizen shall have equality of rights, obligations and opportunities before the law,

(b) the sanctity of the human person shall be recognized and human dignity shall be maintained and enhanced;

(c) governmental actions shall be humane;"

(3) The State shall direct its policy towards ensuring that:

(a) all citizens, without discrimination on any group whatsoever, have the opportunity for securing adequate means of livelihood as well as adequate opportunity to secure suitable employment[130].

Section 18(1) provides thus "Government shall direct its policy towards ensuring that there are equal and adequate educational opportunities at all levels[131]"

Section 19 "The foreign policy objectives shall be:

---

[129] The Constitution of the Federal Republic of Nigeria 1999 As Amended.
[130] *Ibid*
[131] *Ibid*

(a) promotion and protection of national interest

(b) respect for international law and treaty obligations as well as the seeking of settlement of international disputes by negotiation, mediation, conciliation, arbitration and adjudication.[132]

Section 20 provides thus: "The state shall protect and improve the environment and safeguard the water, air and land, forest and wild life of Nigeria. This discussion is not oblivious of the different views and arguments that say Nigeria does not have a clearly defined national interest. This is in line with the fact that some authors believe that the generally acceptable view is national interest is a manifestation of the core values, objectives and philosophy underlying the actions of the leaders.28 This view also believes that the ground norm provides the true basis for the collective action, preference, predictions and sentiments of leaders.[133]

The above Constitutional provision, particularly

Section14 (2) (b) clearly shows that Nigeria as a country has some cove values that need to be promoted and protected. This also shows that Nigeria as a country has national.

In conclusion, the emergence of cyberspace, a virtual global domain, is increasingly impacting almost every aspect of our lives. The domain is transforming our economy and security posture more than ever before, creating opportunities for innovations and the means to improve general welfare of the citizens. However, behind this increasing dependence on cyberspace lies new risks that threaten the national economy and security.

[132] *Ibid*
[133] *Ibid*

Sensitive data, networks and systems that we now trust can be compromised or impaired, in a fashion that detection or defence can be hard, thus undermining our confidence in a connected economy. The Federal government is not unmindful of the diversity of implications of the nation's risk exposure in cyberspace, hence we have put in place cohesive measures towards addressing national risks effectively now and in the immediate future.

Being an issue of national priority in Nigeria, cyber security is now elevated to the level of being handled by the Presidency through the Office of the National Security Adviser (ONSA). A reflection of these could be seen in the presentation of the National Cyber Security Policy and Strategy drafts by the above-mentioned office. From the above definitions, it can be observed that national security is not restricted only to weapons and military preparedness but encompasses political, social and economic well-being of the people. Nigeria is interestingly at a defining moment in the establishment of a cyber-security policy and strategy framework. This is only an aspect of the numerous processes in their developmental stages concerning national security.[134]

In May, 2015, the Cyber Crime Act came to force; the National Cyber Security Policy and Strategy drafts were officially presented at a symposium held in Lagos. Characterized by an unrestricted borderless nature, the importance of security policy implementation through standardized and functional strategies in securing cyberspace cannot be overemphasized because of the government of Nigeria commitment to achieve active support,

[134] Oluwafemi O., & Agada D. O., (2015) *National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis; International Journal of Cyber Criminology* (IJCC) – Publisher & Editor-in-Chief – K. Jaishankar ISSN: 0973-5089 - January – June (2015). Vol. 9 (1): 120–143. DOI: 10.5281/zenodo.22390

participation and contributions of stakeholders from relevant sectors towards achieving increased national cyber security.

CHAPTER THREE
AN ANALYSIS OF LEGAL REGIME IN COMBATING CYBER CRIME

3.1 INTRODUCTION

The Internet has turned into a complex and challenging, if not menacing, gateway where criminal activities have progressed to attacks which are targeted and sophisticated. "Organised crime groups and cyber criminals are working together seamlessly, moving between the real world and virtual environments.[135] The domains of modern activities have extended beyond the turfs of land, sea, air and space to include the cyberspace. In this new environment there are immense endowments deployable for the economic activities, development and governance. Deviants have also leveraged on assets of the cyberspace to commit crimes and compromise national security. The nature and character of these crimes pose serious challenges for regulators across the world. To curb the menace of rogue activities in cybercrime, at international, regional and national level, strategies have been formulated. This chapter shall discuss the legal regimes in combating cybercrime at the international, regional and national level.

3.2 LEGAL FRAMEWORK BASED ON INTERNATIONAL STANDARDS

3.2.1 United Nations Office on Drugs and Crimes[136]

The United Nations has undertaken several important approaches to address the challenge of cybercrime. While in the beginning its response was limited to general guidelines, the organization has in recent times dealt more intensively with the challenges and legal response.

[135] The fight against Transnational Cyber Crime, In April 2007, the Strategic Alliance Cyber Crime Working Group (SACCWG) released its white Paper Transnational Cyber Crime and agreed that Combating Cyber Crime requires Transnational leadership and Cooperation. Platypus Magazine 98 edition, Septempber, 2007.
[136] The United Nations (UN) is an international organization founded in 1945. It had 193 Member States in 2017.

1. United Nations Convention on the Rights of the Child

The United Nations Convention on the Rights of the Child, adopted in 1989,[137] contains several instruments aiming to protect children. It does not define child pornography, nor does it contain provisions that harmonize the criminalization of the distribution of online child pornography. However, Article 34 calls upon Member States to prevent the exploitative use of children in pornographic performances.

2. United Nations General Assembly Resolution 45/121

After the eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (held in Havana, Cuba, 27 August – 7 September 1990), the UN General Assembly adopted a resolution dealing with computer-crime legislation.[138] Based on its Resolution 45/121 (1990), the UN published a manual in 1994 on the prevention and control of computer-related crime.[139]

3. Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography

The Optional Protocol not only addresses the issue of child pornography in general, but explicitly refers to the role of the Internet in distributing such material.[140] Child pornography is defined as any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual

[137] A/RES/44/25, adopted by the UN General Assembly on 12 December 1989.
[138] A/RES/45/121, adopted by the UN General Assembly on 14 December 1990. The full text of the resolution is available at: www.un.org/documents/ga/res/45/a45r121.htm.
[139] United Nation Manual on the Prevention and Control of Computer-Related Crime (United Nations publication, Sales No. E.94.IV.5),available at www.uncjin.org/Documents/EighthCongress.html.
[140] See the preface to the Optional Protocol.

parts of a child for primarily sexual purposes.[141] Article 3 requires the parties to criminalize certain conduct – including acts related to child pornography.

4. Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders

During the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held in Vienna in 2000, the impact of computer-related crimes was discussed in a specific workshop.[142] The debate focused especially on the categories of crime and transnational investigation, as well as legal response to the phenomenon.[143] The conclusions of the workshop contain major elements of the debate that is still ongoing: criminalization is required, legislation needs to include procedural instruments, international cooperation is crucial and public-private partnership should be strengthened.[144] In addition, the importance of capacity building was highlighted – an issue that was picked up again in subsequent years. The Vienna Declaration called upon the Commission on Crime Prevention and Criminal Justice to undertake work in this regard:

5. United Nations General Assembly Resolution 55/63

In its resolution, the General Assembly identified a number of measures to prevent the misuse of information technology, including: Resolution 55/63 invites States to take the necessary steps to combat cybercrime on the regional and international stage. This includes the

[141][141][141] See Art. 2.
[142] See especially the background paper: Crimes related to computer networks, A/CONF.187/10.
[143] Report of the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.185/15, No. 165, available at: www.uncjin.org/Documents/congr10/15e.pdf.
[144] *Ibid*

development of domestic legislation to eliminate safe havens for criminal misuse of technologies, improving law-enforcement capacities to cooperate across borders in the investigation and prosecution of international cases of criminal misuse of information technologies, improving information exchange, enhancing the security of data and computer systems, training law enforcement to deal specifically with the challenges associated with cybercrime, building mutual assistance regimes and raising public awareness of the threat of cybercrime.[145]

6. United Nation General Assembly Resolution 56/121

In 2002, the UN General Assembly adopted another resolution on combating the criminal misuse of information technology.[146] The resolution refers to the existing international approaches in fighting cybercrime and highlights various solutions. Resolution 56/121 underlines the need for cooperation among states in combating the criminal misuse of information technologies. It highlights the role that can be played by the United Nations and other international and regional organizations. The resolution further invites states to take into account the direction provided by the Commission on Crime Prevention and Criminal Justice when developing national legislation.

7. United Nation General Assembly Resolutions 57/239 and 58/199

Resolutions 57/239 and 58/199 are the two main UN General Assembly resolutions dealing with cybersecurity. Without going into detail with regard to cybercrime, they recall Resolutions 55/06 and

[145] A/RES/55/63. The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf.
[146] A/RES/56/121. The full text of the resolution is available at: http://daccessdds.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf.

56/121. Both resolutions furthermore emphasize the need for international cooperation in fighting cybercrime by recognizing that gaps in states' access to and use of information technologies can diminish the effectiveness of international cooperation in combating the criminal misuse of information technology.[147]

8. Eleventh UN Congress on Crime Prevention and Criminal Justice

Cybercrime was discussed during the eleventh UN Congress on Crime Prevention and Criminal Justice (the "UN Crime Congress") in Bangkok, Thailand, in 2005. Several challenges associated with the emerging use of computer systems in committing offences and the transnational dimension were addressed both in the background paper and in workshops.[148] Within the framework of the preparatory meetings in advance of the congress, some member countries such as Egypt called for a new UN convention against cybercrime, and the Western Asian regional preparatory meeting called for the negotiation of such convention.[149] The possibility of negotiating a convention was included in the discussion guide for the eleventh UN Crime Congress.[150] However, the Member States could at this time not decide to initiate a harmonization of legislation. The Bangkok Declaration therefore – without mentioning a specific instrument – refers to existing approaches.

[147] A/RES/57/239, on Creation of a global culture of cybersecurity; A/RES/58/199, on Creation of a global culture of
cybersecurity and the protection of critical information infrastructure.
[148] Measures to Combat Computer-related Crime, eleventh UN Congress on Crime Prevention and Criminal Justice, 2005,
A/CONF.203/14.
[149] Report of the Western Asian Regional Preparatory Meeting for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, A/CONF.2003/RPM.4/1, No. 14.
[150] see: Discussion guide to the eleventh United Nations Congress on Crime Prevention and Criminal Justice, 2003, A/CONF.203/RM.1.

9. United Nations General Assembly Resolution 60/177

UN General Assembly Resolution 60/177 endorsed the 2005 Bangkok Declaration, wherein the international community's efforts to enhance and supplement existing cooperation to prevent computer related crime were encouraged, inviting further exploration of the feasibility of providing assistance to Member States in addressing computer-related crime under the aegis of the United Nations, and in partnership with other similarly focused organizations.[151]

10. Twelfth UN Congress on Crime Prevention and Criminal Justice

At the congress itself, Member States took a major step toward more active involvement of the United Nations in the debate on the issue of computer crime and cybercrime. [152] The deliberations focused on two main issues: how can harmonization of legal standards be achieved, and how can developing countries be supported in fighting cybercrime? The first point is especially relevant if the UN develops comprehensive legal standards or suggests that Member States implement the Council of Europe Convention on Cybercrime. In preparation of the UN Crime Congress, the Council of Europe had expressed concerns regarding a UN approach[153] and had called for support for its Convention on Cybercrime. After an intensive debate,

[151] Declaration Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice, available at:
www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf.

[152] see: Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime, twelfth UN Congress on Crime Prevention and Criminal Justice, A/CONF.213/9.

[153] Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress on Crime Prevention and Criminal Justice, Information Documents SG/Inf(2010)4, 16.02.2010, page 17 *et seq.*

where the limited reach of the Convention on Cybercrime was discussed in particular, the Member States decided not to suggest to ratify the Convention on Cybercrime but to strengthen the UN's role in two important areas, which are reflected in the Salvador Declaration, The Member States thus recommended a strong mandate for the United Nations Office on Drugs and Crimes (UNODC) to provide global capacity building upon request. The second recommendation highlights that, at the time of the UN Crime Congress, Member States were unable to decide whether to develop a legal text or not.

11. United Nations General Assembly Resolution 64/211

In March 2010, the UN General Assembly passed a new resolution[154] as part of the "Creation of a global culture of cybersecurity" initiative. Resolution 64/211 refers to the two major resolutions on cybercrime[155] as well as the two main resolutions on cybersecurity.[156] The resolution further calls on states to use regional international conventions, arrangements and precedents in these reviews. The fact that four out of 18 subjects of the self-assessment tool are related to cybercrime highlights the importance of the ability of law enforcement to combat cybercrime effectively for maintaining cybersecurity.

Following the decision of the Member States to call upon UNODC to set up an intergovernmental working group, the first meeting of the group was held in Vienna in January 2011.[157] The expert group included representatives of

[154] Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.
[155] Resolutions 55/63 and 56/121.
[156] Resolutions 57/239 and 58/199.
[157] The report on the meeting of the open-ended working group (UNODC/CCPCJ/EG.4/2011/3) is available at: www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_3/UNODC_C

Member States, intergovernmental and international organizations, specialized agencies, private sector and academia. During the meeting the members of the expert group discussed a draft structure for a comprehensive study analysing the issue of cybercrime, as well as the response.[158] With regard to the legal response, a number of members underline the usefulness of existing international legal instruments, including the United Nations Convention against Transnational Organized Crime (UNTOC) and the Council of Europe Convention on Cybercrime, and the desirability of elaborating a global legal instrument to address specifically the problem of cybercrime. It was agreed that the decision on whether a global instrument should be developed will be made after the study was conducted. The United Nations Office for Drugs and Crime (UNODC) and the Commission on Crime Prevention and Criminal Justice adopted a resolution on effective crime prevention and criminal justice responses to combat sexual exploitation of children.[159] In 2004, the United Nations Economic and Social Council[160] adopted a resolution on international cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes.[161] A working group was established in 2005. A core group of experts on identity-

---

CPCJ_EG4_2011_3_E.pdf.

[158] Draft topics for consideration in a comprehensive study on the impact of and response to cybercrime, UNODC/CCPCJ/EG.4/2011/2. The document is available at: www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_2/UNODC_CCPCJ_EG4_2011_2_E.pdf.

[159] see: Note by the Secretariat regarding Commission on Crime prevention and criminal justice responses to urban crime, including gang-related activities, and effective crime prevention and criminal justice responses to combat sexual exploitation of children, CN.15/2007/CRP.3, available at: www.unodc.org/pdf/crime/session16th/E_CN15_2007_CRP3_E.pdf. Regarding the initiative relating to the resolution, see: www.america.gov/st/washfile-english/2007/April/20070423135940ajesrom0.709469.html.

[160] The United Nations Economic and Social Council (ECOSOC) is a principal organ to coordinate economic, social, and related work and serve as a central forum for discussing international economic and social issues. For more information, see: www.un.org/ecosoc/.

[161] ECOSOC Resolution 2004/26, on International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes, available at: www.un.org/ecosoc/docs/2004/Resolution%202004-26.pdf.

related crime was created to undertake a comprehensive study on the issue. In 2007, the ECOSOC adopted a resolution on international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime. Neither of these two resolutions explicitly addresses the challenges of Internet-related crimes, but they are applicable to those offences as well. In 2011 UNODC and the International Telecommunication Union (ITU) signed a memorandum of understanding related to cybercrime. The MOU covers cooperation (especially capacity building and technical assistance for developing countries), training and joint workshops. With regard to the capacity building activities the two organizations can refer to a wide network of field offices in all continents. Furthermore the organizations agreed to a joined dissemination of information and knowledge and data analysis.[162]

3.2.2 International Telecommunication Union

The International Telecommunication Union (ITU), as a specialized agency within the United Nations, plays a leading role in the standardization and development of telecommunications as well as cybersecurity issues.[163]

Among other activities, ITU was the lead agency of the World Summit on the Information Society (WSIS) that took place in two phases in Geneva, Switzerland (2003) and in Tunis, Tunisia (2005). Governments, policy-makers and experts from around the world shared ideas and experiences about how

[162] For further information see: www.unodc.org/unodc/en/frontpage/2011/May/unodc-and-itu-to-cooperate-moreclosely-to-make-the-internet-safer.html.

[163] The International Telecommunication Union (ITU) with headquarters in Geneva was founded as the International Telegraph Union in 1865. It is a specialized agency of the United Nations. ITU has 192 Member States and more than 700 Sector Members and Associates. For more information, see: www.itu.int.

best to address the emerging issues associated with the development of a global information society, including the development of compatible standards and laws. The outputs of the Summit are contained in the *Geneva Declaration of Principles*, the *Geneva Plan of Action*; the *Tunis Commitment* and the *Tunis Agenda for the Information Society*. The Geneva Plan of Action highlights the importance of measures in the fight against cybercrime:[164]

Cybercrime was also addressed at the second phase of WSIS in Tunis in 2005. The Tunis Agenda for the Information Society[165] highlights the need for international cooperation in the fight against cybercrime and refers to the existing legislative approaches such as the UN General Assembly resolutions and the Council of Europe Convention on Cybercrime.[166]

i) Global Cybersecurity Agenda

The Global Cybersecurity Agenda is made up of seven key goals, and built upon five strategic pillars, including the elaboration of strategies for the development of model cybercrime legislation.[167] The seven goals are the following:

1. Elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures.
2. Elaboration of strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime.

---

[164] WSIS Geneva Plan of Action, 2003, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0.

[165] WSIS Tunis Agenda for the Information Society, 2005, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.

[166] *Ibid*

[167] The five pillars are: legal measures, technical and procedural measures, organizational structures, capacity building,
international cooperation. For more information, see: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

3. Development of a strategy for the establishment of globally accepted minimum security criteria and accreditation schemes for software applications and systems.
4. Development of strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives.
5. Development of strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organizational structures to ensure the recognition of digital credentials for individuals across geographical boundaries.
6. Development of a global strategy to facilitate human and institutional capacity-building to enhance knowledge and know-how across sectors and in all the above-mentioned areas.
7. Advice on potential framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas.

In order to analyse and develop measure and strategies with regard to the seven goals of the GCA, the ITU Secretary-General created a high-level expert group (HLEG) bringing together representatives from Member States, industry as well as the scientific field.[168]In 2008, the expert group concluded negotiations and published the "Global Strategic Report".[169]

ii) Capacity building

Under the umbrella of the ITU GCA, ITU-D works to assist countries in implementing harmonized cybersecurity-related activities at the

[168] See: www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html.
[169] www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html; See: *Gerck*e, Zeitschrift fuer Urheber- undMedienrecht, 2009, Issue 7, page 533.

national, regional and international level. ITU's mandate in capacity building was emphasized by Resolution 130 (Rev. Guadalajara, 2010) of the ITU Plenipotentiary Conference. Based on the resolution, ITU has the mandate to assist Member States, in particular developing countries, in the elaboration of appropriate and workable legal measures relating to protection against cyberthreats.

This includes capacity-building activities in the development of national strategies, legislation and enforcement, organizational structures (e.g. watch, warning and incident response), among other areas. ITU has organized several regional conferences which have specifically addressed, *inter alia*, the issue of cybercrime.[170] Together with partners from the public and private sectors, ITU-D has developed cybersecurity/CIIP tools to assist Member States in raising national awareness, conducting national cybersecurity self-assessments, revising legislation and expanding watch, warning and incident-response capabilities. These tools include Understanding Cybercrime: A

[170] 23-25 November 2009 (Santo Domingo, Dominican Republic):www.itu.int/ITUD/cyb/events/2009/santo-domingo;23-25 September 2009 (Hyderabad, India): 2009 ITU Regional Cybersecurity Forum for Asia-Pacific; 4-5 June 2009 (Tunis, Tunisia): 2009 ITU Regional Cybersecurity Forum for Africa and Arab States; 18-22 May 2009 (Geneva, Switzerland): WSIS Forum of Events 2009, including Action Line C5 dedicated to building confidence and security in the
use of ICTs, and activities for child online protection; 7-9 September 2009 and 6-7 April 2009 (Geneva, Switzerland): ITUD Rapporteur's Group Meeting on Question 22/1 on Securing Information and Communication Networks; 7-9 October 2008 (Sofia, Bulgaria): ITU Regional Cybersecurity Forum for Europe and the Commonwealth of Independent States (CIS); 25-28 August 2008 (Lusaka, Zambia): ITU Regional Cybersecurity Forum for Eastern and Western Africa; 15-18 July
2008 (Brisbane, Australia): ITU Regional Cybersecurity Forum for Asia Pacific and Seminar on the Economics of Cybersecurity; 18-21 February 2008 (Doha, Qatar): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP) and Cybersecurity Forensics Workshop; 27-29 November 2007 (Praia, Cape Verde): ITU West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and CIIP, 29-31 October 2007
(Damascus, Syria): ITU Regional Workshop on E-Signatures and Identity Management; 16-18 October 2007 (Buenos Aires, Argentina): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP); 17 September 2007 (Geneva, Switzerland): Workshop on Frameworks for National Action: Cybersecurity and Critical Information Infrastructure Protection (CIIP); 28-31 August 2007 (Hanoi, Vietnam): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP).

Guide for Developing Countries, the ITU National Cybersecurity/CIIP Self-Assessment Tool and the ITU Botnet Mitigation Toolkit.[171]

iii) Resolutions

ITU has adopted several cybersecurity-related resolutions that are relevant to cybercrime, while not directly addressing the issue with specific criminal law provisions.

xiv. ITU Plenipotentiary Conference Resolution 130 (Rev. Guadalajara, 2010), on Strengthening the role of ITU in building confidence and security in the use of information and communication technologies.

xv. ITU Plenipotentiary Conference Resolution 149 (Antalya, 2006), on Study of definitions and terminology relating to building confidence and security in the use of information and communication technologies.

xvi. Resolution 45 (Doha, 2006) of the World Telecommunication Development Conference (WTDC), on Mechanisms for enhancing cooperation on cybersecurity, including combating spam and the report from *Meeting on Mechanisms for Cooperation on Cybersecurity and Combating Spam* (31 August – 1 September 2006).

xvii. Resolution 50 (Rev. Johannesburg, 2008) of the World Telecommunication Standardization Assembly (WTSA), on Cybersecurity.

xviii. Resolution 52 (Rev. Johannesburg, 2008) of the World Telecommunication Standardization Assembly (WTSA), on Countering and combating spam.

[171] *Ibid*

xix. Resolution 58 (Johannesburg, 2008) of the World Telecommunication Standardization Assembly (WTSA), on Encouraging the creation of national computer incident response teams, particularly for developing countries.[172]

3.3 LEGAL REGIME IN COMBATING CYBER CRIME AT REGIONAL LEVEL

In addition to the international organizations that are globally active, a number of international Organizations that focus of specific regions have move forward on activities that deal with issues related to cybercrime.

3.3.1 Council of Europe[173]

The Council of Europe is playing an active role in addressing the challenges of cybercrime. In 1976, the Council of Europe highlighted the international nature of computer-related crimes and discussed the topic at a conference dealing with aspects of economic crimes. This topic has since remained on its agenda.[174] In 1985, the Council of Europe appointed an Expert Committee to discuss the legal aspects of computer crimes.[175] In 1989, the European

[172] *Ibid*

[173] The Council of Europe, based in Strasbourg and founded in 1949, is an international organization representing 47 Member States in the European region. The Council of Europe is not to be confused with the Council of the European Union and the European Council (informally called the European Summit), as the Council of Europe is not part of the European Union, but a separate organization. In the first edition of this guide, the Council of Europe Convention was listed as an international approach. In consistency with the status of the international debate and UNGA Resolution 60/177, it is characterized as a regional approach and has been moved to this section.

[174] Twelfth Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime in
Strasbourg, 1976.

[175] The Expert Committee consisted of 15 experts, as well as observers from Canada, Japan, United States, the EEC, OECD
and UN. Source: *Nilsson* in *Sieber*, Information Technology Crime, page 577.

Committee on Crime Problems adopted the "Expert Report on Computer-Related Crime", analysing the substantive criminal legal provisions necessary to fight new forms of electronic crimes, including computer fraud and forgery.[176] The Committee of Ministers in 1989 adopted a recommendation[177] that specifically highlighted the international nature of computer crime:

In 1995, the Committee of Ministers adopted another recommendation dealing with the problems arising from transnational computer crimes.[178] Guidelines for the drafting of adequate legislation were summarized in the Appendix to the Recommendation.[179]

5) **Council of Europe Convention on Cybercrime and the Additional Protocol**

The European Committee on Crime Problems (CDPC) decided in 1996 to set up a committee of experts to deal with cybercrime.[180] The idea of going beyond principles for another recommendation and drafting a convention was present at the time of the establishment of the Committee of Experts.[181] Between 1997 and 2000, the committee held

[176] *Ibid*
[177] Recommendation No. R (89) 9, adopted by the Committee of Ministers on 13 September 1989 at the 428th Meeting of
the Ministers Deputies.
[178] Recommendation No. R (95) 13, adopted by the Committee of Ministers on 11 September 1995 at the 543rd Meeting of
the Ministers Deputies.
[179] The Guidelines deal with investigative instruments (e.g. search and seizure) as well as electronic evidence and international cooperation.
[180] Decision CDPC/103/211196. CDPC explained its decision by pointing out the international dimension of computer
crimes: "By connecting to communication and information services, users create a kind of common space, called "cyber-space", which is used for legitimate purposes, but may also be the subject of misuse.
[181] Explanatory Report of the Convention on Cybercrime (185), No. 10.

ten meetings in plenary and fifteen meetings of its open-ended Drafting Group. The Assembly adopted the draft Convention on Cybercrime in the second part of its plenary session in April 2001.[182] The finalized draft Convention was submitted for approval to CDPC and to the Committee of Ministers for adoption and opening for signature.[183] The Convention on Cybercrime was opened for signature at a signing ceremony in Budapest on 23 November 2001, during which 30 countries signed the Convention on Cybercrime (including four non-members of the Council of Europe – Canada, United States, Japan and South Africa – that participated in the negotiations). By April 2012, 47 states[184] have signed and 33 states[185] have ratified[186] the Council of Europe Convention on Cybercrime. In the meantime seven states were invited to accede to the Convention on Cybercrime, but have not done so.[187] The Convention on Cybercrime is today recognized as an important regional instrument in the fight against cybercrime and is supported by different international organizations.[188]

[182] The full text of Convention 185 (Convention on Cybercrime), the First Additional Protocol and the list of signatures and
ratifications are available at: www.coe.int.
[183] Understanding cybercrime: Phenomena, challenges andlegal response *Op cit* p. *124*
[184] Albania, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic,
Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia,
Slovenia, Spain, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Turkey, Ukraine, United Kingdom,
Canada, Japan, South Africa, United States.
[185] Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France,
Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Moldova, Montenegro, Netherlands, Norway, Portugal, Romania,
Serbia, Slovakia, Slovenia, Spain, The Former Yugoslav Republic of Macedonia, Ukraine, United Kingdom, United States.
[186] The need for a ratification is laid down in Article 36 of the Convention on Cybercrime
[187] Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico and Philippines.
[188] The Convention on Cybercrime shall be distributed to all Interpol member countries
in the four official languages", available at: www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp;

The Convention on Cybercrime was followed by the First Additional Protocol to the Convention on Cybercrime.[189] In the fourth draft version from 1998, the Convention still included a provision that required the parties to criminalize illegal content "concerning in particular matters such as child pornography and racial hatred".[190] To avoid a situation where countries would not be able to sign the Convention because of freedom of expression concerns, those issues were removed from the Convention on Cybercrime during the drafting process and integrated into a separate protocol. By January 2012, 35 states[191] have signed and 20 states[192] have ratified the Additional Protocol.

6) **Debate and limitation of the Council of Europe Convention on Cybercrime**[193] However, the debate in the twelfth Crime Congress highlighted that ten years after its opening for signature, the impact of the Convention is limited.[194] As of January 2011, the United States is the only country outside Europe that has ratified the instrument. It is true that the impact of the Convention cannot be measured solely by the number of signatures or ratifications, since countries such as

---

UNGA Resolutions 55/63 and56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but notlimited to, the Council of Europe's Convention on Cybercrime", available at: http://ec.europa.eu/information_society/activities/internationalrel/docs/wsis/tunis_agenda.pdf; APEC called for economies to study the Convention on Cybercrime, see: ITU Global Cybersecurity Agenda / High-Level Experts Group,
Global Strategic Report, 2008, page 18, available at:
www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html; OAS called for an evaluation of the Convention while designing Cybercrime legislation, see: ITU Global Cybersecurity Agenda / High-Level Experts Group,
Global Strategic Report, 2008, page 19, available at:
www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

[189] Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic
nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int.

[190] See Art. 3 of the Fourth Draft Convention, PC-CY (98) Draft No. 4, 17.04.1998.

[191] Albania (SUPRA).

[192] *Ibid*

[193] *Understanding cybercrime: Phenomena, challenges and legal response Op cit p.126*

[194] see: *Gercke*, 10 Years Convention on Cybercrime, Computer Law Review International, 2011, page 142 et seq.

Argentina,[195] Pakistan,[196] Philippines,[197] Egypt,[198] Botswana[199] and Nigeria[200] have used the Convention as a model and drafted parts of their legislation in accordance with the Convention on Cybercrime without formally acceding to it. Despite this, the Council of Europe claimed that more than 100 countries have signed, ratified or used the Convention when drafting domestic legislation.[201]

7) Global debate

One frequently criticized aspect of the Convention on Cybercrime is the inadequate representation of developing countries in the drafting process.[202] Despite the transnational dimension of cybercrime, its impact in the different regions of the world is different. This is especially relevant for developing countries.[203] Not only was the Convention on Cybercrime negotiated without any broad involvement of developing countries in Asia, Africa and Latin America, but it also places restrictive conditions on the participation of non-members of the Council of Europe, even though it was designed to be open to nonmembers. Based on Article 37 thereof, accession to the Convention

---

[195] Draft Code of Criminal Procedure, written by the Advisory Committee on the Reform of Criminal Procedural Legislation,
set up by Decree No. 115 of the National Executive Power of 13 February 2007 (Boletín Oficial of 16 February 2007).
[196] Draft Electronic Crime Act 2006.
[197] Draft Act Defining Cybercrime, providing for Prevention, Suppression and Imposition of Penalties therefore and for
other Purposes, House Bill No. 3777.
[198] Draft Law of Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.
[199] Draft Cybercrime and Computer related Crimes Bill 2007, Bill No. 17 of 2007.
[200] Draft Computer Security and Critical Information Infrastructure Protection Bill 2005.
[201] Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress, IDSG/Inf(2010)4, 2010, page 18.
[202] *El Sonbaty*, (2007) Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on
Cybercrime, Morocco , page 28, available at: www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.
[203] See in this context, for example: *OECD*, Spam Issues in Developing Countries, DSTI/CP/ICCP/SPAM(2005)6/FINAL, 2005,
page 4,

on Cybercrime requires consulting with and obtaining the unanimous consent of the contracting states to the Convention on Cybercrime. In addition, participation in the deliberations on possible future amendments is restricted to parties to the

Convention.[204] The debate within the framework of preparation of the twelfth UN Crime Congress showed that developing countries in particular are interested in an international approach rather than joining regional initiatives. During the regional preparatory meetings for the twelfth United Nations Congress on Crime Prevention and Criminal Justice for Latin America and Caribbean[205], Western Asia[206], Asia and Pacific[207]and Africa,[208]countries called for the development of an international convention on cybercrime. Similar calls were raised within academia.

8) Not designed for small and developing countries

Small and developing countries face difficulties in implementing the standards of the Convention. The fact that the smallest Council of Europe Member States did not ratify[209]the Convention in the last ten years clearly underlines that it is not only challenging for small countries outside of Europe but also small European countries. One of the provisions that causes difficulties when it comes to the implementation in small countries is the need to establish a

[204] See Art. 44 Convention on Cybercrime.
[205] "The Meeting also noted the imperative need to develop an international convention on cybercrime", held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).
[206] Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).
[207] Report of the Asian and Pacific Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).
[208] Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).
[209] Andorra, Monaco and San Marino did not even sign the Convention. Lichtenstein and Malta signed but never ratified
the Convention.

24/7 point of contact. Such contact point can have a highly positive impact on the speed of investigations and Article 35 is consequently one of the most important instruments provided by the Convention.[210]

However, it should be mentioned that recently the Council of Europe has published a study analysing the effectiveness of international cooperation against cybercrime and a study on the functioning of 24/7 points of contact against cybercrime[211]and the result of these two studies is that not all countries which have ratified the Convention have established such a contact point even countries which have provided such a contact point often only use it for limited purposes. The main problem for developing countries is the fact that the establishment of such contact point is mandatory. While for developed countries establishing and maintaining such a contact point will most likely not be challenging utilising a specialized police force dealing with cybercrime in night and day shifts, is however a challenge for countries where the specialized police force dealing with cybercrime consists of only one single police man. In those cases the obligation will require significant investments.[212]

9) Convention on the Protection of Children

Within its approach to improve the protection of minors against sexual exploitation, the Council of Europe introduced a new Convention in 2007.[213]

[210] See Explanatory Report to the Convention on Cybercrime, No. 298.
[211] The Functioning of 24/7 points of contact for cybercrime, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/567_24_7report3a%20_2%20april09.pdf.
[212] ICB4PAC Workshop on Concepts and Techniques of Developing CyberCrime Policy and Legislation, Apia, Samoa 22-25 August 2011.
[213] Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual

On the first day the Convention on the Protection of Children opened for signature 23 states signed the Convention. By April 2012, it had 42 signatory states,[214] of which 18 have ratified the Convention.[215] One of the key aims of the Convention on the Protection of Children is the harmonization of criminal law provisions aimed at protecting children from sexual exploitation.[216] To achieve this aim, the Convention contains a set of criminal law provisions. Apart from criminalization of the sexual abuse of children (Article 18), the Convention contains provisions dealing with the exchange of child pornography (Article 20) and the solicitation of children for sexual purposes (Article 23).

It is the considered view of the writer, that the Convention did not provide for comprehensive legal approaches, with other approaches – especially the Commonwealth Model Law on Computer and Computer-related Crime[217] as well as the EU instruments such as the E-Commerce Directive[218], shows that important aspects are missing. Examples are provisions dealing with the admissibility of electronic evidence[219] or with the liability of Internet Service Providers (ISPs). Especially the missing provision of a basic regulatory

---

Abuse (CETS No. 201).

[214] Austria, Belgium, Bulgaria, Croatia, Cyprus, Finland, France, Germany, Greece, Ireland, Lithuania, Moldova, Netherlands,
Norway, Poland, Portugal, Romania, San Marino, Serbia, Slovenia, Sweden, The former Yugoslav Republic of Macedonia
and Turkey. Albania, Armenia, Azerbaijan, Denmark, Estonia, Georgia, Hungary, Iceland, Italy, Liechtenstein, Luxembourg, Malta, Monaco, Montenegro, Slovakia, Spain, Switzerland, Ukraine and the United Kingdom followed.

[215] Albania Austria, Denmark, France, Greece, Malta, Montenegro, Netherlands, San Marino, Serbia and Spain.

[216] *Gercke*, Op cit

[217] Model Law on Computer and Computer Related Crime, LMM(02)17. For more information about the Model Law see:

[218] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178, 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the United States and European Union E-Commerce Regulations (including the EU E-Commerce Directive), see: *Pappas*, Comparative US & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol. 31, 2003, page 325 *et seq.*

[219] For further information and references on electronic evidence see blow: § 6.5.

framework related to the admissibility of electronic evidence has significant consequences as electronic evidence is widely characterized as a new category of evidence.[220] And unless a country has other instruments in place or its courts hold such evidence admissible, the country might not be able to sentence any offenders despite having fully implemented the Convention.

3.3.2 Organisation for Economic Co-operation and Development[221]

In 1983, the Organisation for Economic Co-operation and Development (OECD) initiated a study on the possibility of international harmonization of criminal law in order to address the problem of computer crime.[222] In 1985, it published a report that analysed the current legislation and made proposals for the fight against cybercrime. It recommended a minimum list of offences that countries should consider criminalizing, e.g. computer-related fraud, computer-related forgery, the alteration of computer programs and data, and the interception of the communications. In 1990, the Information, Computer and Communications Policy (ICCP) Committee created an Expert Group to develop a set of guidelines for information security, which was drafted by 1992 and then adopted by the OECD Council.[223] The guidelines include, among other aspects, the issues of sanctions. After reviewing the guidelines in 1997, the ICCP created a second Expert Group in 2001 that updated the guidelines. In 2002, a new version of the guidelines "OECD Guidelines for the

[220] *Lange/Nimsger*, (2004) Electronic Evidence and Discovery, 1. Regarding the historical development of computer
forensics and digital evidence, see: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View,
International Journal of Digital Evidence, 2002, Vol. 1, No. 1.

[221] The Organisation for Economic Co-operation and Development was founded 1961. It has 34 member countries and is
based in Paris. For more information, see: www.oecd.org.

[222] *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 8, available at:
www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[223] In 1992, the Council of the OECD adopted the Recommendation concerning Guidelines for the Security of Information
Systems. The 24 OECD member countries adopted the guidelines later.

Security of Information Systems and Networks: Towards a Culture of Security" was adopted as a Recommendation of the OECD Council.[224] The guidelines contain nine complementary principles.

In 2005, OECD published a report that analysed the impact of spam on developing countries.[225] The report showed that, on account of their more limited and more expensive resources, spam is a much more serious issue in developing countries than in developed countries such as the OECD Member States.[226] After receiving a request from the Strategic Planning Unit of the Executive Office of the Secretary General of the United Nations to produce a comparative outline of domestic legislative solutions regarding the use of the Internet for terrorist purposes, in 2007 OECD published a report on the legislative treatment of "cyberterror" in the domestic law of individual states.[227] In 2008, OECD published a Scoping Paper on online identity theft.[228] The paper provides an overview of the characteristics of identity theft, the different forms of identity theft, victim-related issues as well as law-enforcement schemes. The paper highlights that most OECD countries do not address the issue *per se* by means of specific provisions, and that the question whether ID theft should be criminalized as a standalone offence needs to be considered.[229] In 2009, OECD published a report on malicious software.

[224] Adopted by the OECD Council at its 1037th session on 25 July 2002. The 2002 OECD Guidelines for the Security of
Information Systems and Networks: Towards a Culture of Security, available at:
www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html.
[225] Spam Issue in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.
[226] *Ibid*
[227] The report is available at:
www.legislationline.org/upload/lawreviews/6c/8b/82fbe0f348b5153338e15b446ae1.pdf.
[228] Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI/CP(2007)3/FINAL, 2008, available at:
www.oecd.org/dataoecd/35/24/40644196.pdf.
[229] *Ibid*

Although the report briefly addresses aspects of criminalization, the focus is on the scope of malware and its economic impact.[230]

[230] Computer Viruses and other malicious software: A threat to the internet economy, OECD, 2009.

3.3.3 Asia-Pacific Economic Cooperation[231]

The Asia-Pacific Economic Cooperation (APEC) has identified cybercrime as an important field of activity, and APEC leaders have called for closer cooperation among officials involved in the fight against cybercrime. The Declaration of the 2008 meeting of the APEC Telecommunication and Information Ministers in Bangkok, Thailand, highlighted the importance of continuing collaboration to combat cybercrime.[232] Until now, APEC has not provided a legal framework on cybercrime, but has referred to international standards such as the Budapest Convention on Cybercrime. In addition, APEC has closely studied the national cybercrime legislation in various countries under a cybercrime legislation survey, and has developed a database of approaches to assist economies in developing and reviewing legislation.[233] The questionnaire used for the survey was based on the legal framework provided by the Budapest Convention on Cybercrime.

h. Statement on fighting terrorism (2002)

In 2002, APEC leaders released a Statement on Fighting Terrorism and Promoting Growth to enact comprehensive laws relating to cybercrime and develop national cybercrime investigating capabilities. They committed to endeavouring to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with the

[231] The Asia-Pacific Economic Cooperation (APEC) is a group of Pacific Rim countries dealing with the improvement of economic and political ties. It has 21 members.

[232] The Ministers stated in the declaration "their call for continued collaboration and sharing of information and experience between member economies to support a safe and trusted ICT environment including effective responses to ensure security against cyber threats, malicious attacks and spam." For more information, see: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html.

[233] See: Report to Leaders and Ministers on Actions of the Telecommunications and Information Working Group to Address Cybercrime and Cybersecurity, 2003/AMM/017.

provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 and the Council of Europe Convention on Cybercrime. [234]

i. Conference on cybercrime legislation (2005)

APEC has organized various conferences and called for closer cooperation among officials involved in the fight against cybercrime. In 2005, APEC organized a Conference on Cybercrime Legislation. The primary objectives of the conference were to promote the development of comprehensive legal frameworks to combat cybercrime and promote cybersecurity; assist law-enforcement authorities to respond to cutting-edge issues and the challenges raised by advances in technology; promote cooperation between cybercrime investigators across the region.[235]

j. Telecommunications and Information Working Group

The APEC Telecommunications and Information Working Group[236]actively participated in APEC's approaches to increase cybersecurity. In 2002, it adopted the APEC Cybersecurity Strategy.[237]

---

[234] APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico, on 26 October 2002.
Regarding national legislation on cybercrime in the Asian-Pacific region, see: *Urbas*, Cybercrime Legislation in the Asia-
Pacific Region, 2001, available at: www.aic.gov.au/conferences/other/urbas_gregor/2001-04-cybercrime.pdf.

[235] Cybercrime Legislation and Enforcement Capacity Building Project – 3rd Conference of Experts and Training Seminar,
APEC Telecommunications and Information Working Group, 32nd Meeting, 5-9 September 2005, Seoul, Korea.

[236] "Economies are currently implementing and enacting cybersecurity laws, consistent with the UN General Assembly
Resolution 55/63 (2000) and the Convention on Cybercrime (2001). The TEL Cybercrime Legislation initiative and
Enforcement Capacity Building Project will support institutions to implement new laws."

[237] The APEC Telecommunications and Information Working Group was founded in 1990. It aims to improve telecommunications and information infrastructure in the Asia-Pacific region by developing information policies. For
more information, see:
www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

The Working Group expressed their position regarding cybercrime legislation by referring to existing international approaches from the UN and the Council of Europe. Experiences with drafting cybercrime legislation were discussed within the context of the e-Security Task Group of the Telecommunications and Information Working Group during two conferences in Thailand in 2003.[238]

3.3.4 The Commonwealth

Cybercrime is among the issues addressed by the Commonwealth. The activities concentrate in particular on harmonization of legislation. This approach to harmonize legislation within the Commonwealth and enable international cooperation was influenced, among other things, by the fact that, without such an approach, it would require no fewer than 1 272 bilateral treaties within the Commonwealth to deal with international cooperation in this matter.[239] The Expert Group presented its report and recommendations in March 2002.[240] Later in 2002, the draft Model Law on Computer and Computer Related Crime was presented.[241] In addition to providing legislation; the Commonwealth has organized several training activities. The Commonwealth Network of IT and Development (COMNET-IT) co-organized training on cybercrime in April 2007.

In 2009, the Commonwealth Third Country Training Programme on legal framework for ICT was held in Malta, with the support of the Commonwealth Fund for Technical Co-operation (CFTC). Training was organized in 2011, In

[238] 2003/SOMIII/ECSG/O21.
[239] *Bourne*,(2002) Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf.
[240] See: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FABAA77-86970A639B05%7D_Computer%20Crime.pdf (Annex 1).
[241] Model Law on Computer and Computer Related Crime, LMM(02)17; the Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf.

2011 the Commonwealth presented "The Commonwealth Cybercrime Initiative". The main objective of the initiative is to assist Commonwealth countries in building their institutional, human and technical capacities with respect to policy, legislation, regulation, investigation and law enforcement. It aims to enable all Commonwealth countries to effectively cooperate in the global combat of cybercrime.[242]

3.3.5 African Union

In 2011 the African Union presented the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa.[243] The Convention is more comprehensive than most other regional approaches. It contains four parts. Part one is related to electronic commerce. It addresses various aspects such as contractual responsibility of an electronic provider of goods and services[244], treaty obligations in electronic form[245] and security of electronic transactions.[246] The second part deals with data protection issues.[247] The third part is related to combating cybercrime. Section 1 contains five chapters. This includes a set of six definitions (electronic communication, computerized data, racism and xenophobia in ICTs, minor, child pornography and computer system).[248]

In addition the third part addresses the need of a national cybersecurity policy and a related strategy.[249] The second chapter deals with general aspects related

[242] For more information see: www.waigf.org/IMG/pdf/Cybercrime_Initiative_Outline.pdf.
[243] The Draft Convention is available for download at: www.itu.int/ITUD/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf
[244] See Part 1, Sec. II, Ch. II.
[245] See Part 1, Sec. IV.
[246] See Part 1, Sec. V.
[247] See Part 2.
[248] Art. III-1.
[249] Part 3, Chaptr 1, Art. 1 and Art. 2.

to legal measures. This includes standards related to statuatory authorities, democratic principles, protection of essential information infrastructure, harmonization, double criminality and international cooperation[250]. The third chapter addresses issues related to a national cyber security system. This includes a culture of security, the role of the government, public-private partnership, education and training and public awareness-raising.[251] Chapter 4 is dedicated to national cyber security monitoring structures. The fifth chapter deals with international cooperation. The main difference to comparable regional frameworks such as the Council of Europe Convention on Cybercrime is the fact that the Draft African Union Convention– if no other instrument for international cooperation is in place – cannot be used for such purpose. The different conception is especially expressed by Articles 21 and 25.

Section II of the third part deals with substantive penal law. Section 1 includes a criminalization of illegal access to a computer system,[252] illegal remaining in a computer system,[253] illegal system interference[254], illegal data input,[255] illegal data interception[256] and illegal data interference.[257] The provisions show a lot of similarities with best practices from other regions – including standards introduced within Africa. One example is the criminalization of illegal remaining in a computer system that was introduced by the Draft ECOWAS Directive.

[250] Art. III-1-1 to Art. III-1-7
[251] Art. III-1-8 to Art. III-1-12
[252] Art. III-2.
[253] Art. III-3.
[254] Art. III-4.
[255] Art. III-5.
[256] Art. III-6.
[257] Art. III-7 1).

One new concept – however, not criminal law provision but a side measure – that was in this regard not introduced by other regional frameworks is the introduction of an obligation of businesses to submit their products from vulnerability testing.

Section 2 includes the criminalization of aspects of computer-related forgery,[258] illegal use of data[259], illegal system interference with the intent to obtain an advantage[260], data protection violations[261], illegal devices[262] and participation in a criminal organization.[263]

Section 3 deals with the criminalization of illegal content. The Draft African Convention introduces a criminalization of producing and disseminating child pornography,[264] procuring and importing child pornography[265], possessing child pornography[266], facilitating the access of minors to pornography[267], dissemination of racist or xenophobic material[268] , racist attacks perpetrated through computer systems[269] , racist abuse through computer systems[270] and denying or approving genocide or crimes against humanity.[271] The last section of Chapter 1 contains provisions that deal in a broader manner with legislation related to Cybercrime and the admissibility of electronic evidence ("written electronic matter"). Chapter two contains provisions that intend to update traditional provisions to ensure applicability when it comes to the involvement

[258] Art. III-8..
[259] Art. III-9.
[260] Art. III-10.
[261] Art. III-11.
[262] Art. III-12.
[263] Art. III-13.
[264] Art. III-14.
[265] Art. III-15.
[266] Art. III-16.
[267] Art. III-17.
[268] Art. III-19.
[269] Art. III-20.
[270] Art. III-21.
[271] Art. III-22.

of computer systems and data. It requires countries to set up an aggravation of penalty if traditional crimes are committed by using information and communication technology[272], the criminalization violation of property by offences such as theft, abuse of trust or blackmail involving computer data[273], update provisions that include dissemination facilities to ensure that the use of means of digital electronic communication is covered[274]and ensure that provisions that protect secrecy in the interest of national security are applicable with regard to computer data.[275] Such provisions are not included in other regional frameworks. With regard to Article III-24 it is uncertain why the mere fact that a computer system was used at one stage during the commission of a traditional offence (eg. the offenders send an email prior to breaking into a bank instead of making a phone call) shall lead to an aggravated sentence. Article III-28 – Article III- 35 deal with liability and sanctions. Section III deals with procedural law. It requires that Member States enable the conservation of computer data[276], the seizure of computer data [277] , expedited preservation[278] and interception of data communication.[279]

3.3.6 Arab League and Gulf Cooperation Council[280]

A number of countries in the Arabic region have already undertaken national measures and adopted approaches to combat cybercrime, or are in the process of drafting legislation.[281] Examples of such countries include Pakistan[282],

[272] Art. III-24.
[273] Art. III-25.
[274] Art. III-26.
[275] Art. III-27.
[276] Art. III-36.
[277] Art. III-37.
[278] Art. III-39.
[279] Art. III-41.
[280] The League of Arab States is a regional organization, with currently 22 members.
[281] See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 20, available at:

Egypt[283] and the United Arabic Emirates (UAE)[284]. In order to harmonize legislation in the region, UAE submitted model legislation to the Arab League (Guiding Law to Fight IT Crime).[285] In 2003, the Arab Interior Ministers Council and the Arab Justice Ministers Council adopted the law. The Gulf Cooperation Council (GCC) recommended at a conference in 2007 that the GCC countries seek a joint approach that takes into consideration international standards.[286]

3.3.7 Organization of American States[287]

Since 1999, the Organization of American States (OAS) has actively been addressing the issue of cybercrime within the region. Among others, the organization has held a number of meetings within the mandate and scope of REMJA, the Ministers of Justice or Ministers or Attorneys General of the Americas.[288]

REMJA has held eight meetings until 2010.[289] At the third meeting, in 2000, the Ministers of Justice or Ministers or Attorneys General of the Americas addressed the topic of cybercrime and agreed on a number of recommendations.[290] The meeting further recommended that Member States should review mechanisms to facilitate broad and efficient cooperation among

---

www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
[282] Draft Electronic Crime Act 2006.
[283] Draft Law on Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.
[284] Law No. 2 of 2006, enacted in February 2006.
[285] Regional Conference Booklet on: Cybercrime, Morocco, 2007, page 6, available at: www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.
[286] Decision of the Arab Justice Ministers Council, 19th session, 495-D19-8/10/2003.
[287] The Organization of American States is an international organization with 34 active Member States. For more information, see: www.oas.org/documents/eng/memberstates.asp.
[288] For more information, see: www.oas.org/juridico/english/cyber.htm, and the Final report of the Fifth Meeting of
REMJA, which contains the full list of reports, results of the plenary session and conclusions and recommendations, at:
www.oas.org/juridico/english/ministry_of_justice_v.htm.
[289] *Ibid*
[290] *Ibid*

themselves to combat cybercrime and study, where possible, the development of technical and legal capacity to join the 24/7 Network established by the G8 to assist in cybercrime investigations. Member States were asked to evaluate the advisability of implementing the principles of the Council of Europe Convention on Cybercrime and consider the possibility of acceding to that Convention.

The recommendations called for OAS Member States to review and, if appropriate, update the structure and work of domestic bodies, or agencies in charge of enforcing the laws so as to adapt to the shifting nature of cybercrime, including by reviewing the relationship between agencies that combat cybercrime and those that provide traditional police or mutual legal assistance.[291]

Finally, the secretariats of the Inter-American Committee against Terrorism (CICTE) and the Inter-American Telecommunication Commission (CITEL) and the Working Group on Cybercrime were requested to continue developing permanent coordination and cooperation actions to ensure the implementation of the Comprehensive Inter-American Cybersecurity Strategy adopted through OAS General Assembly Resolution AG/RES. 2004 (XXXIV-O/04).[292]

In 2010, REMJA addressed the issue of cybercrime at their eighth meeting. They briefly discussed the importance of continuing to consolidate and update the Inter-American Portal for Cooperation in Cybercrime through the OAS Internet page, and strengthening states' capacity to develop legislation and procedural measures related to cybercrime and electronic evidence. In

[291] *Ibid*

[292] Conclusions and Recommendations of REMJA-VII, 2008, are available at: www.oas.org/juridico/english/cybVII_CR.pdf.

addition, the meeting's recommendations highlighted the desire to strengthen mechanisms that allow for the exchange of information and cooperation with other international organizations and agencies in the area of cybercrime, such as the Council of Europe, the UN, the EU, APEC, OECD, the G8, the Commonwealth and Interpol, so that OAS Member States can take advantage of developments in those entities. [293]

3.3.8 Caribbean

In December 2008, ITU and the EU launched the project "Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures" (HIPCAR) to promote the ICT sector in the Caribbean region.[294] The project forms part of the programme "ACP-Information and Communication Technologies" and the ninth European Development Fund. Beneficiary countries are 15 Caribbean countries.[295] The aim of the project is to assist CARIFORUM countries to harmonize their ICT policies and legal frameworks.[296]

The model legislative text contains a complex set of definitions, and substantive criminal law provisions, including provisions dealing with issues like SPAM that have a high priority for the region but are not necessarily

[293] Conclusions and Recommendations of REMJA-VIII, 2010, are available at: ww.oas.org/en/sla/dlc/remja/recom_VIII_en.pdf.
[294] see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.
[295] The beneficiary countries are: Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic,
Grenada, Guyana, Haiti, Jamaica, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Suriname and Trinidad
and Tobago.
[296] CARIFORUM is a regional organization of 15 independent countries in the Caribbean region (Antigua and Barbuda,
Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, Saint Kitts and Nevis, Saint
Lucia, Saint Vincent and the Grenadines, Suriname, and Trinidad and Tobago).

contained in regional frameworks such as the Council of Europe Convention on Cybercrime.[297]

Furthermore, the text contains procedural law provisions (including advanced investigation instruments such as the use of remote forensic tools) and provisions on the liability of Internet service providers (ISPs).[298]

3.3.9 Pacific

In parallel to the ITU and EU co-funded project in the Caribbean the same organizations launched a project in the Pacific (ICB4PAC).[299]The project aims – based on a request by the the Pacific Island countries – to provide capacity building related to ICT policies and regulations. In this regard it focuses on building human and institutional capacity in the field of ICT through training, education and knowledge sharing measures. Beneficiary countries are 15 Pacific Island countries.[300] In March 2011 a workshop dealing with the current cybercrime legislation in the Pacific region was hosted in Vanuatu.[301]During the workshop a comprehensive comparative legal analysis was presented that provided an overview about existing legislation in the region as well as a comparison with best practices from other regions. As a follow up to this workshop a conference dealing with techniques of developing cybercrime policies and legislation was organized in August 2011 in Samoa.[302] During the conference best practices from other regions were presented and structures for

[297] *Ibid*
[298] *Ibid*
[299] For further information about the project see: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.
[300] Cook Islands, East Timor, Fiji, Kiribati, Marshall Islands, Federated States of Micronesia, Nauru, Niue, Palau, Papua New
Guinea, Samoa, Salomon Islands, Tonga, Tuvalu and Vanuatu.
[301] More information about the event are available at: www.itu.int/ITUD/
projects/ITU_EC_ACP/icb4pis/events/2011/port_vila/port_vila.html.
[302] see: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/events/2011/samoa/samoa.html.

a harmonized policy and legislation were developed. They addressed substantive criminal law, procedural law, international cooperation, liability of Internet Service Provider (ISP), electronic evidence and crime prevention measures.

In April 2011 the Secretariat of the Pacific Community organized a conference related to the Fight against Cybercrime in the Pacific.[303] The event was co-organized by the Council of Europe. During the conference aspects related to substantive criminal law, procedural law and international cooperation were discussed.[304]

3.4 Legal Responses in Combating Cyber Crime in Nigeria.

Recent trend in legal responses to Cybercrime and Cybersecurity in Nigeria the first sets of relevant legislations are:-

3. **Criminal Code Act:**[305] This act provides for advance fee fraud scam with the '419 scam' having been derived from its section 419, which provides for obtaining by false pretence.

> "Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years.[306]"

This section has been used for years by the Nigerian law enforcement agencies for prosecuting alleged acquisition of property by false pretence. Given that the Act is a relic of colonialism; its provisions are ill-suited for cyberspace

[303] More information about the event are available at: www.spc.int/en/component/content/article/704-responding-tocybercrime-threats-in-the-pacific.html.
[304] An overview about the output of the conference is available at: and www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_tonga_apr_11/AGREED_Cybercrime_Worksh op_Outcomes.pdf.
[305] CAP C28, LFN 2004.
[306] (Part 6, chapters 34 &38, Laws of the Federation of Nigeria Act, 1990)

criminal governance as it was enacted to penalised general offence in the southern part of Nigeria it does apply to cybercrimes.[307]

4. **Economic and Financial Crimes Commission (EFCC) Act 2004**:[308] This act, enacted in 2004, gives the Commission powers to arrest and prosecute any person suspected to be involved in the promotion of cybercrime in any form including drug trafficking, money laundering and terrorism. The Commission was imbued with extensive powers of arrest and prosecution which raised concerns about abuse. The EFCC continues to make efforts to eradicate the menace of cybercrime especially that colloquially known as cyber criminals or hackers, Indeed, cyber cafes were raided with hundreds of suspects arrested and successfully prosecuted with the ill-gotten wealth either remitted to the victims or forfeited to the Federal Government. For more details on EFCC see chapter four of this work.

5. Money Laundering (Prohibition) Act (MLA) 2011 (as amended): This Act "makes comprehensive provisions to prohibit the financing of terrorism, the laundering of the proceeds of a crime, or an illegal act." All financial institutions are required to report transactions made that are above specified thresholds for individuals and corporate bodies. The threshold is billed at US$10,000 or its equivalent shall be reported to the Central Bank of Nigeria, Security and exchange Commission or the Commission in writing within 7 days from the date of transaction. The Act is essentially structured to enable the authorities monitor cash transactions in a bid to tackle money laundering.

[307] Olanikpekun O., *op cit* p.15
[308] CAP E1, LFN 2004.

By section 14 (1) (a) & (b)[309]

"A person who

a. converts or transfer resources or property derived directly or indirectly from illicit traffic in narcotic drugs or psychotropic substances or any illegal act, with the aim of either concealing or disguising the illicit origin of the resources or property, or aiding any person involved in the illicit traffic in narcotic drugs or psychotropic substances or any other crime or illegal act to evade the legal consequences of his action; or

b. collaborates in concealing or disguising the genuine nature, origin, location, disposition, movement or ownership of the resources, property or rights thereto derived directly or indirectly from illicit traffic narcotic drugs or psychotropic substances or any other crime or illegal act, commits an offence under this section and is liable on conviction to imprisonment for a term of not less than two years or more than three years.

6. **Advance Fee Fraud and Other Related Offences Act 2006:**

This Act outlaws every form of fraud including obtaining property by false pretense and obtaining funds through unlawful activities. Unlike previous legislations, this law obliges industry players including ISPs and cybercafé operators to register with the EFCC and monitor activities of internet users and report any suspicious activities to the EFCC.[310] If properly enforced, the government is better enabled to guard against cybercrime. In *Federal Republic of Nigeria v. Abdul*,[311] the accused was arraigned on a two-count charge of being in possession of documents containing false pretences contrary to Section 6(8)(b) and 1(3) of the Advance Fee Fraud and Other Related Offences Act. The accused was arrested in a cybercafé in Benin City by a group of EFCC operatives, following a petition to the Commission by a citizen alleging the incidence of Internet crimes activities at the

[309] Money Laundering (Prohibition) Act (MLA) 2011 (as amended)
[310] Section 13.
[311] [2007] EFCLR 204 at 228

cybercafé. The accused and other customers of the cybercafé were subjected to a search, at the end of which a handwritten letter and a diary containing several email addresses were recovered from the accused. Subsequently, the EFCC investigators, using the addresses found in the dairy also discovered a number of scam e-mails in the e-mail of the accused. The e-mails were printed out by an official of the EFCC. At the trial, the handwritten letter, diary and printouts were tendered as exhibits by the prosecution. One of the questions that arose for determination by the court was whether or not the printouts which were tendered and admitted in evidence as Exhibits D, D1 and D2, could be said to be in the possession of the accused, when they were not found physically with him but were printed out of his e-mail box after his arrest. *Idahosa, J***,** discharged and acquitted the accused in the absence of a forensic expert witness stated:

> The Prosecution did not call the said Olaolu Adegbite to tell the Court how he managed to do what PW3 said he did. It must be understood that the court is not entitled to employ its own knowledge of this new technology, to complete the case of the prosecution. The problem is that with this new technology, the traditional definitions of possession... seems inadequate, to describe a situation where there are electronic mail boxes, with documents in them floating, about in space. There is a need to explain this to the court vide an expert witness. This would enable the Court determine whether or not the fact of a document floating about in space in the mail box of the accused was in his possession.

The Act of 2011 does not seem to have dealt with the problems associated with the use of electronic evidence in cybercrime prosecution.[312]

7. **Nigeria Deposit Insurance Corporation (NDIC) Act 2006:** Sections 27 – 32 of the Act mandate the NDIC to carry out onsite and offsite surveillance of insured financial institutions. The principal rationale for this mandate is the prevention of fraud in the banking system. Due to the potent threat of electronic/cyber fraud, the NDIC and CBN have developed the Electronic Financial Audit Sub-System (E-FASS) towards the actualisation of its mandate under sections 27 – 32 of the Act.

8. **Banks and Other Financial Institutions (BOFIA) Act**:[313] Sections 31 – 36 of the Act mandate the CBN to carry out onsite and offsite surveillance of regulated financial institutions. The principal rationale for this mandate is the prevention of fraud in the banking system. Due to the potent threat of electronic/cyber fraud, the CBN and NDIC have developed the Electronic Financial Audit Sub-System (E-FASS) towards the actualisation of its mandate under sections 31 – 36 of the Act.

9. An Overview of Cybercrimes (Prohibition, Prevention etc.) Act, 2015

[312] Dr. Kathleen O., Dr. Wiseman U., Nyako A., Tosin O., (2016) *Prosecution of Cyber crimes in Nigeria: Matters arising* Paper Presented at 49th Annual Nigerian Association of Law Teachers (NALT) Conference Nasarawa State University, Keffi. 27Th May

[313] CAP B3, LFN 2004.

In terms of rationale the Act was enacted to provide for the prohibition, prevention, detection, response, investigation and prosecution of cybercrimes; and for other related matters.[314]

The statutory objectives of the Act importantly include:

1. Provision of an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria.
2. Promotion of cybersecurity and protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.[315]

In term of structure and content, the Act is divided into 8 parts of 59 sections. Part I is on the object and application of the Act. Part II provides for the protection of critical national information infrastructure. Part III of the Act creates certain offences and stipulates penalties. Section 6 provides for the offence of hacking a computer system or network for fraudulent purposes thereby obtaining any data vital to national security. Building on the platform created by the Advance Fee Fraud Act above, section 7 requires all cybercafé operators to register as business concerns both with the Computer Professionals' Registration Council and the Corporate Affairs Commission in order to closely monitor the use to which their computer systems are put. Section 7(2) goes further to specifically outlaw e-frauds committed in cybercafés and imposes up to three years' imprisonment. With respect to banking, sections 9, 11 – 14 criminalizes the interception of electronic transfers and/or emails and all forms of computer related frauds. The crux of

[314] See preamble to the Act, 2015.
[315] See Article 1, Ibid.

cybercrime in relation to the banking sector is encapsulated in section 14 of the Act. Section 14 criminalizes hacking of computer systems by all persons including employees in the public or private sector and staff of any financial institution with the intention to defraud and cause financial harm to other individuals or corporate bodies. Such offence is punishable by up to seven years' imprisonment. The theft of ATMs and other electronic devices is also punishable under this Part. Furthermore, section 22 criminalizes identity theft and impersonation while section 30 makes it an offence to manipulate ATMs or Point of Sale terminals with the intention to defraud. Phishing is punishable under sections 32 and 36 while electronic cards related frauds are made punishable under sections 33 – 35.

Part IV provides for the duties of financial institutions and service providers in the fight against cybercrime. The provisions of sections 37 – 40 which impose these duties can be seen as consumer protection measures. Financial institutions are obliged to verify customer identities prior to the conclusion of any dealings while service providers are mandated to record all traffic data and make same available upon request by any law enforcement agency. Part V provides for the administration and enforcement of the Act. The office of the National Security Adviser is made the coordinating body for all security and enforcement agencies under the Act and is empowered to do all things necessary to enable the effective performance of all enforcement agencies under the Act while establishing and maintaining a National Computer Emergency Response Team (CERT) Coordination Centre and National Computer Forensic Laboratory for the purpose of effectively implementing a comprehensive cyber security strategy. Furthermore, the Attorney General of

the Federation is empowered to enhance the existing legal framework as the need may arise in accordance with technological advancement in order to keep the Act in conformity with international standards. Section 42 establishes the Cybercrime Advisory Council to ensure the promotion of cybersecurity in Nigeria. Section 44 also establishes the National Cybersecurity Fund.

Part VI empowers the authorities to apply *ex parte* for the issuance of a warrant to search suspected premises in order to obtain electronic evidence in related crime investigation. Suspected offenders may also be prosecuted by relevant law enforcement agencies, subject to the powers of the Attorney General. The power to make an *ex parte* application ought to be applied with caution, given the proclivities for the misuse and abuse of *ex parte* applications and orders. This has been a subject of concern in recent times.[316]

Part VII contains jurisdictional provisions and international cooperation. The Federal High Court is imbued with the jurisdiction to try all offences under the Act. Finally, Part VIII contains miscellaneous provisions such as powers of the minister to make regulations in conformity with changing technology and interpretation of specific terms used in the Act.

It is an Act that enjoins Nigerians with the global community on the thorny issue of policing the internet. The challenges manifested in the area of enforcement, compliance, cybercrime investigation, cybersecurity funds, the conflict arising from the National Security Agencies Act which cannot be amended except by the constitution and others. On enforcement, S. 7 of Cybercrimes Act mandates the operators of cybercafes to register as business

[316]*Seplat Petroleum Development v Brittania-U Nig Ltd &Ors* (2014) LPELR-23126 (CA); Agbomago v Okpogo (2005) All FWLR (Pt. 291) 1606; *Omega Bank (Nig) Plc v OBC Ltd* (2005) 8 NWLR (Pt. 928) 547; *Fagbola v Titilayo Plastics Industries Ltd* (2005) 2 NWLR (Pt. 909) 1.

name with Corporate Affairs Commission as well as Computer Professionals Registration Council. Cybercafes shall maintain a register of users through sign-in register, and that the register shall be available to law enforcement personnel whenever needed but made no provision for sanction if the section is violated.

S.36 (12) of the constitution of the Federal Republic of Nigeria 1999 provides that:

> Subject as otherwise provided by this constitution, a person shall not be convicted of criminal offence unless that offence is defined and the penalty therefore is prescribed in a written law, and in this subsection, a written law refers to an Act of the National Assembly or a Law of a state, any subsidiary legislation or instrument under the provision of a law.

It is therefore settled principle of law that any provision of law that do not prescribed punishment for violation is not law because it serve no purpose, the section mere provided a statement with regards to cybercafé owners by prescribing for registration of cybercafés and maintaining a register of users through sign in register but the Act did not provide punitive measure for anyone who failed to complied with this provision. In *Attorney General of the Federation V Isong* [317] the appellant was charged, tried and convicted for the offences under S. 3 & 9 of the firearms Act of 1966. None of the said section prescribes a penalty for the offences. It was held that the conviction was a violation of S.33(12) of the 1979 constitution. Also recently, in *Olieh V Federal Republic of Nigeria*[318] in this case the appellants were tried before the Failed Banks Tribunal in Lagos pursuant to the failed Banks (Recovery of

[317] (1986)1 QLEN 75
[318] (2005) ALL FWLR (pt.281) 1746

Debts) and Financial Malpractices in Banks Decree, 1994. The appellants were found guilty and convicted on three counts of falsely boosting the balance of A.C.B PLC's clearing account with the central Bank of Nigeria contrary to S. 435(2) of the criminal Code and punishable under S. 23(4) of the failed Banks Decree, the appellants appealed against their conviction and sentences contending among other things that it was unconstitutional to convict them for conspiracy to boast and boosting an account when such offence is unknown to Nigerian Law. Relying on the decision in *Aoko Vs Fagbemi* [319] as well as *Federal Republic of Nigeria v Ifegwu*[320] the court held that the conviction and sentences were null and void. The court held inter alia:

> Nobody can be convicted of any offence except that created under a written law and to convict any person under a non-existing offence or an offence unknown to law is unconstitutional, null and void. In the instant case, counts 1,4 & 9 in the charge before the trial failed Banks, Tribunal dealing with falsely boosting on account are unknown to the law and the Tribunal had no jurisdiction to try the appellants and the judgment, conviction and sentence are consequently set aside.[321]

See also, *Asake V Nigerian Army Council*[322] the right to be tried under a known law was held to be applicable also to trial before court martial (Military Tribunals), *Fabiyi JCA.,* who read the lead Judgment of the Court of Appeal held inter alia;

> In strongly, feel that an act that will constitute an offence cannot be left to conjecture at the whims and caprices of the GOC, 2 mechanized Division, Nigerian Army, such is not in tune with the provision of section 33(12) of the 1979 constitution I am afraid S. 71 of the Army Act under which the appellant was arraigned cannot stand…. Therefore, the

[319] (1961)ALL NLR 400
[320] (2003) FWLR (pt.167) 703
[321] Per Omokri JCA Pp. 1768-1769
[322] (2007)ALL FWLR (pt.396) 737

> arraignment, conviction and sentence imposed on the appellants are nullities and must be set aside anon.

The Act in its part IV specifically stipulates the "Duties of Financial Institutions". S. 37 (3) thereof provides; "Any Financial Institution that makes unauthorized debit on a customer's account shall upon written notification by the customer, provide clear legal authorization for such debit to the customer, or reverse such debit within 72 hours. Any financial institution that fails to reverse such debit within 72 hours shall be guilty of an offence and liable on conviction to restitution of the debit and a fine of N5m". How many financial institutions can verge not to have breached this provision? Where then lies the efficacy when s. 19 (3) Cybercrimes Act shifts the burden to the bank customer "to prove the financial institution in question could have done more to safeguard its information integrity".

The Act is in conflict with the constitution of the Federal Republic of Nigeria 1999 as amended in respect of the provision of right to privacy. S. 38 that provides for duties of service providers as records retention and protection of data also was apt when in its subsection (5) reflected the protections of the law: "Anyone exercising any function under this section shall have due regard to the individual's right to privacy under the constitution of the Federal Republic of Nigeria 1999 and shall take appropriate measures to safeguard the confidentiality of the data retained: processed or retrieved for the purpose of law enforcement". One wonders if such assurances can make a bank customer to go home and sleep like a baby. Unless the exercise is transparent enough some fundamental rights of some citizens may be infringed. Some of the rights have been specifically guaranteed by s. 37 of the 1999 constitution even the

advent of terrorism has led to suggestion and bills that tend to whittle down those provisions.

By s. 40 of Cybercrimes Act which provides for failure of service provider to perform certain duties, the various telephone/ GSM network providers are obliged to render assistance to the law enforcement agencies with their duties to track offenders especially when the alleged crimes were committed. It takes the spirit of a patriotic NSA which has proved scarce to comply with these provisions. If not, why has Nigerian GSM network providers not assisted the Federal government in its onslaught against Boko Haram who have been using the mobile phones, videos and internet communications without detection.

The 8th Assembly is keen in considering a proposed "Nigerian Electronic Communications Bill" which failed to sail through the 7th Assembly. One of the provisions, s. 15 (1) criminalizes unsolicited and irritating messages which is common with most communication operators. Indeed a jail term of not less than 1 year or a fine of N2m, as well as a death sentence are imposed. The highest sentence applied to "offenders who commits crimes against the law by penalizing any person who, by means of public electronic communication network, persistently sends a message or other matter that (a) is grossly offensive or causes any such message or matter to be so sent; (in this case telecom operators) or (b) sending electronic messages that are known to be false, and could cause annoyance, inconvenience or needless anxiety to another or cause".

One of the principal objectives of the passage of Cybercrimes (prohibition, prevention etc) Act 2015 is the protection of critical National Information

Infrastructure: but no where in the Act is "National Information Infrastructure" defined. However, s.4 provides for "Audit and inspection of critical National Information Infrastructure" by the office of the National Security Adviser (NSA) through a presidential order made under s.3. Section 3 also failed to define what the "Audit" should include or exclude as the case may be, except providing for "Designation of certain computer systems or networks as critical National Information Infrastructure". Perhaps the advantage is that by designating certain computer systems is like an open cheque which list could be expanded or diminished since the exercise may only be undertaken on the recommendation of the NSA.

Now, let me briefly comment on the common grievances on average banks/financial institutions customers often complain of unauthorized disbursement from their accounts and the question becomes who bears the liability? This is one of the challenges of e-transaction which the Cybercrimes Act should have properly dealt with. Presently, the Act criminalizes a few activities through digital platform but allocation of liability when such thing happen is glaringly absent except that the Act prescribes mitigating effort and burden of proving that the bank had not done enough to protect their customers.

There is need for our National Assembly pass into law of two bills that could address the potential problems which are still before the 8th Assembly. They are: "Payment System Management Bill" and "Electronic Transactions Bill".

10. **Computer Security and Protection Bill, 2009**

This Bill seeks to make provisions for - (a) securing computer and computer networks as well as critic information infrastructure in Nigeria; (b) offences and penalties relating to unlawful acts committee with the use of computers and (c) the establishment of the Nigeria Computer Security and protection Agency to provide legal basis and technical infrastructure for combating cybercrime in Nigeria.

It is structured into 9 parts, 53 sections and a schedule as follows: - Part 1 - establishment of the Nigerian computer security and protection agency and its governing board, etc. Establishment of the Agency, etc.; Establishment and membership of the Governing Board; Tenure of office; Cessation of membership; Allowances, etc. of members. Part 2 - Functions and powers of the agency: Functions of the Agency; Powers of the Agency. Part 3 - Management and staff of the agency: Director-General and other staff of the Agency; Pensions; Staff regulations; Structure and principal officers of the Agency. Part 4- Financial provisions: Fund of the Agency; Expenditure of the Agency; Estimate; Accounts and audits; Annual reports, etc; Power to accept gifts; Power to borrow; Exemption from tax. Part 5- Offences: Unlawful access to a computer, etc; Unauthorised disclosure of access code; Illegal communication using computer etc.; System interference and misuse of devices; Denial of service; Identity theft and impersonation; Records retention by service providers; Failure of service provider to perform certain duties; Cybersquarnnp. Cyber-teITorism' Violation of intellectual property rights with the use of computer, etc.; Using pattern. computer for unlawful sexual purposes etc; of conspiracy and abetment. Part critical information infrastructure; Critical information etc; Audit and inspection of critical

information infrastructure; Offences against critical information infrastructure; Civil liability; Part 7- General provisions: Introduction, etc; Powers of search and arrest; Obstruction; computer evidence; Prosecution. Part 8 - al Proceedings: Limitation of suits against the Agency, etc; Service of documents; restriction on execution against property of the Agency; Indemnity; Part 9 - Miscellaneous: directives by the President, etc; Power to make regulations; Interpretation; Short Title. Schedule- Supplementary Provisions Relating to the Board, etc.

Under section 6, the Agency shall- (a) establish and maintain a system for monitoring and tracking the suspected misuse of any computer for the commission of any crime in Nigeria; (b) gather and compute data on any offence committed or perpetrated through the use of any computer for the purposes of investigation, prosecution and enforcement under this Act and other relevant laws in Nigeria; (c) formulate measures and strategies to prevent the utilization of any computer for the commission of any crime in Nigeria; (d) in collaboration with the relevant bodies and agencies, formulate policies, strategies and action plans for the development sourcing and certification of information technology and other communications for the prevention of the commission of any crime with the use of any computer in Nigeria; (e) in collaboration with the relevant regardless and agencies design measures and develop strategies the protection of sensitive national information and communications infrastructure; (f) formulate strategies and obstacles for securing intergovernmental data exchange and activities; (g) formulate strategies and adopt measures to prevent Crimes that are committed through the use of input printers; (h) assist other law enforcement agencies in

the (i) allegation of crimes committed with the use of computers; Carry out public enlightenment campaigns or public awareness programmes to educate Nigerians on crimes committed in the cyberspace and fraud-related activities on the Internet; collaborate with relevant international agencies and organizations on combating crimes and fraudulent activities carried out with the use of computers; (k) create and maintain a quick response team for computer related emergencies in Nigeria; (I) liaise with the Attorney-General of the Federation for the purpose of initiating proceedings and processes in relation to extradition. deportation and mutual legal assistance matters with respect to offences under this Act; and (m) carry out such other activities as are necessary or expedient to ensure the efficient performance of the functions of the Agency under this Act.[323]

11. Telecommunications Facilities (Lawful Interception of Information) Bill, 2010

This Bill seeks to require telecommunications service providers to put in place and maintain certain capabilities that facilitate the lawful interception of information transmitted by telecommunications and to provide basic information about their subscribers to the Nigeria Police Force and the State Security Service. It is divided into 13 parts, 54 Sections and 2 schedules as follows: - Part 1 General: Purpose of the Act; Application of the Act. Part 2 - Obligations concerning interceptions: Obligation concerning interception; Operational requirements for transmission apparatus; No degradation of capabilities; Maintaining capabilities in respect of new services;

[323] *Ibid*

Beginning to operate transmission apparatus; New software; Time limited compliance for small service provider; Global limit; Order suspending obligations: Ministerial orders; Part 3 - Obligations concerning subscriber information: Provision of subscriber information; Exceptional circumstances; Use of information; Internal audit.; Preservation of existing authority; Obligation to provide information; Obligation to assist in assessment and testing; Notification of change; Notification of simultaneous Interception capability; Persons engaged in interceptions; Mandatory reporting in respect of existing service providers; No redundant performance required; Exemption order by the President. Part 4- Regulations: Regulations. Part 5 – Inspection: Designation of inspectors: Power of inspectors. P, 6 - Administrative monetary penalties: Part 7 Determination of Responsibility and Penalty: Payment of penalty; Making representations; Presumed responsibility. Pan 8 - Appeal to Minister: Right of appeal. Part 9 - Rules about Violations: Liability of employees and agents; Officers of corporate bodies, etc; Due diligence; Continuing violation' Limitation period; Violation or offence; Admissibility of documents. Part 10 - Recovery of Penalties an Amounts: Debts to the Government of the Federation; Certificate, Part 11 - Offences: Misleading statements and information; Offence' Due diligence; Officers of corporate bodies, etc; Continuing offence; Limitation or prescription. Part 12- Injunctions: Injection. Part 13 - Interpretation and Short Title: Interpretation; Short Title and Schedules

1: Exclusions from the Application of the Act; Schedule 2: Partial Application of the Act.

Under section 1, the purpose of this Act is to ensure that telecommunications service providers have the capability to enable national security and law enforcement agencies to exercise their authority to intercept communications, and to require service providers to provide subscriber and other information, without unreasonably impairing the privacy of individuals, the provision of telecommunications services to Nigerians or the competitiveness of the Nigerian telecommunications industry.

Under section 2(1), this Act does not apply to telecommunications service providers in respect of the telecommunications services specified in Part I of Schedule I or to the telecommunications service providers in the classes listed in Pal1 2 of Schedule 1 in respect of the activities specified in it for that class. (2) This Act (other than sections 5, 6, 12, 18 to 20, 22 and 26 to 52) does not apply to the telecommunications service providers in the classes listed in Pan I of Schedule 2 in respect of the activities specified in it that class. (3) This Act, other than section 20, does not apply to the telecommunications fasses listed in Part 2 of Schedule 2 in respect of the activities Certified in it for that class. (4) The President may, on the commendation of the Minister, by order, amend Schedule 1 or Schedule 2. .[324]

12. Cybersecurity Bill, 2011

The Bill seeks to provide measures for national cybcrsecurity and for the prevention, detection, response and prosecution of cybercrimes and other related matters. It is divided into 6 parts and 38 Sections as follows: - Part 1

[324] *Ibid*

General Provisions: Objects and scope. Part 2 - Offences and Penalties: Unlawful access to a computer; Unlawful interception of communications; Unauthorized modification of computer program or data; System interference; Misuse of devices; Computer related forgery; Computer related fraud; Child pornography and related offences; Identity theft and impersonation; Cybersquatting; Cyberterrorism; Racist and xenophobic offences; Records retention and protection of data by service providers;

Interception of electronic communications; Failure of service provider to perform certain duties; Attempt, conspiracy, aiding and abetting; Corporate liability. Part 3 - Protection of Critical Information Infrastructure: Designation of certain computer systems or networks as national critical information infrastructure; Audit and Inspection of critical information infrastructure; Offences against critical information Infrastructure. Part 4 - Search, Arrest and Prosecutions: Jurisdiction to try offences under this Act; Powers of sear and arrest; Obstruction; Prosecution of offences; Order of forfeiture of assets; Order for payment of compensation restitution.; Compounding of offences. Part 5 - International Co-operation: Extradition, Request for mutual assistance' Evidence pursuant to a request; Form of request; Preservation and expedited disclosure of computer data within international cooperation; Designation of contact point for 24/7 Network. Part 6- Miscellaneous: Directives of a general character' Regulations; Interpretation; Short Title.

Under Section 1, objects and scope: (1) The objects and scope of this Act are to - (a) provide an effective legal framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria; and (b)

enhance cybersecunty and the protection of computer systems and networks, electronic communications; data and computer programs in Nigeria; (2) The provisions of this Act shall be enforced by law enforcement agencies in Nigeria to the extent of the agency's statutory powers.[325]

13. Electronic Transactions Bill, 2015

This Bill seeks to provide for the facilitation of electronic commerce in Nigeria. In terms of structure and contents, this Bill has 24 sections covering the following matters: - Objectives of the Act; Application of the Act; Non-discrimination against electronic information; Writing requirements; Prescribed forms; Signature requirements; Requirement to produce an original document; Keeping written documents; Integrity of information; Recognition of foreign electronic documents and signatures; Government uses; Exemptions; Certain other laws not affected; Consent; Contracts; Automated contracts; Mistakes in partly automated contracts; Expression of will; Time and place of sending and receiving electronic information; Attribution of electronic communications; Consumer protection; Regulation; Interpretation; Short Title.

Under section 1, the objects of this Act are: (a) to promote harmonization of legal rules on electronic transactions across national boundaries; (b) to facilitate the appropriate use by electronic transactions; (c) to promote business and communications confidence in electronic transactions; and (e) to enable business community to use electronic communications in their an actions with government transaction Under section 2, the provisions of this Act shall apply transactions both in the private and public sectors. to section 3

[325] Ladan M.T., *Op Cit p.296*

deals with Non-discrimination against (1) As from the commencement of this Act, no Information shall not be denied legal effect, validity or an internet solely on the ground that it is in electronic form.

(2) In sections 4, 5, 6, 7 and 8, where rules of law-(a) require formation to be In writing, given, signed, original, or retained, the requirement is met if the section is complied with; (b) provide consequences. Where the information is not in waiting, given, signed, original, or retained, the consequences are avoided if the section is complied with; and (c) provide consequences if the information is in writing, given, signed, original or retained, the consequences are achieved if the section is complied with.

Section 23 defines the following key terms:- "electronic" includes created, recorded, transmitted or stored in digital or other intangible form by electronic, magnetic, optical or by any other means that has capabilities for creation, recording, transmission or storage similar to those means;

"electronic signature" means information in electronic form that a person has created or adopted in order to sign a document and that is in, attached to or associated with a document."information system" means a system for generating, sending, receiving, storing or otherwise processing electronic communications.

Sections 15 and 16 provide for e-contracts as follows: (1) Unless the parties agree otherwise, an offer, the acceptance of an offer or any other matter that is material to the form. Operation of a contract may be expressed-(a) by means of information in electronic form; or (b) by an act that is ended telecommunication electronics or clicking on an appropriate Icon or other

place on a computer screen, or by speaking. (2) A contract is not invalid or unenforceable by reason only of being in electronic form.

Section 16 states that, a contract may be formed by the interaction of computer programmes or other electronic means used to initiate an act or to respond to electronic information, in whole or in part, without review by an individual at the time of the response or act.[326]

14. Electronic Fraud Prohibition Bill, 2008

This Bill seeks to prohibit all Electronic Fraud in the Federal Republic of Nigeria on unauthorized Access to computer be it public or private, registration of Cybercafe to ensure monitoring of such cybercafes, interception of electronic messages, willful misdirection of E-messages for fraudulent purposes, fraudulent issuance of E-money orders, sending obscene messages, manipulation of computer data, purchase of forged E-cards, falsification of E-data, validity of electronic signatures and its exceptions, diversion of E-mail for personal gains in financial institutions, E-identity theft, E-card fraud, usage of fake E-access devices, manipulation of ATMIPOS terminals, computer damage and for other related matters.

Section 1 of the Bill prohibits electronic fraud as follows: (1) From the commencement of this Act no person or body corporate shall: (a) without authorisation access a computer (or) and other electronic devices or in case of authorisation, exceeds authorised access to computers and or communication devices; (b) use counterfeit access devices; (c) Use unauthorised access devices; (d) possess any device designed to manipulate credit or ATM card; (e) damage a government computer with the intent to defraud; (f) access

[326] *Ibid*

computer and or electronic device to commit espionage: (g) traffic in pass words for public, private and or financial Institutions computer or relevant electronic devices; (h) traffic in any password or similar information, through which computer may be accessed without authorisation with intent defraud, copy financial 15 institutions website, erring customers with intention to defraud customers and financial institutions; and (i) intentionally create computer worms destroy government computer. (2) Anybody who contravenes any of the subsections above shall be guilty of an offence punishable with a sentence of 7 years imprisonment or a fine of 5 million Naira or both.

The bill which has 47 sections further provides for the following matters:- What constitutes unauthorized access; registration of cybercafé; meaning of computer; protected computer; computer manipulation; intercepting electronic messages, emails, electronic money transfers; tampering· with protected computers; willful misdirection of electronic messages; prohibition of obtaining by false pretences any electronic message or data; willful hiding of any electronic message by any government, fraudulent issuance of electronic money orders or e-payments or/and debit orders; fraudulent messages in respect of electronic money transfer instructions; protection of electronic devices against computer hacking and obscence messages; unauthorized sending of money transfer messages; purchasing of forged e-cards; manipulation of e-data; falsification of e-data: validity of e-signatures; and exceptions thereto etc[327]

[327] *Ibid*

In conclusion, the writer is of the considered opinion that crimes, conduct that constitutes cybercrime must be expressly prohibited by legislation. It must also be sanctioned by legislation. Thus, the regulatory framework discussed above are inadequate because they are not comprehensive legal approaches also there is need for an effective policy and regulatory framework to tackle cybercrime and ensure effective internal control mechanisms. More often than not, the effects of cybercrime ripple across several jurisdictions. In this wise, efforts to tackle and sanction cybercrime viewed on international, regional and national perspective must be enhanced.

CHAPTER FOUR

ISSUE AND CHALLENGES IN COMBATING CYBERCRIME

4.1 Introduction

Recent developments in ICTs have not only resulted in new cybercrimes and new criminal methods, but also new methods of investigating cybercrime. Advances in ICTs have greatly expanded the abilities of law-enforcement agencies. Conversely, offenders may use new tools to prevent identification and hamper investigation which poses lot challenges in the cyber realm. This chapter focuses on the law enforcement and other security body's skills, knowledge, techniques for effective investigations in curbing cybercrime, the role of judiciary in the admissibility of electronic evidence in cyber crime cases and the challenges of fighting cybercrime.

4.2 Law Enforcement in Combating Cyber Crime (Skills, Knowledge, Techniques for Effective Investigation)

Law-enforcement agencies can now use the increasing power of computer systems and complex forensic software to speed up investigations and automate search procedures.[328] It can prove difficult to automate investigation processes. While a keyword-based search for illegal content can be carried out easily, the identification of illegal pictures is more problematic. Hash-value based approaches are only successful if pictures have been rated previously,

[328] See: Giordano/Maciag, (2005) Cyber Forensics: *A Military Operations Perspective, International Journal* of Digital Evidence, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04843F3-99E5-632BFF420389C0633B1B. pdf ; Reith, (2005) An Examination of Digital Forensic Models, *International Journal of Digital Evidence*,Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, Vol. 119, page 531
et seq.

the hash value is stored in a database and the picture that was analysed has not been modified.[329]

Forensic software is able to search automatically for child-pornography images by comparing the files on the hard disk of suspects with information about known images. For example, in late 2007, authorities found a number of pictures of the sexual abuse of children. In order to prevent identification of offender had digitally modified the part of the pictures showing his face before publishing the pictures over the Internet. Computer forensic experts were able to unpick the modifications and reconstruct the suspect's face.[330] Although the successful investigation clearly demonstrates the potential of computer forensics, this case is no proof of a breakthrough in child-pornography investigation. If the offender had simply covered his face with a white spot, identification would have been impossible.

i. Use of ICTs and the need for new investigative instruments

Offenders use ICTs in various ways in the preparation and execution of their offences.[331] Law enforcement agencies need adequate instruments to investigate potential criminal acts. Some instruments (such as data retention) could interfere with the rights of innocent Internet users.[332] If the severity of the criminal offence is out of proportion with the intensity of interference, the

[329] see: Kerr, (2005) Searches and Seizures in a digital world, Harvard Law Review, Vol. 119, p 546 *et seq.*; Howard, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, *Berkeley Technology Law Journal*, Vol. 19, page 1233.

[330] For more information about the case, see: Interpol in Appeal to find Paedophile Suspect, The New York Times, 09.10.2007, available at: www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin; as well as the information provided on the Interpol website, available at: www.interpol.int/Public/THB/vico/Default.asp

[331] Regarding the use of ICTs by terrorist groups, see: Conway, (2006) Terrorist Use of the Internet and Fighting Back, *Information and Security*, page 16; Hutchinson, (2006) "Information terrorism: networked influence" available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/iwar/Hutchinson%20-%20Information%20terrorism_%20networked%20influence.pdf; *Gercke*, Cyberterrorism, *Computer Law Review International* 2007, p 64.

[332] Relating to these concerns, see: Advocate General Opinion, 18.07.2007, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top.

use of investigative instruments could be unjustified or unlawful. As a result, some instruments that could improve investigation have not yet been introduced in a number of countries.

The introduction of investigative instruments is always the result of a trade-off between the advantages for law-enforcement agencies and interference with the rights of innocent Internet users. It is essential to monitor ongoing criminal activities to evaluate whether threat levels change. Often, the introduction of new instruments has been justified on the basis of the "fight against terrorism", but this is more of a far reaching motivation, rather than a specific justification *per se*.

ii. Failure of Traditional Investigation Instruments

Investigating and prosecuting cybercrime requires Internet-specific tools and instruments that enable competent authorities to carry out investigations.[333] In this context, instruments to identify the offender and collect the evidence required for the criminal proceedings are essential.[334] These instruments may be the same as those used in traditional terrorist investigations unrelated to computer technology. But in a growing number of Internet-related cases, traditional investigation instruments are not sufficient to identify an offender. One example is the interception of voice-over-IP (VoIP) communication.[335] In

[333] This was also highlighted by the drafters of the Council of Europe Convention on Cybercrime, which contains a set of essential investigation instruments. The drafters of the report point out: "Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques", see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 132.

[334] see: Goerling (2006), The Myth Of User Education, at www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. They mustall understand what they can and can't do on the Internet and be warned of the potential dangers. As use of theInternet grows, we'll naturally have to step up our efforts in this respect."

[335] The term "voice over Internet protocol" (VoIP) is use to describe the transmission technology for delivering voice communication using packet-switched networks and related protocols. For more information, see: Swale,(2001) Voice Over IP: Systems and Solutions, *Black*, Voice Over IP, 2001.

recent decades, states have developed investigation instruments, such as wiretapping, that enable them to intercept landline as well as mobile-phone communications.[336] The interception of traditional voice calls is usually carried out through telecom providers.[337] Applying the same principle to VoIP, law-enforcement agencies would operate through Internet service providers (ISPs) and service providers supplying VoIP services. However, if the service is based on peer-to-peer technology, service providers may generally be unable to intercept communications, as the relevant data is transferred directly between the communicating partners.[338] Therefore, new technical solutions together with related legal instruments are necessary.

iii. Encryption Technology

Another factor that can complicate the investigation of cybercrime is encryption technology, which protects information from access by unauthorized people and is a key technical solution in the fight against cybercrime[339]. Encryption is a technique of turning a plain text into an obscured format by using an algorithm.[340] Like anonymity, encryption is not

[336] see: Karpagavinayagam/State/Festor, (2007) Monitoring Architecture for Lawful Interception in VoIP Networks, *in Second International Conference on Internet Monitoring and Protection* – ICIMP 2007. Regarding the challenges related to interception of data communication, see*:* Swale/Chochliouros/Spiliopoulou/Chochliouros,(2007) Measures for Ensuring Data Protection and Citizen Privacy Against theThreat of Crime and Terrorism – The European Response, in *Janczewski/Colarik*, Cyber Warfare and Cyber Terrorism,, page 424.

[337] Regarding the differences between PSTN and VoIP communication, see: Seedorf, (2008) Lawful Interception in P2P-Based VoIP Systems, in *Schulzrinne/State/Niccolini*, Principles, Systems and Applications of IP Telecommunication. Services and
Security for Next Generation Networks, page 217 *et seq.*

[338] see Bellovin and others, (2006) Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP; *Simon/Slay*, Voice over IP: Forensic Computing Implications, *Seedorf*, (2008) Lawful Interception in P2P-Based VoIP Systems, in *Schulzrinne/State/Niccolini*, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, p.217 *et seq*.

[339] See *Huebner/Bem/Bem*, Computer Forensics – Past, Present and Future, No.6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding the mathematical background, see: *Menezes*, Handbook of Applied Cryptography, 1996, page 49 *et seq*

[340] *Lowman*, (2010) The Effect of File and Disk Encryption on Computer Forensics, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Fore
nsics.pdf.

new, but computer technology has transformed the field.[341] For a long time it was subject to secrecy. In an interconnected environment, such secrecy is difficult to maintain.[342]

The widespread availability of easy-to-use software tools and the integration of encryption technology in the operating systems now make it possible to encrypt computer data with the click of a mouse and thereby increases the chance of law-enforcement agencies being confronted with encrypted material.[343] Various software products are available that enable users to protect files against unauthorized access.[344] But it is uncertain to what extent offenders already use encryption technology to mask their activities.[345] One survey on child pornography suggested that only 6 per cent of arrested child-pornography possessors used encryption technology[346], but experts highlight the threat of an increasing use of encryption technology in cybercrime cases.[347]

---

[341] Singh; (2006) The Code Book*: The Science of Secrecy from Ancient Egypt to Quantum* Cryptography; *D'Agapeyen*, Codes
and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology, available at: www.csecst.
gc.ca/documents/about-cse/museum.pdf.

[342] Kahn, (1979) *Cryptology goes Public, Foreign Affairs*, Vol. 58, p143.

[343] *Lowman, Op Cit*

[344] Examples include the software Pretty Good Privacy (see www.pgp.com) or True Crypt (see www.truecrypt.org).

[345] see: Zanini/Edwards, The Networking of Terror in the Information Age, in Arquilla/Ronfeldt, Networks and Netwars: The Future of Terror, Crime, and Militancy, p37, available at: http://192.5.14.110/pubs/monograph_reports/MR1382/MR1382.ch2.pdf. Flamm, Cyber Terrorism and Information Warfare: Academic Perspectives: Cryptography, available at: www.terrorismcentral.com/Library/Teasers/Flamm.html;
Casey Practical Approaches to Recovering Encrypted Digital Evidence, *International Journal of Digital Evidence,* Vol. 1,
Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

[346] See: Wolak/ Finkelhor/ Mitchell,(2005) Child-Pornography Possessors Arrested in Internet-Related Crimes: *Findings From the National Juvenile Online Victimization Study*, p9, available at www.missingkids.com/en_US/publications/NC144.pdf.

[347] Denning/Baugh, (1997) Encryption and Evolving Technologies as Tolls of Organised Crime and Terrorism, available at:
www.cs.georgetown.edu/~denning/crypto/oc-rpt.txt.

Depending on encryption technique and key size, this process could take decades.[348] For example, if an offender uses encryption software with a 20-bit encryption, the size of the key space is around one million. Using a current computer processing one million operations per second, the encryption could be broken in less than one second. However, if offenders use a 40-bit encryption, it could take up to two weeks to break the encryption. In 2002, the Wall Street Journal was for example able to successfully decrypt files found on an Al Qaeda computer that were encrypted with 40-bit encryption.[349]Using a 56-bit encryption, a single computer would take up to 2 285 years to break the encryption. If offenders use a 128-bit encryption, a billion computer systems operating solely on the encryption could take thousands of billions years to break it. The latest version of the popular encryption software PGP permits 1 024-bit encryption. Current encryption software goes far beyond the encryption of single files. The latest version of Microsoft's operating systems, for example, allows the encryption of an entire hard disk.[350] Users can easily install encryption software. Although some computer forensic experts believe that this function does not threaten them,[351] the widespread availability of this technology for any user could result in greater use of encryption. Tools are also available to encrypt communications – for example, e-mails and Phone

[348] Schneier, Applied Cryptography, p185; Bellare/Rogaway, (2005) Introduction to Modern Cryptography, p36, available at: www.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf.
[349] Usborne, Has an old computer revealed that Reid toured world searching out new targets for al-Qaida?, The Independent, January, 18,.2002, available at: www.independent.co.uk/news/world/americas/has-an-old-computer-revealedthat-
reid-toured-world-searching-out-new-targets-for-alqaida-663609.html; *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at:
http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Fore
nsics.pdf
[350] This technology is called BitLocker. For more information, see: "Windows Vista Security and Data Protection Improvements", 2005, available at: http://technet.microsoft.com/en-us/windowsvista/aa905073.aspx.
[351] See Leyden, Vista encryption 'no threat' to computer forensics, The Register, 02.02.2007, available at: www.theregister.co.uk/2007/02/02/computer_forensics_vista/.

calls – that can be sent using VoIP.[352] Using encrypted VoIP technology, offenders can protect voice conversations from interception.[353]

Techniques can also be combined. Using software tools, offenders can encrypt messages and exchange them in pictures or images – this technology is called steganography.[354] For investigative authorities, it is difficult to distinguish the harmless exchange of holiday pictures and the exchange of pictures with encrypted hidden messages.[355] The availability and use of encryption technologies by criminals is a challenge for law-enforcement agencies. Various legal approaches to address the problem are currently under discussion,[356] including: potential obligations for software developers to install a back-door for law-enforcement agencies; limitations on key strength; and obligations to disclose keys, in the case of criminal investigations.[357] But encryption technology is not only used by offenders – there are various ways such technology is used for legal purposes. Without adequate access to

[352] see: Simon/Slay, (2006) Voice over IP: Forensic Computing Implications, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.
[353] *Ibid.*
[354] For further information, see: Provos/Honeyman, Hide and Seek: *An Introduction to Steganography*, available at: http://niels.xtdnet.nl/papers/practical.pdf; Kharrazi/Sencar/Memon, Image Steganography: Concepts and Practice, available at: http://isis.poly.edu/~steganography/pubs/ims04.pdf; *Labs*, Developments in Steganography, available at: http://web.media.mit.edu/~jrs/jrs_hiding99.pdf; *Anderson/Petitcolas*, On The Limits of Steganography, available at: www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf; *Curran/Bailey*, An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence, Vol. 2, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0AD276C-EACF-6F38-E32EFA1ADF1E36CC.pdf.
[355] see: Jackson/Grunsch/Claypoole/Lamont, Blind Steganography Detection Using a Computational Immune: *A Work in Progress*, *International Journal of Digital Evidence*, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04D31C4-A8D2-ADFD-E80423612B6AF885.pdf; Farid, Detecting Steganographic Messages in Digital Images, Technical Report TR2001-412, 2001; Friedrich/Goljan, Practical Steganalysis of Digital Images, Proceedings of SPIE Photonic West 2002: Electronic Imaging, Security and Watermarking of Multimedia Content IV, 4675, p 1 *et seq.*; Johnson/Duric/Jajodia, (2001) Information Hiding: Steganography and Watermarking, Attacks and Countermeasures.
[356] *Ibid*
[357] *Ibid*

encryption technology, it may be difficult to protect sensitive information. Given the growing number of attacks, self-protection is an important element of cyber security.[358]

iv. Investigation Coordination and Consistency problems

Even where cooperation between nations can be achieved, significant roadblocks stand in the way of effective international cybercrime investigations. The mechanisms available to facilitate investigations are often inefficient and lack oversight as to the process by which cybercriminals are pursued. An example of one such mechanism is the use of Mutual Legal Assistance Treaties, commonly known as MLATs. Under an MLAT, prosecutors in one country may request assistance from their counterparts in a foreign country in order to perform tasks including the investigation of suspects and the collection of evidence.[359] Once provided by the foreign counterpart, the collected evidence may be used in a prosecution in the requesting attorney's country.[360] While simple in concept, the MLAT process is often difficult and time-consuming to accomplish. As an example, for an attorney from the United States to seek subpoena information, execute a search warrant, or gain compliance with a court order under an MLAT, the attorney must provide a specific request (which must be approved by the foreign nation's courts) identifying, among other information, the requesting agency, a description of the subject matter and nature of the investigation (including the specific criminal offenses suspected to have been committed),

[358] *Ibid*
[359] Funk, T. Marcus.(2014) "Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges," *Federal Judicial Center*, p. 2-3.
[360] *Ibid*

and a description of the evidence, information, or other assistance sought.[361] The detailed nature of this request and the requirement for international approval can often complicate and impede efforts at information gathering. This can be particularly true early in an investigation, when the theories driving a prosecution effort may still be in the process of development.

Despite these challenges, the MLAT process remains preferable to the use of "letters rogatory," the predominant alternative method for gathering information across international borders. Under an MLAT, a request for information is made based upon a binding treaty guaranteeing cooperation between the contracting nations; in comparison, a letter rogatory is merely an informal request that relies on the goodwill of foreign courts and law enforcement officials to be properly executed.[362]

While it is widely accepted that the formal MLAT procedures will require reform to be effective against cybercrime, the Game over Zeus case provides a fantastic example of how informal international cooperation can and will help provide effective prosecutorial outcomes. In an area where technology consistently outpaces the laws that govern it, such collaborative action will likely be needed to ensure governments keep pace with cybercriminals going forward.[363]

v. Difficulties with Identification and Disclosure of Traffic Data

[361] *Ibid* p. 7
[362] Pengelley, Pamela. "A Compelling Situation: Enforcing American Letters Rogatory In Ontario," *La Revue Du Barreau Canadien*, Vol. 85, p. 346.
[363] "U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator," *U.S. Department of Justice*, June 2, 2014.

Separate from inter-country inefficiencies, nearly all cybercrime investigations encounter a common impediment – the anonymity of the internet, and the ability of criminals to cover their tracks. Since 1998, the International Corporation for Assigned Names and Numbers, or ICANN, has been responsible for, among other tasks, "coordinating the allocation and assignment of three unique identifies for the internet" – domain names, IP addresses, and protocol port and parameter numbers.[364] In plain English, this means that ICANN directly or indirectly oversees how and where individuals and their computers are identified on the Internet. Under current standards, ICANN effectively allows anonymous registration of domains, and does not appear to independently verify contact information provided to it by third-party registrar companies.[365]

Minor changes to the operation of ICANN could provide significant barriers to the use of computer networks for criminal purposes. For example, if ICANN were to require the submission and verification of a government-issued identification in order to register a domain name, the pool of individuals who submit false information would almost certainly shrink. As ICANN's registration requirements evolve over time, the organization will have no choice but to weigh privacy concerns against the need for effective tracing of criminal actions online.

Apart from ICANN's registration requirements, much other inefficiency exist in pursuing the identities of cybercriminals. International cybercrime cases

[364] "Bylaws for Internet Corporation for Assigned Names and Numbers," *ICANN*, July 30, 2014.
[365] "Registrar Accreditation Agreement," *ICANN*, May 21, 2009; *see also* "Verifying Contact Information for ICANN Validation," *GoDaddy, Inc.*, undated (verifying only that a user has provided GoDaddy with an "active and accurate" e-mail account in order to confirm ICANN validation).

often involve tracing a hack through multiple IP addresses around the world, which can, in turn, mean digging through multiple layers of anonymity. Because speed is key to keep online "trails" from growing cold, some intergovernmental organizations have recognized a special need for expedited disclosure of cyberspace traffic data across international lines. One such effort in this area has been spearheaded by the Council of Europe, who requires (with few exceptions) that where a "tracing" request is made between Council member-states, "a sufficient amount of traffic data" must be "expeditiously disclose[d]" in order "to identify the service provider and the path through which the communication was transmitted.[366]" Ultimately, if the global community is able to meet the unique challenges presented by cybercrime, it will do so because sovereign nations band together, combine their resources, and recognize that cybercriminals rarely restrict themselves to the borders of a single nation. By embracing a policy of openness, and by placing an emphasis on efficient and effective collaboration, the world be best able to beat back the ever-growing and increasingly sophisticated plague of hackers lurking online.

vi. Organizational Structures

An effective fight against cybercrime requires highly developed organizational structures. Without having the right structures in place, it will hardly be possible to carry out complex investigations that require the assistance of different legal as well as technical experts. When dealing with cybercrime the competent investigation authorities, as well as courts, need to deal with

[366] "Convention on Cybercrime," *Council of Europe*, Budapest, 23.XI.2001, Article 30.

electronic evidence. Dealing with such evidence presents a number of challenges[367] but also opens up new possibilities for investigation and for the work of forensic experts and courts.[368] In those cases where no other sources of evidence are available, the ability to successfully identify and prosecute an offender may depend upon the correct collection and evaluation of electronic evidence.[369] This influences the way law-enforcement agencies and courts deal with such evidence.[370] While traditional documents are introduced by handing out the original document in court, digital evidence in some cases requires specific procedures that do not allow conversion into traditional evidence, e.g. by presenting a printout of files and other discovered data.[371] Having legislation in place that deals with the admissibility of evidence is therefore seen as vital in the fight against cybercrime.

In a nutshell, the writer, postulate that the Law-enforcement agencies can now use the increasing power of computer systems and complex forensic software to speed up investigations and automate search procedures.[372] It can prove difficult to automate investigation processes. While a keyword-based search for illegal content can be carried out easily, the identification of illegal

[367] Casey, (2004) Digital Evidence and Computer Crime, p 9.
[368] Vaciago, Digital Evidence, 2012.
[369] Regarding the need for formalization of computer forensics, see: Leigland/Krings,(2004) A Formalization of Digital Forensics, *International Journal of Digital Evidence*, Vol.3, No.2.
[370] Regarding the difficulties of dealing with digital evidence on the basis of traditional procedures and doctrines, see:
Moore, (2004) To View or not to view: Examining the Plain View Doctrine and Digital Evidence, *American Journal of Criminal*
Justice, Vol. 29, No. 1, p 57 *et seq.*
[371] See Vacca, (2005) *Computer Forensics, Computer Crime Scene Investigation,* 2nd Edition, p 3. Regarding the early
discussion about the use of printouts, see: Robinson, (1970) The Admissibility of Computer Printouts under the Business
Records Exception in Texas, *South Texas Law Journal*, Vol. 12, p 291 *et seq.*
[372] See: Giordano/Maciag, Cyber Forensics: A Military Operations Perspective, International Journal of Digital Evidence,
Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04843F3-99E5-632BFF420389C0633B1B.
pdf ; Reith, An Examination of Digital Forensic Models, *International Journal of Digital Evidence,*
Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf; Kerr, (2005) Searches and Seizures in a digital world, *Harvard Law Review*, Vol. 119, page 531*et seq.*

pictures is more problematic. Hash-value based approaches are only successful if pictures have been rated previously, the hash value is stored in a database and the picture that was analysed has not been modified[373]. Perform investigations for combating cybercrime; collect and analyse data and information; carry out technical activities for researching computer systems; draft internal rules and procedures for cybercrime investigation; - assist other departments in performing investigations; perform activities for international judicial assistance for criminal issues, within national and international mutual assistance; conduct public awareness cybercrime prevention activities. Research, conduct quality research activities into cybercrime trends both domestically and internationally to inform the future requirements for countering cybercrime; work with academic and industry partners to develop tools and techniques to assist in the efforts to combat cybercrime. Intelligence gathering, perform activities for international co-operation and information exchange with other similar bodies from abroad; perform analyses, studies, and evaluation of the criminal phenomenon; gathering both open source and covert Internet intelligence. Training, establish a professional training programme for digital forensic specialist and cybercrime investigators to ensure that the correct level of knowledge and skills are available.[374]

[373] Kerr, *Op Cit* p546; Howard, Don't Cache out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, *Berkeley Technology Law Journal*, Vol. 19, p1233.
[374] Nigel Jones (United Kingdom) and Virgil Spiridon (Romania) (2009) Council of Europe/EU joint Project on Cybercrime in Georgia: *Proposals for the establishment of a High Tech Crime Unit. Criminal money flows on the Internet* paper presented in March 2011.

4.3 The Role of Judiciary in the Admissibility of Electronic Evidence in Cyber Crime Cases

By the provision of the Cybercrime Act[375] it confirm jurisdiction on the Federal High Court.

The Act provides thus;

10) The Federal High Court located in any part of Nigeria regardless of the location where the offence is committed shall have jurisdiction to try offences under this Act, if committed –

(a) In Nigeria; or

(b) In a ship or aircraft registered in Nigeria; or

(c) By citizen or resident in Nigeria if the person's conduct would also constitute an offence under a law of the country where the offences was committed; or

(d) Outside Nigeria, where –

3. The victim of the offence is a citizen or resident of Nigeria; or

4. The alleged offender is in Nigeria and not extradited to any other country for prosecution.

Electronically generated evidence how applicable in our court system, especially due to the low costs[376] compared to the storage of physical documents, the number of digital documents is increasing.[377] Digitization and the emerging use of ICTs have a great impact on procedures related to the collection of evidence and its use in court.[378] As a consequence of this development, digital evidence has been introduced as a new source of

[375] Section 50 of Cybercrime Act

[376] Giordano,(2006) Electronic Evidence and the Law, *Information Systems Frontiers*, Vol. 6, No.2, p161; Willinger/Wilson, (2004) Negotiating the Minefields of Electronic Discovery, *Richmond Journal of Law & Technology*, Vol. X, No. 5.

[377] Lange/Nimsger,(2004) Electronic Evidence and Discovery,p.6.

[378] Casey, *Op cit* p 11; Lange/Nimsger, (2004) Electronic Evidence and Discovery, p.1; Hosmer, (2002 Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, Vol.1, No.1, p 1

evidence.[379] It is defined as any data stored or transmitted using computer technology that supports the theory of how an offence occurred.[380] Handling digital evidence is accompanied with unique challenges and requires specific procedures.[381] One of the most difficult aspects is to maintain the integrity of the digital evidence.[382] Digital data are highly fragile and can easily be deleted or modified[383]. This is especially relevant for information stored in the system memory RAM that is automatically deleted when the system is shut down[384] and therefore requires special preservation techniques In addition, new developments can have great impact on dealing with digital evidence. An example is cloud computing. In the past, investigators were able to focus on the suspects' premises when searching for computer data. Today, they need to take into consideration that digital information might be stored abroad and can only be accessed remotely, if necessary.[385] Digital evidence plays an important role in various phases of cybercrime investigations. It is in general possible to separate four phases.[386] The first phase is identification of the relevant evidence. It is followed by collection and preservation of the evidence.[387] The third phase includes the analysis of computer technology and digital evidence. Finally, the evidence needs to be presented in court. In addition to the procedures that relate to the presentation of digital evidence in court, the ways

[379] Lange/Nimsger *Op Cit p.1*
[380]Casey, *Op cit* p12, see also: The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm.
[381] Moore, Op cit p.59
[382] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1,
page 1.
[383] *Moore, Op cit* p.58
[384] Nolan/O'Sullivan/Branson/Waits, (2005) *First Responders Guide to Computer Forensics,* p 88.
[385] Casey, Op cit p.20
[386] see: Ciardhuain, (2004) An Extended Model of Cybercrime Investigation, *International Journal of Digital Evidence,* Vol. 3, No. 1. See also: Ruibin/Gaertner, (2005) Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, *International Journal of Digital Evidence*, Vol. 4, No. 1, who differentiate between six different phases.
[387] See: Nolan/O'Sullivan/Branson/*Waits, Op cit* p 88.

in which digital evidence is collected requires special attention. The collection of digital evidence is linked to computer forensics.

The impact of ICT on the Law of Evidence in Nigeria is reflected in the following improved provisions of the new Evidence Act, 2011, which repealed the old Evidence Act[388].

First, expectedly, certain definitions under the Act have been modified to reflect the prevailing attitude of the Act to issues such as documents and admissibility of electronically generated evidence, amongst others. Perhaps, the most significant modification is the new definition of a 'document'. The broadness of this definition can conveniently accommodate all known forms of storage or record of information. The inadequacy of the repealed Act in this regard is highlighted in the case of *Udoro v. Governor, Akwa-Ibom State*[389] where a video cassette was rejected in evidence since it was clearly not envisaged under section 2(1) of the repealed Act.

However, the unbridled broadness of what constitutes a document may constitute serious problems for practitioners in the application of the Act. This is because the definition of a document does not only accommodate information in all forms of devices; it also accommodates the device itself as a form of document. For instance, information stored in a flash drive can tightly be described as a document under paragraph (a) of the definition of "document". Under paragraph (d) of the same definition, the flash drive itself also constitutes a document under the Act. The implication of this interesting provision is that "documents" such as flash drives, tapes or sound track can also be classified as private and public documents under sections 102 and 103 of the Act. Where such documents fall within the purview of public

[388] Cap. E. 14, Laws of the Federation of Nigeria, 2004.

[389] (2010)11 NWLR (pt. 1205)322

documents, the law requires that only a certified true copy of same can be admissible in evidence. Section 104 of the Act explains what is meant by a certified true copy of a document. The pungent question that arises here is "how does a public officer in custody of a flash drive or a sound track certify a copy of such device as a certified true copy in compliance with the modalities stipulated in section 104?" we can ask a further question, "where is the 'foot' of a copy of such a document where at the law requires the public custodian to write a certification thereof?" Without doubt, the answer (if any) to the above questions will border on the ridiculous and lead to further questions. There is a need to harmonies and reconcile this expanded definition of document with other aspects of the Act in order to eliminate such amusing confusion. A possible solution would be to reconsider the definition of a document. The legislature, in the course of trying to solve one problem, may have unwittingly created another. It may be helpful if the Act is amended to create a distinction between 'devices' and 'documents' as forms of evidence. Different considerations should apply to both forms in the application of the Act. For Instance, while 'public documents' may require certification as a pre-requisite for admissibility, some other form of authentication should be created for 'public devices'. This is the fact that section 104 of the Act is clearly designed or 'documents' and does not in any way envisage 'devices'.

Another crucial issue, which comes to mind, is on the rigidity of the provisions dealing with the requirement for certification of public documents. There is a need to qualify the requirement of certification in certain cases. The blanket requirement of certification for all documents (and devices) emanating from public authorities is bound to occasion hardship and injustice. Those

provisions have to be re-visited and appropriately qualified. Unfortunately, the understanding of what constitutes a 'banker's book' remains unchanged under the Act. One would have thought the legislators would heed the clarion call handed by our appellate Court in the cases of *Yesufu vs. ACB*[390] and *UBA V. SAFPU & 3 ors*[391] on the need to amend the Evidence Act definition of 'banker's book' to reflect the bankers' daily use of the computer in the ordinary course of business.

In this regard, the definition of the 'banker's book' in section 2 of The Corrupt Practices and other Related Offences Act 2000[392] is highly desirable in this era of modernizing our law of evidence. That provision defines the term to include inter alia "all other books and documents or electronic devices used in the ordinary course of business of a bank". Admittedly, computer-generated statements of account can be admissible under section 84 of the Evidence Act subject to substantial compliance with the conditions stipulated there under. There is however a need to amend this definition of banker's books to reflect the prevailing tenor of the Act.

The Act attempts a definition of a computer as any device for storing and processing information. It is however unclear why the legislature decided to explain what it means for information to be derived from other information under the definition of a computer. It is sufficient to state that two different concepts are defined under this head and it is important not to confuse the definition of both concepts. We hope that this unnecessary ambiguity would be cured in subsequent amendments of the Act.

[390] (1976)4 SC 1
[391] (2004)3 NWLR (pt. 861) 516 at 541-543; Cf, Decision of the Court of Appeal in FRN v Fani-Kayode
[392] Cap C31 LFN 2004.

Second, the provisions of Section 51 and 52 of the Act proved on the repealed Act sections 38 and 39 by organizing the admissibility of electronic records regularly kept in the ordinary course of business. This is obviously in cognizance of remarkable decisions to the effect that the old vision of section 38 must be construed to include entries kept by electronic process such as a computer.[393]" It must however be pointed out that the electronic records referred to in section 51 can only be restricted to electronic records of accounts and not just electronic records of any fact.

It is also important to observe that section 52 does not solely refer to public officers. By making reference to records by 'any other person in the performance of a duty specially enjoined by the law of the country', the provision can be extended to include records kept by private persons pursuant to statutory obligations to keep such records. For instance, private and public companies incorporated under the Companies and Allied Matters Act are obliged to keep certain records under the Companies and Allied Matters Act.

Third, section 84 of the 2011 Act provides for admissibility of statements in documents produced by computers. Prior to the enactment of the Act, the CS have resorted to all forms of judicial ingenuity to admit computer-generated evidence even in the face of inadequate or non-existent statutory framework. For example, in the case of *Anyaebosi v. R. T. Briscoe Nig. Ltd*[394] the Supreme Court, *per Karibi-Whyte JSC*, upheld the admissibility of a computerized statement of account relying on section 97(l)(d)&(g) and 97(2) of the repeated

[393] See; Trade Bank Plc v. Chami (2003)13 NWLR (pt. 836)158@ 216-217 ESSO WA Inc v. Oyegbola (1969) NMLR 194.
[394] (2000) 2 NWLR (pt 165) p56

Act.[395] Those provisions permit the admissibility of secondary evidence when the original is of such a nature as not to be easily movable or where the original consist of numerous accounts or other documents which cannot conveniently be examined in Court. One area where the issue of computer-generated evidence has generated great controversy is the admissibility of computer-generated statement of account. The Court of Appeal was faced with this issue in the case of *FRN v. Fani-Kayode*'[396] where the appellant appealed against the trial Court's rejection of a computer-generated statement of account in evidence. In allowing the appeal, the Court observed that there is nothing in the Act to suggest that a computerized statement of account is excluded under the definition of the terms 'document' and 'Bankers' books'. In the illuminating contributory judgment of *Saulawa JCA*, reliance was placed on the old Supreme Court case of *Esso WA Inc. v. Oyegbola*[397] when his Lordship observed thus- Undoubtedly, the provisions of the Evidence Act, and indeed most of the Nigerian statutes, including the Grundnorm itself, the Constitution of the Federal Republic of Nigeria, 1999, need to be generally overhauled to meet the exigencies of the modern computer age ... The law cannot be and is not ignorant of modern business methods and must not shut its eyes to the mysteries of the computer."[398]

Therefore, it is our view that, this section is arguably the most innovative provision of this Act since it settles an issue which had been the main reason for collective calls for the amendment of the Evidence Act. Apart from guaranteeing the admissibility of computer-generated evidence, this provision

[395] Cf, Sections 89(d)&(g) and 90(1)(a)&(d) of the repealed Act.
[396] (2010)14 NWLR (pt. 1214)481, see also Oghoyone v. Oghoyone (2010)3 NWLR (pt. 1182)564 at 585.
[397] (1969) NMLR 194
[398] See; the dictum of Saulawa JCA at 506-507

also contains cumulative conditions for the admissibility of such evidence. In view of the fact that there is no corresponding provision in the repealed Act, let us briefly examine each of these conditions-

8. **Document must emanate from computer during a period when the computer was used regularly to store or process information for the purposes of any activities regularly carried all over that period**

This first condition to be satisfied for the admissibility of computer-generated evidence can be broken down as follows-

i. The regular use of the computer for information processing or storage over a given period must be established;

ii. The information processed or stored by the computer must be for the purpose of any activities regularly carried on over that given period by anybody;

iii. The document must have been produced by the computer during the same period in which the computer was regularly used for storage or processing of information.

Indeed, several problems of admissibility are bound to arise from this condition. The Act requires some sort of consistent use of the computer for specific purposes as a prerequisite for the admissibility of documents produced by such computer. This means a computer that is regularly used to store or process minutes of meetings cannot produce a statement of account that will be admissible under this section.

Another germane issue under this provision is the question of time of production. At what point is a document said to be produced by a computer? The tenor of the Act Suggests that 'production' of a document is synonymous with 'minting' of the document. This interpretation will definitely lead to further confusion. It is submitted that the word 'produced' should be construed to include documents stored or processed on the computer during that period whether or not they were printed out. Fortunately, the decision of the Court of Appeal in *Trade Bank Plc v. Chami*[399] is relevant to this issue. In that case, the Court held inter alia that a document which had been fed into a computer prior to the commencement of suit but printed out during the pendency of the suit does not fall within 'documents made during the pendency of a suit'. This means the Court considered the time of production of the document to be the time when same was fed into the computer and not when it was printed out. This approach, it is submitted, represents the desired construction of the word 'produced' in this provision.

9. **There must have been a regular supply of similar information in the ordinary course.**

The information derived from a computer which can be admissible under this section must not be of an isolated nature. There must have been a regular supply of similar or related information to the computer in the ordinary course over the period under review. Our concerns raised above are also pertinent here as this condition may operate to unduly restrict the nature of evidence that may be admissible under this provision.

[399] (2003)13 NWLR (pt. 836) 158 at 213 -216

10. **The computer must have been operating properly or operating ill such a way that the production and accuracy of the document will not be affected**

The party seeking to tender such evidence must show that the computer was properly functioning at all times material to the time of production of the document. It would appear that once there is a prima facie reason to believe that the computer was properly functioning, the patty against whom such evidence is sought to be tendered bears the onus of showing that the generating-computer was malfunctioning in such a way that the accuracy or production of the document cannot be trusted.

In *King v. State ex. Rei Murdock Acceptance Corp,*[400] the Court set the following guidelines in ensuring reliability of information obtained from computers namely:

k. That the electronic computing equipment is recognized as standard equipment.

l. The entries were made in the regular course of business at or reasonably near the time of the happening of the event recorded.

m. The foundation testimony satisfied the trial Court that the sources of information, method and time of preparation were such as to indicate its trustworthiness and justify its admission[401]

11. The information contained in the document is derived or reproduced from information supplied to the computer ill the ordinary course of those activities

[400] See Afe Babalola, Law and Practice of Evidence in Nigeria, p. 262
[401] Cf. Section 34(1)(b) of the Act.

The essential factor here is that the information must have been supplied to the computer in the ordinary course of the activities. In addition to the foregoing, it is important to also consider the provisions of subsection (5) of the section in order to ascertain the extent of its application.

i. **Information supplied in any appropriate form (section 84(5)a)**

Here, the law recognizes information supplied to the computer either directly or by means of any appropriate equipment. The phrase 'with or without human intervention' tends to suggest that it is intended to accommodate information supplied to a computer by means of the internet (e.g. internet downloads) or emails. In other words, the law is not restricted to documents which are directly supplied into the computer; it also includes documents which may be obtained 'through' the computer.

ii. **Information supplied to a different computer for the purpose of a collective activity (section 84(5)b)**

In our audit report scenario above, assuming some portions of the audit report is saved on my personal computer at home; such portion can be treated as information supplied to a computer in the course of the audit activity as required under the law. In other words, the documents envisaged under the Act are not restricted to documents directly derived from the 'usual' computers used in the course of the material activity. The law is concerned with the fact that the document was supplied in the ordinary course of those activities irrespective of the particular computer which was used in the process.

iii. **Documents produced directly or indirectly by a computer (section 84(Sc)**

> The law recognizes documents which are produced by means of appropriate devices such as flash drives, iPods, disks and other devices that may be used to transmit or obtain information from a computer with or without human intervention. Of course, this provision recognizes the current technological trends in the world whereby all manners of devices can be created for interaction with computers.

Another aspect of this section which is likely to generate sufficient debate is the exact purport of subsection (4). While it is conceded that the certificate described under this provision is intended to facilitate the establishment of the conditions stipulated in subsection (2), it is submitted that there is nothing in the provision that suggests that the certificate is a pre-requisite to the admissibility of a document under this provision. In other words, a fulfillment of the conditions stipulated in subsection (2) justifies the admissibility of such document whether or not a certificate under subsection (4) is produced. In this regard, it is instructive to note that the certificate is not required to deal with 'all' the matters mentioned in subsection (2), rather it suffices for the certificate to deal with 'any' of the matters to which subsection (2) relates.[402]

Also, while it is true that this section can be construed to recognize emails and internet downloads as computer-generated, it is difficult to see how such documents can be admissible under this provision in view of the requirement of some sort of consistency and connection in the activities that culminate in the production of documents that can be admissible under this provision. The constant reference to 'ordinary course of activities' in the section raises

[402] See. Section 84(4)(c) of the Evidence Act.

questions on the extent to which this provision has settled the issues relating to the admissibility of computer-generated evidence in Nigeria.

Fifth, Section 93 of the Act provides for proof of signature, handwriting and electronic signature in execution of documents. An electronic signature or e-signature is any electronic means that indicates either that a person adopts the contents of an electronic message or more broadly that the person who claims to have written a message is the one who wrote it and that the message received is the one that was sent. Under the United States Code, an electronic signature for the purpose of United States' Law is 'an electronic sound, symbol or process attached to or logically associated with a contract or other record and executed or adopted by a person with the Intent to sign the record.[403]"

In English law, any insertion of a name by the purported signer or a natural person authorised by him constitutes a valid signature. However, an automatically inserted email address does not constitute a signature. This can be inferred from the decision of the English High Court in the case of *Mehta v. J Pereira Femandes'*[404] which explained the idea of an electronic signature as follows- "if a party or a party's agent sending an email types his or her or his or her principal's name to the extent required or permitted by existing case law in the body of an email, then in my view that would be a sufficient signature". Indeed, Courts in various jurisdictions have decided' that enforceable electronic signatures can include agreements made by email, entering a personal identification number (PIN) into a bank ATM, signing a credit or debit slip with a digital pen pad device at a point of sale, installing software with a click wrap software license agreement on the package and signing

[403] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cbi?dbname=106_cong_public_laws&docid=f:pub1229.106.pdf accessed on the June, 20, 2016 at 12:24pm.
[404] http://www.baillii.org/cgi-bin/markup.cgi?doc=/ew/cases/EWHC/Ch/2006/813.htm English High Court 2006

electronic documents online.[405] Section 100 of the repealed Act laid sufficient emphasis on a person's 'handwriting' to justify the inference that only a 'handwritten signature' was envisaged under that Act. Thus, I order to give effect to previous provisions of the Act in relation to admissibility of electronic evidence, this section introduce two subsections in modification of section 100 of the repealed Act. The purport of the newly introduced provisions is to recognize the validity of an electronic signature whenever document is required to be signed under any rule of evidence.

It is instructive to note that though the Act provides an example of how an electronic signature may be proved; any, other suitable manner may be employed in proving an electronic signature. The method provided by the Act involves showing that it is necessary for a person to execute a symbol of security procedure before gaining access to an electronic record. For instance, if a financial transaction is recorded on a computer and authenticated by an electronic signature, evidence that such record cannot be accessed by any person without a particular security code or password[406] is sufficient evidence of the electronic signature of the record. Obviously, this provision is fraught with difficulties in its construction and its practicability. The main difficulty however would lie in the ease at which such provisions can be manipulated for mischievous purposes. For instance, section 84(4) of this Act provides for a certificate satisfying the Court of certain conditions and 'signed' by the maker. By virtue of subsection (2) of this provision, the maker of such certificate can lawfully append an electronic signature upon such certificate. In other words,

[405] http://www.arbitrate.org.uk/nvmay03/ectrcts4.htm

[406] Such security code or password should be shown to ordinarily be within the exclusive knowledge of the person alleged to have signed the document. This is necessary in order to demonstrate that the document can only have signed by that person.

the legislative attempt to address a, mischief in section 84 has been frustrated' by this provision. This is because such an electronically-signed certificate must now be subjected to the same conditions stipulated in section 84(2). Indeed, it must be acknowledged that proof of matters such as electronic signature would be an extremely technical issue which the law cannot adequately provide for. It would' however be interesting to see how the Courts would approach the application of this provision.

Sixth, Section 151 of the Act provides for presumption as to public maps and charts. In modern times, most government departments, especially land registries,[407] have developed computerized registries in order to modernize their operations and boost efficiency. It would therefore be a calamity if computerized maps or charts are not recognized as evidence under the law. Thus this provision modifies section 119 of the repealed Act by taking cognizance of the admissibility .of maps and charts which are reproduced inter alia by any mechanical or electronic process.

Further, section 153 of the Act provides for presumption as to telegraphic messages. This provision introduces another interesting presumption in addition to the presumption in respect of telegraph messages.[408] The Court may presume that an email sent to an addressee corresponds with the message which the sender fed into his computer. The 'Court is however precluded from making any presumption as to the receiver of such message. The logic here is simple; it is easier to presume that a particular message was sent to a particular person but it may be difficult to presume that the message was received by the addressee as same might have been read or received by another person.

[407] For instance, the Abuja Geographic Information System (AGIS)
[408] Cf, Section 121 of the repealed Act.

Furthermore, the evidence foundation of electronic evidence in shipping cases dates back 2002 when the Supreme Court of Nigeria in its judgment in *P.A. Awolaha & Ors v. Seatrade Groningen B. V.,*[409] recognised that the exchange of contracts affreightment by telex, facsimile, the internet and modern forms of information technology were the order of the day. This was what his Lordship *Belgore J.S.C.* stated at page 535 of the judgment.

More recently in the case of *Continental Sales Limited v. R. Shipping Inc.*[410], the Court of Appeal (Lagos Division) held at page 85 per O*gunwumiju J.C.A.* that: Email is a form of communication that is set down in writing. It is not moral, the fact that is electronic is immaterial. It is not in thin air, it can be downloaded and as real as a hard copy of a letter or mail in your hand". As such the use of electronic mails has over the years taken deep root not only in transactions leading to contracts of affreightment worldwide but also in the litigation process. Bills of lading, charter parties and other shipping documents are now oed and exchanged by e-mails which are then downloaded computers and tendered in Court without necessarily producing the originals themselves. In the very recent case of *Dr. Imoro Kubor & Another v. Honourable Seriake Henry Dickson & Others*[411] the Supreme Court of Nigeria had to consider the issue of the admissibility of a newspaper publication (a public document) which was downloaded from the internet and which document had been tendered and rejected by the lower Court. His Lordship *Onnoghen J.S.C.* while interpreting the provisions of Section 84 of the Evidence Act limited it only to the provisions of Section 84(2) of the Evidence Act. After setting out the section in extenso, he held further.

[409] (2002) 4 NWLR (pt 758) 520
[410] (2013) 4 NWLR (pt 1343)67
[411] (2013) 4 NWLR (pt1345) 534

> "A party that seeks to tender in evidence a computer generated document needs to do more than just tendering same from the bar. Evidence in relation to the use of the computer must be called to establish the above conditions. In the instant case there was no evidence on record to show that the appellants in tendering Exhibits "D" and "L" satisfied any of the above conditions. In fact, they did not, as the documents were tendered and admitted from the bar. No witness testified before tendering the documents to there was no opportunity to lay the necessary foundations for their admission as e-documents under section 84 of the Evidence Act 2011. Since the appellants never fulfilled the pre-conditions laid down by the laws Exhibits "D" and "L" were inadmissible as computer generated evidence/documents.[412]"

India's experience Section 65B (4) India has come a long way on the subject of admissibility of electronic evidence. Indian courts have developed case law regarding admissibility of electronic records, and judges in the country have also demonstrated perceptiveness in interpreting the law on the issue. Section 65B of the Indian[413] is in pari materia with Section 84 of the Nigeria[414]. Section 65B (4) of the India[415] mandates the production of a certificate of authentication as we have it under section 84(4). Despite the mandatory nature of the provision, the original attitude of Indian courts was to ignore the requirements. For instance, in *State V. Mohd. Afzal & Ors*[416], a Delhi High Court, held that Section 65B(4) provides an alternative method to prove electronic record. Also, the Supreme Court of India, *in Navjot Sandhu V Afsan Guru*[417] held that courts could admit electronic records such as printouts and compact discs (CDs) as prima facie evidence without certificate of authentication. This trend continued for nine years until 2014. In 2014, there was a shift in the attitude of Indian courts towards interpretation of Section

[412] *Ibid*
[413] the Indian Evidence Act 1872 (as amended)
[414] Evidence Act, 2011.
[415] *Op Cit* Indian Evidence Act
[416] (2003) Delhi High Court
[417] (2005) Supreme Court of India

65B. A creative interpretation was resorted to in order to enhance the process of authentication as contained in 65B. The Supreme Court of India conclusively decided that electronic records can be proved only in accordance with the procedure set out under Section 65B of the Evidence Act (Nigeria's 84). *In Anvar V.P.K. V. Basheer, & ors*[418], the Supreme Court overruled its own decision *In Navjot Sandhu V Afsan Guru (Supra*) and redefined the law on admissibility of electronic records to reflect the letters of section 65B and ensure the credibility and evidential valueof electronically generated evidence. In that case, *Mr. P.V. Anvar* who had lost the previous Assembly election contended that his opponent *P.K. Basheer* had tarnished his image and assassinated his character. The Supreme Court of India declined to accept the view that the courts could admit electronic records without certificate of authentication. It held that in the case of any electronic record, for instance, CD, VCD, chip e.t.c., the same must be accompanied by a certificate in terms of Section 65B, obtained at the time of taking the document without which the secondary evidence pertaining to that electronic record is inadmissible.

The essence being to enhance and safeguard the authenticity of such evidence. Explaining the rationale behind the decision, the Supreme Court of India stated:"Most importantly, such a certificate must accompany the electronic record like computer printout, Compact Disc (CD), Video Compact Disc (VCD), pen drive, etc., pertaining to which a statement is sought to be given in evidence, when the same is produced in evidence. Electronic records being more susceptible to tampering, alteration, transposition, excision e.t.c., without such safeguards, the whole trial based on proof of electronic records can lead

[418] (2014) Supreme Court of India

to travesty of justice". This is a progressive approach of interpreting provisions relating to production of certificate of authentication. Recently, the decision in Anvar's case was followed in *Jagdeo Sigh v. The State & Ors*[419], which involved the admissibility of intercepted telephone calls in a CD and CDR, which were without a certificate under Section 65B of the Indian Evidence Act. The High Court of New Delhi (*Per Muralidhar, J.)* held that the secondary electronic evidence without a certificate is inadmissible and cannot be looked into by the court for any purpose. Finally, I posit that strict compliance with Section 84(4) is mandatory for a person who seeks to tender electronically generated evidence. Proper and holistic interpretation of Section 84[420] is what is required to appreciate this point. Any other construction will be inconsistent with the spirit and letters of Section 84[421]. Additionally, the purpose for which the subsection has been enacted will be defeated. The world is advancing in technology at an astronomical rate. Our law must be construed progressively to move with technological advancement.[422]

4.4 Challenging Issues facing the Judiciary in Combating Cyber Crime

4.4.1 Legal Challenges in Tackling Cybercrime

Despite the legislative and regulatory measures to counter cybercrime, there are a few legal challenges that remain. These will be considered in turn.

xx. **Jurisdictional problems**

[419] (2015) Supreme Court of India
[420] the Evidence Act, 2011
[421] *Ibid*
[422] Justice alaba Omolaye- Ajileye (2016) A Guide to Admissibility of Electronic Evidence

Simply put, jurisdiction can be defined as scope of authority. It is the inauguration of legal authority.[423] Jurisdiction is arguably the most topical issue in Nigerian jurisprudence and 'probably one of the most contested issues in the regulation of cyberspace.'[424] Prior to the enactment of the Cybercrime Act, the trial of a financial cybercrime would have raised complex jurisdictional issues, given the recent decisions of the Court of Appeal in *Okey Nwosu v FRN*[425] and *Akingbola v FRN*[426] that criminal jurisdiction over matters delineated in Section 251 of the Constitution belongs exclusively to the Federal High Court. This issue is far from settled, as a decision of the Supreme Court is in the offing.[427] However, with respect to cybercrimes, the Cybercrime Act has expressly stipulated exclusive jurisdiction for the Federal High Court in respect of offences created under the Act.[428] The vesting of powers to hear offences of cybercrimes under section 50 of the Cybercrime Act creates a burden on the Federal High Court where is already inundated with cases already specified under S.251 of the Constitution, but in our opinion there should be a special division for such case to aid smooth and fast dispensation of justice this is because it can cause delay in the prosecution of cybercrimes in Nigeria.

The jurisdictional challenge emphasises the need for regional and/or international harmonisation of anti-cybercrime regulations and laws. With particular reference to banking, the challenge is exacerbated by globalisation and the attendant blurring of traditional territorial borders in financial markets. Realistically, establishing an international anti-cybercrime regime might not

[423] Dorsett S., and S McVeigh (2012) Jurisdiction Routledge, p. 4.
[424] Olanikpekun O., *op cit* p.23
[425] (2013) LPELR-22143.
[426] (2014) LPELR-24258.
[427] The decision in *Okey Nwosu v FRN* is now on appeal to the Supreme Court.
[428] Section 50.

go beyond the level of 'soft law.'[429] It has been aptly observed that international financial law comprises mostly of 'soft law,' with a system of 'equal and sovereign states whose actions are limited only by rules freely accepted as legally binding.'[430] Harmonisation is perhaps more realistically feasible on a regional rather than on an international level, as there is likely to be more convergence of regulatory and legislative objectives at the regional level.[431]

The CECC has emerged as a relatively successful model at the European level because of the EC legislative framework.[432] Such standardised framework is yet to be put in place in Africa. Perhaps, policy makers can explore the more feasible option of bilateral arrangements. Again, the ratification and domestication of the CECC will enable Nigeria to take advantage of the mutual assistance and reciprocity provisions. A major limitation of the provisions of section 50 of the Cybercrime Act is the fact that other foreign States are not bound to enforce them.

While S. 51 of the same Act provide that "offences under the Act shall be extraditable where the extradition Act. Though under the international laws, a country has no obligation to turn over a criminal to the requesting entity. Section 52 of the Cybercrime Act, recognises the need for international

[429]See generally Degan, V D (1997) *Sources of International Law* Nijhh off Publishers London p.238; Alexander K and Ors, (2006) Global Governance of Financial Systems: *The International Regulation of Systemic Risk*, Oxford University Press Chapter 4; Abbott K W and Snidal, (2000) 'Hard and Soft Law in International Governance' 54 International Organization 3, 421; Chodosh, H., (1991) 'Neither Treaty nor Custom: The Emergence of Declarative International Law' *26 Texas International Law Journal* 88; Weil, P., (1983) 'Toward Relative Normativity in *International Law' 77 American Journal of International Law* p.413; Brummer, C., (2012) *Soft Law and the Global Financial System, Rule Making in the 21st Century,* Cambridge University Press.

[430] Lastra R M., Note 50, 501.

[431] In recent years, regional cooperation and institutions have developed faster and easier than international systems. See Mansfield E D., and Milner H.V, (1999) '*The New Wave of Regionalism' 53(3) International Organization* P.589.

[432] Goddard J., and Ors, (2007) 'European Banking: An Overview' *31 Journal of Banking and Finance* Vol 7, P.1911; Alford D, (2006) 'The Lamfalussy Process and EU Bank Regulation: Preliminary Assessment and Future *21 Journal of International Banking Law & Regulation 2*, 59; Marttila J, (2005) 'The Main Challenge for CEBS: Convergence of Supervisory Practices Across the European Union' 20 *Journal of International Banking Law & Regulation 7*, 341;

cooperation. Perhaps, this provision might be utilised for cross-border cooperation agreements, with provisions for information sharing and cooperation in investigation and prosecution. Such agreements will ensure mutual recognition of domestic regulatory and legislative provisions, so that cybercriminals do not find jurisdictional safe havens by exploiting discrepancies in national laws.[433]

Electronic robbers and forgers leave fewer clues than white-collar criminals who alter checks or intercept promissory notes. For example, a skilled forger who adds zeroes to a check leaves more clues than a digital thief. The use of false email headers, offshore sites, and anonymous e-mailers also make catching cybercriminals more difficult. Because cybercrime is borderless by its nature, it creates new methods of concealing wrongdoing.[434] "Dual criminality and jurisdictional conflicts" is a principle of international criminal law under which an accused individual may be extradited "only if the alleged criminal conduct is considered criminal under the laws of both the surrendering and requesting nations." *U.S. v. Saccoccia,* [435]. This principle often provides a direct roadblock to prosecution of international cybercrime, and it was a key factor in barring prosecution of the Love Bug attack – the extradition treaty between the Philippines and the United States demands dual criminality.[436] As a result of the Philippines' lack of computer crime statutes, the actions of the GRAMMER Soft ring were not considered a punishable

[433] On cross-border cooperation, see Pratt R., and Schiffman H., (2007) 'Cross-Border Cooperation and Information Exchange: Overcoming the barriers to Regulatory Cooperation' in *Working Together: Improving Regulatory Cooperation and Information Exchange,* Monetary and Financial Systems Department IMF Washington DC.

[434] Cybercrime Before the S. Judiciary Comm., Criminal Justice Oversight Subcomm. and House Judiciary Comm., Crime Subcomm., 106th Congress (2000) (statement of Michael A. Vatis, Dir., Nat'l Infrastructure Prot. Ctr., FBI), *available at* http://www.usdoj.gov/criminal/cybercrime/vatis.htm accessed 02/06/2016 at 9:42am..

[435] 18 F.3d 795 (9th Cir. 1994).

[436] *See* U.S. Treaty Doc. 104-16, Extradition Treaty with the Philippines ("Article 2(1) defines an extraditable offense as one punishable under the laws of both Contracting Parties by deprivation of liberty for a period of more than one year, or by a more severe penalty").

offense outside of its borders; thus, investigators from the United States were unable to extradite members of the GRAMMER Soft hacking ring to face prosecution.

In response to these frequent dead-ends, the international community has taken steps to help encourage greater cooperation between nations with respect to cybercrime, including passage of UN General Assembly Resolution 55/63, designed at combating international "criminal misuse of information technologies." Resolution 55/63 specifically calls on all member states to "eliminate safe havens for those who criminally misuse information technologies," and further establishes that "law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States." UN General Assembly Resolution 55/63, "Combating the criminal misuse of information technologies." These global efforts have been echoed on the regional level as well, with groups such as the Organization of American States calling upon its member-states to "creat[e] a framework for enacting laws that protect information systems, prevent the use of computers to facilitate illegal activity, and punish cybercrime.[437] Despite these efforts, there remains significant resistance to abandoning the "dual criminality" principle, as nations are loath to expose their citizens to international criminal liability when such acts are not illegal under (and sometimes condoned by) the accused's native government. Moreover, as

[437]See, Organization of American States Resolution AG/RES 2004 (XXXIV-O/04), "Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cyber Security: A Multidimentional and Multidisciplinary Approach to Creating a Culture of Cyber Security.

seen in the Sony hack, many nations (including the United States) recognize the utility of cyber warfare as a key method of non-military aggression, and they may be resistant to allowing foreign governments to extend jurisdiction over such actions.[438]At this time, jurisdictional and other issues related to "dual criminality" seem likely to persist into the future; insufficient incentives exist for governments to change current practices and allow greater international oversight over their online actions and the actions of their citizens. Despite this, countries may find themselves needing to weigh the advantages of jurisdictional sovereignty against their ability to effectively combat an ever-increasing number of cross-border cybercrime attacks.

xxi. Evidential Issues

Although the Evidence Act 2011 had significantly ameliorated the hitherto major obstacle to the admissibility of evidence, the problem is not over, S. 126 and 127 of the Act[439] requires all facts to be proved in court by direct oral evidence unless with regards to the contents of a document. The implication is that witnesses and victims of cybercrime must be in Nigeria for such trial, considering the cost implications. The Act has not make provision for the adoption of technology for taking aid or transmission of testimonies, for example, through video conferencing etc., for this challenges to be mitigated. S. 15 also gave judge discretion to exclude some evidence obtained improperly or in contravention of law unless the judge deem same to be desirable.

[438] *See*, *e.g.*, Sanger, David. "Obama Order Sped Up Wave of Cyberattacks Against Iran, *N.Y. Times* (discussing the Stuxnet cyberattack launched by the United States and Israel against the computer systems operating Iran's nuclear enrichment facilities); *See also* Hancock, David. "Feds Out-Hack Russian Hackers," *CBS News*, May 12, 2002 (discussing the Invita operation, the FBI counter-hacking sting of Russian nationals engaged in the theft of credit-card information).

[439] Evidence Act 2011

Section 84 of the Evidence Act (EA) 2011 provides for the admissibility of computer-generated evidence. It makes computer-generated evidence admissible in any proceedings upon the fulfilment of certain conditions including the production of a certificate identifying the document and the information contained in it were produced by proper operating computers. There is no gain saying that all evidence to be tendered in proceedings bordering on cybercrime will be of a computer-generated nature. Consequently, section 84 of the EA must be complied with. In *Kubor v Dickson,*[440] the Supreme Court held that for computer-generated evidence to be admissible in court, all the conditions set out in section 84 of the EA must be fulfilled. These conditions were discussed earlier in this chapter.

Prior to the promulgation of section 84 of the EA, attempts to tender computer-generated evidence met with admissibility bottlenecks.[441] The precise nature of the requirement of section 84 of the EA remains unclear and it is certain that the admissibility of computer generated evidence will still remain a challenge. Moving forward, specific provisions in the CA dealing with admissibility of evidence should facilitate the trial of offences established under the Act. S. 15 of the Act[442] which provides that the 'rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence on the mere grounds that it is constituted by a data message.' It further mandates that information contained in data messages must 'be given full evidential weight.'So long as the Evidence Act remains applicable to the Cybercrime Act, admissibility issues will continue to hinder the expedited prosecution of cybercrimes.

[440] (2013) 4 NWLR (Pt. 1345) 534.
[441] Yesufu v African Continental Bank Limited (2012) 1 BFLR 757.
[442] South African Electronic Communications and Transactions Act 25 of 2002 (ECT)

xxii. Legality of the BVN Directive

The BVN is aimed at checkmating both cybercrime and money laundering. However, the irony of the BVN requirement is that it triggers the inherent risk of leaving bank customers vulnerable to cybercrime attacks. The BVN requirement involves the storage of sensitive biometric data, which in itself is the target of cybercriminals.

A more fundamental issue is the legality of the BVN Directive itself. The Directive was made pursuant to powers conferred by section 57 of BOFIA. This power to make guidelines is intended for the furtherance of the general objects of BOFIA. By the tenor of the provisions of BOFIA, the powers of the CBN are exercisable only over licensed banks and other financial institutions. Before exercising such powers the requirement for notices had to be observed.

xxiii. Privacy concerns

Section 37 of the Constitution guarantees the right to privacy of citizens. This right must extend to the most private and sensitive data and information of citizens, including biometric data. This raises a two-fold concern. The first relates to the constitutionality of the requirement for personal information under the KYC and BVN initiatives. This requirement might be considered intrusive and a breach of the constitutionally guaranteed right to privacy, particularly given the multiplicity of biometric data requests by various

regulators in Nigeria.[443] The researcher, suggest that there should be harmonization among service provider and for the government to have a centralized data base which could aid in checkmating the excesses of customers and to eschew multiplicity biometric data.

The second implication raised by the constitutional right to privacy is the obligation placed on government and its agencies to safeguard the various data and information banks and their customers. A failure to protect the information of citizens from cyber attacks will constitute a fundamental breach of the constitutionally enshrined right to privacy.

xxiv. Social networking new platforms for cybercrime

Social networking sites and the number of users expanded considerably in recent years[444], and are now also used for spreading malware, offer targets for other form of cybercrime and constitute security risks. According to *Sophos,*[445] social networks have become a viable and lucrative market for malware distribution with Web 2.0 botnets stealing data, displaying fake anti-virus alerts and generating income for criminals. The proportion of companies reporting spam and malware attacks via social networking increased by 70% in 2009. Employees logging on to social networking sites thus pose serious security risks to the information systems of their companies or institutions by opening them up for spam, phishing, malware and data infiltration.[446]

xxv. Technical expertise

Section 41 of the CA mandates the office of the NSA to:

[443] The National Identity Management Commission, Federal Road Safety Commission, Nigerian Communications Commission (NCC), National Immigration Service and other public as well as private institutions have initiated compulsory biometric data registration requirement.
[444] Facebook alone claimed some 845 million active users in December 2011 (http://www.facebook.com/press/info.php?statistics).
[445] Sophos Security Threat Report 2010 (August 2010). http://www.sophos.com/security/topic/security-report-2010.html
[446] *www.coe.int/cybercrime*

a) Establish and maintain a National Computer Emergency Responses Team (CERT) Coordination Centre responsible for managing cyber incidences in Nigeria;
b) Establish and maintain a National Computer Forensic Laboratory and coordinate utilisation of the facility by all law enforcement, security and intelligence agencies;
c) build capacity for the effective discharge of the functions of all relevant security, intelligence, law enforcement and military services under this Act or any other law on cybercrime in Nigeria;

These requirements underscore the distinct nature of cybercrime policing, investigation and prosecution. Law enforcement agents and prosecutors now have to deal with a new wave of crime and criminals for which they probably have no training. Cybercriminals ply their trade with a daring level of ingenuity. Law enforcement agents have to be equally ingenious in counteracting them. Accordingly, it has been observed that policy makers 'need to develop holistic new models and practitioners to convert information security from a folk art to a disciplined art. Other cybercrimes challenges are; unemployment, poverty rate, corruption, lack of standards and national central control, lack of infrastructure, lack of National functional databases, proliferation of Cybercafés.

xxvi. Reliance on Information Communication Technology

Daily communications depend on Information Communication Technology (ICTs) and Internet-based services, including Voice over Internet Protocol (VoIP) calls or email communications.[447] ICTs are now responsible for the

[447] See: www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996.accessed on 09/06/2016 at 07:47

control and management functions in buildings, cars and aviation services.[448] The supply of energy, water and communication services depend on ICTs. The further integration of ICTs into everyday life is likely to continue.[449] Growing reliance on ICTs makes systems and services more vulnerable to attacks against critical infrastructures.[450] Even short interruptions to services could cause huge financial damages to e-commerce businesses.[451]

It is not only civil communications that could be interrupted by attacks; the dependence on ICTs is a major risk for military communications.[452] Existing technical infrastructure has a number of weaknesses, such as the monoculture or homogeneity of operating systems. Many private users and SMEs use Microsoft's operating system, so offenders can design effective attacks by concentrating on this single target.[453]The dependence of society on ICTs is not limited to the western countries.[454] Developing countries also face challenges in preventing attacks against their infrastructure and users. The development

[448] Goodman, (2001) The Civil Aviation Analogy – International Cooperation to Protect Civil Aviation Against Cyber Crime and
Terrorism in: Sofaer/Goodman, *The Transnational Dimension of Cyber Crime and Terrorism*, p 69, available at: http://media.hoover.org/documents/0817999825_69.pdf.

[449] Bohn/Coroama/Langheinrich/Mattern/Rohs, Living in a World of Smart Everyday Objects – Social, Economic & Ethical
Implications, *Journal of Human and Ecological Risk Assessment*, Vol. 10, page 763 *et seq.*, available at: www.vs.inf.ethz.ch/res/papers/hera.pdf.

[450] Sofaer/Goodman, *Op Cit* p.3

[451] "Sasser". In 2004, the worm affected computers running versions of Microsoft's Windows
operating system. As a result of the worm, a number of services were interrupted. Among them were the US airline "Delta Airlines" that had to cancel several trans-Atlantic flights because its computer systems had been swamped by the
worm, whilst the electronic mapping services of the British Coastguard were disabled for a few hours. See Heise News,
04.01.2005, available at: www.heise.de/newsticker/meldung/54746; BBC News, "Sasser net worm affects millions",
04.05.2004, available at: http://news.bbc.co.uk/1/hi/technology/3682537.stm.

[452] *Shimeall/Williams/Dunlevy*, Countering cyber war, NATO review, Winter 2001/2002, page 16, available at: www.cert.org/archive/pdf/counter_cyberwar.pdf.

[453] see *Picker*, Cyber Security: Of Heterogeneity and Autarky, available at: http://picker.uchicago.edu/Papers/PickerCyber.200.pdf; Warning: Microsoft 'Monoculture', Associated Press, 15.02.2014, available at www.wired.com/news/privacy/0,1848,62307,00.html

[454] see: Spam issues in developing countries, 2005, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

of cheaper infrastructure technologies such as WiMAX [455] has enabled developing countries to offer Internet services to more people. Developing countries have a unique opportunity to integrate security measures early on. This may require greater upfront investments, but the integration of security measures at a later point may prove more expensive in the long run. Strategies must be formulated to prevent such attacks and develop countermeasures, including the development and promotion of technical means of protection, as well as adequate and sufficient laws enabling law-enforcement agencies to fight cybercrime effectively.[456]

xxvii. Number of users

The popularity of the Internet and its services is growing fast, with over 2 billion Internet users worldwide by 2010. Computer companies and ISPs are focusing on developing countries with the greatest potential for further growth.[457] In 2005, the number of Internet users in developing countries surpassed the number in industrial nations, while the development of cheap hardware and wireless access will enable even more people to access the Internet.[458] With the growing number of people connected to the Internet, the number of targets and offenders increases.[459] It is difficult to estimate how many people use the Internet for illegal activities. Even if only 0.1 per cent of users committed crimes, the total number of offenders would be more than one million. Although Internet usage rates are lower in developing countries, promoting cyber security is not easier, as offenders can commit offences from

[455] The WiMAX Forum, available at www.wimaxforum.org; *Andrews, Ghosh Rias*, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking"; *Nuaymi*, WiMAX Technology for Broadband Wireless Access.
[456] see:World Information Society Report 2007,p.95, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.
[457] See Wallsten, (2002) Regulation and Internet Use in Developing Countries, p 2.
[458] see: The WiMAX Forum at www.wimaxforum.org; Andrews, Ghosh, Rias, *Op Cit*.
[459] see: World Information Society Report 2007, Op Cit p. 95,

around the world.[460] The increasing number of Internet users causes difficulties for the law-enforcement agencies because it is relatively difficult to automate investigation processes. While a keyword-based search for illegal content can be carried out rather easily, the identification of illegal pictures is more problematic. Hash-value based approaches are for example only successful if the pictures were rated previously, the hash value was stored in a data base, and the picture that was analysed has not been modified.[461]

xxviii. Availability of devices and access

Only basic equipment is needed to commit computer crimes. Committing an offence requires hardware, software and Internet access. With regard to hardware, the power of computers is growing continuously.[462] There are a number of initiatives to enable people in developing countries to use ICTs more widely.[463] Criminals can commit serious computer crimes with only cheap or second-hand computer technology – knowledge counts for far more than equipment. The date of the computer technology available has little influence on the use of that equipment to commit cybercrimes. Committing cybercrime can be made easier through specialist software tools. Offenders can download software tools designed to locate open ports or break password protection.[464] Due to mirroring techniques and peer-to-peer exchange, it is

[460] Phishing Activity Trends, Report for the Month of April 2007, available at: www.antiphishing.org/reports/apwg_report_april_2007.pdf. Regarding phishing, see above pg
[461] see: *Kerr, Searches and Seizures in a digital world*, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, *Berkeley Technology Law Journal*, Vol. 19, page 1233.
[462] *Moore*, Cramming more components onto integrated circuits, Electronics, Volume 38, Number 8, 1965, available at: ftp://download.intel.com/museum/Moores_Law/Articles-Press_Releases/Gordon_Moore_1965_Article.pdf; *Stokes*, Understanding Moore's Law, available at: http://arstechnica.com/articles/paedia/cpu/moore.ars/.
[463] "World Information Society Report 2007", ITU, Geneva, available at: www.itu.int/wisr/
[464] *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 *et seq.*, available at: www.212cafe.com/download/e-book/A.pdf.

difficult to limit the widespread availability of such devices.[465] The last vital element is Internet access. Although the cost of Internet access is higher in most developing countries than in industrialized countries, the number of Internet users in developing countries is growing rapidly. Offenders will generally not subscribe to an Internet service to limit their chances of being identified, but prefer services they can use without (verified) registration. A typical way of getting access to networks is the so-called "wardriving". The term describes the act of driving around searching for accessible wireless networks.[466] The most common methods criminals can use to access the network fairly anonymously are public Internet terminals, open (wireless) networks, hacked networks and prepaid services without registration requirements. Law-enforcement agencies are taking action to restrict uncontrolled access to Internet services to avoid criminal abuse of these services. In Italy and China, for example, the use of public Internet terminals requires the identification of users.[467] However, there are arguments against such identification requirements. Although the restriction of access could prevent crimes and facilitate the investigations of law-enforcement agencies, such legislation could hinder the growth of the information society and the development of e-commerce.[468]

It has been suggested that this limitation on access to the Internet could violate human rights. For example, the European Court has ruled in a number of cases

[465] In order to limit the availability of such tools, some countries criminalize their production and offer. An example of such
a provision can be found in Art. 6 of the Council of Europe Convention on Cybercrime.
[466] see: Ryan, (2004) War, Peace, or Stalemate: *Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics*, *Virginia Journal of Law and Technology*, Vol. 9, available at: www.vjolt.net/vol9/issue3/v9i3_a07-Ryan.pdf
[467] See for example the article "Privacy and data retention policies in selected countries",availableat www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.
[468] see: Burnheim,(1999) The right to communicate, The Internet in Africa, available at: www.article19.org/pdfs/publications/africa-internet.pdf

on broadcasting that the right to freedom of expression applies not only to the content of information, but also to the means of transmission or reception. In the case *Autronic v. Switzerland*,[469] the court held that extensive interpretation is necessary since any restriction imposed on the means necessarily interferes with the right to receive and impart information. If these principles are applied to potential limitations on Internet access, it is possible that such legislative approaches could entail violation of human rights.

xxix. Power of the Attorney General

The Cybercrime Act require the consent of the Attorney General of the Federation before some certain offences created by the Act could be prosecuted and also the power of nolle prosequi

4.5 The Role of Security and Intelligent Agencies in Curbing Cyber Crime

The terrorist groups may have their harm intents to access the state systems of high value for the state and security structure such as the police, military and other state security agencies. The increase of concern by national state agencies to prevent and combat the cybercrimes in informatics or informative systems, including the cyber terrorism against information systems that are part of critical or strategic structures of one country, requires development of co-operation to ensure judicial co-operation in the fight against organized cybercrime and terrorism. The specialized criminal groups to commit

[469] Autronic v. Switzerland, Application No. 12726/87, Judgement of 22 May 1990, para. 47. Summary available at:
http://sim.law.uu.nl/sim/caselaw/Hof.nsf/2422ec00f1ace923c1256681002b47f1/cd1bcbf61104580ec1256640004c1d0
b?OpenDocument.

cybercrime develop their activities through computer viruses against individual users of internet and above all with sophisticated operations aiming to block the official addresses of private and public institutions such as banks, in order to unlawfully obtain the data or to infiltrate to classified information so to exchange them. Therefore, state institutions both national state agencies as well as international agencies specific role in combating crimes in general and cybercrime in specific are thus;.

15. **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 communications technology (ICT) agencies of government and key private sector ICT organisations.[470] It was established in 2004 by the Federal Executive Council (FEC) on the recommendation of the President. The group was created to deliberate on and propose ways of tackling the malaise of cybercrimes in Nigeria.[471] This includes; educating Nigerians on cybercrimes and cyber security; undertaking international awareness programs for the purpose of informing the world of Nigeria's policy on cyber crimes and to draw global attention to steps taken by the Nigerian government to rid the country of cybercrimes; providing legal and technical assistance to National Assembly on cyber crimes and cyber security in order to promote general understanding of the subject matter among the legislators.[472]/[473]

16. National Information Technology Development Agency Act 2007 (NITDA)

[470] Chawki, M.(2009) Nigeria tackles Advance Fee Fraud*; in Journal of Information, Law and Technology* (JILT), May 28, 2009. Accessed from http://go.warwick.ac.uk/jilt/2009-/chawki on 9/7/2016, p.13
[471] *Ibid*
[472] *Ibid*
[473] Abubakar Is'haq (2016*) An examination of the institutional Framework for Combating Cybercrimes in Nigerian*: Being a Seminar Paper Presented at the Faculty of Law, Ahmadu Bello University, Zaria.

In 2001, the National Policy on Information Technology[474] 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/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.[475] The policy also seeks to protect and promote the interest, assets and safety of Nigeria 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[476] 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 and NITDA's mission is to make Nigeria IT capable country as well as using IT as an engine for sustainable development.[477] It is also NITDA's mandate to ensure the safety of the Nigerian cyber space and a successful implementation of an electronic government program. In this regard, NITDA formulates the National Information Systems and Network Security Standards and Guidelines in January, 2013.[478] Draft Guidelines on Data Protection in September, 2014.[479] Guidelines on Nigeria Content Development in Information and Communication Technology (lCT) in December, 2013[480] and the Standard for

[474] For elucidation on development in ICT Policy in Nigeria, see Ladan, M.T. *Op Cit.,n.1*, pp.133-134
[475] Seeparagraphs 2, 3 and 4 of the National Information Technology Policy. Accessedfromhttp://www.nitda.gov.ng/document/nigeriaitpolicy.pdf. on May 6,2015 at 4:15pm.
[476] See Chapter 12, para., 12.1*Ibid.*
[477] *Ibid.*
[478] See paragraph 2.1 (a) of the National Information System and Network Security Standards and Guidelines.
[479] The Guidelines serve as reference for data collections, data custodians, data processors, systems Auditors among others. See Guidelines on Data Protection Draft Version 3.1 published by National Information Technology Development Agency(NITDA), September, 2013. Accessed from http://www.nitda.govs,ng/ on May 5, 2015, at 2:00pm.
[480] The Guidelines were issued with the view to provide a Framework for the Regulation and Legislation on the Creation, Distribution and use of Information Technology within Nigeria. See para. 5 of the Guidelines.

Digital and Computer Forensics in Nigeria in March, 2014.[481] 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 no much commitment towards the actualisation of the ideals of the policy in respect of cyber laws and security. The only commitment so far is the enactment,[482] though some specific cybercrimes legislation are still lying comatose before the National Assembly despite all the cries for their immediate passage.[483]

17. Nigerian Communications Commission (NCC)

The Nigerian Communications Commission (NCC) was established under the Nigerian Communications Act.[484] The NCC is the independent national regulatory authority for the telecommunication industries in Nigeria. The Commission 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.[485] In furtherance of its mandate, the Commission has put in place guidelines for the provisions of Internet Service Providers (ISP) and other internet protocol based telecommunication services.[486]

The Guidelines require ISPs to ensure that users are informed of any statement of cybercrimes prevention or acceptable internet use published by the Commission or any other authority and that failure to comply with these acceptable use requirements may lead to criminal prosecutions.[487] Internet

[481] The objective of the standard document is to develop the standard for the implementation of digital and computer forensics in Nigeria in terms of electronic evidence acquisition, analysis and presentation in law Courts
[482] Cybercrimes Act 2015.
[483] See for example, *Computer Security and Critical Infrastructure Protection Bill 2005, Cyber Security and Data Protection Agency Bill 2008, Electronic Fraud (Prohibition) Bill 2008* etc. The Bill is yet to be assented by the President of the Federal Republic of Nigeria
[484] *Cap.* N97 LFN 2004
[485] Section 3 of the Nigerian Communication s Act.
[486] The guidelines are made pursuant to Section 70(2) of the Act.
[487] *Ibid*, para., 5

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 Commission or any other legal authority.[488] These include information regarding particular users and the content of their communications, while contacting the Commission 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 of face the wrath of the commission. The Commission gave the deadline in a notice titled "Final 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.[489] It has been submitted and this researcher conceded that the possibility of encroachment on the fundamental right to privacy necessitates the putting in place of laws, rather than mere guidelines, strike the right balance between law enforcement and protection of human rights.[490]/[491]

18. 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.[492] The EFCC is vested with the powers to investigate, prevent and prosecute financial crimes

[488] *Ibid, para, 6. For further* discussion on the NCC Guidelines for 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.
[489] See Muhammed, H., (2009) 'NCC Clamps down on Illegal ISPs, Cyber Cafes, '*Daily Trust*. Monday, February 23, *pp.55*
[490] *Ibid*
[491] Abubakar Is'haq *Op Cit.303*
[492] See Section 2 of the EFCC Act 2004

such as the Advance Fee Fraud and corrupt practices among others.[493] 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.[494] The Commission is also responsible for identifying, tracing, freezing, confiscating and seizing proceeds of economic crimes. EFCC also host the Nigerian Financial 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.[495] 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.[496]

One of the watershed cases of cybercrimes handled by the EFCC was the case of *FRN Vs Amadi*.[497] In this case, 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 (AFFA). The accused was alleged to have attempted to obtain the sum of US $125,000 from one Fabio Fajans by sending a payment schedule containing false pretence to the said Fabio Fajans requesting for

[493] In Moore vs EFCC, (2010) Economic Crimes Law Report (ECLR) 312 at 314, where it was held that Section 6 & 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 toany of the functions stated in Section 6 and the special function in Section 7 of EFCC Act.
[494] Chawki, M. *Op Cit., n,4.* P.11
[495] *Ibid*
[496] *Ibid*
[497] (2005) 2 QCCR 129.

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 Garnes, 2003. The prosecution witness (PWl), *Abdulkarim Chukkol*[498] who acted as agent provocateur stated that the Commission 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, the operator of the fake website responded and series of communication ensued. The prosecution witness subsequently introduced himself as Fabio 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 (Damon Yelma) the Investigating Police Officer (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 as 7946846 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 (Benjamin Billie), an officer of the Multi-links testified that the accused bought the Multi-links line from one of

[498] EFCC Staff of the Advance Fee fraud unit and Head of Cybercrimes Unit Lagos Office. He is responsible for investigating Cybercrimes at the Commission. In an interview granted in the course of this research , he reliably disclosed that EFCC is now receiving ICT training from reputable international security organisations such as the FBI, Organisation for Economic Cooperation and Development (OECD)and Microsoft among others.

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 (Bala Dahiru Hamidu), an officer of the CBN stated 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 www.efcconline.com. 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 PWI alias Fabio Fajans in the bundles of documents admitted as Exhibit P 1. The evidence of PW 1 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. PWI acted throughout as an agent provocateur. The testimony of PWI 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 PWI alias Fabio Fajans gave direct evidence that he received the emails containing false pretence from the accused ... The accused persori 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 heard 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.[499] 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*.[500] 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 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

[499] See Appeal No: CA/L/389/2005
[500] (2008) 18 NWLR. (pt. 119)259

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 first 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*[501] is one of the cases where the apex court In Nigeria pronounced on internet or computer related crimes in Nigeria.

In 2013, the EFCC recorded 177 convictions in different courts across the country.[502] Of the 117 convictions recorded by the EFCC, 57 of which 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 is the principal enactment now in place for combating cybercrimes in Nigeria. This represents 49 percent of the total convictions secured by the EFCC in the year 2013. It can be seen from some of the cases stated in the EFCC Record of Convictions 201'3 that the courts have exercised wide discretions in sentencing the convicts to various terms' of imprisonment. And,

[501] Supra.
[502] See EFCC Record of Convictions, 2013

far from applying the minimum term of imprisonment as provided by the Act,[503] the courts have resorted to giving different terms of imprisonment for the same offence[504] and in some cases, with option of fine.[505] The least sentence under the AFFA 2006 is 3 years imprisonment.[506] 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 positive and commendable, however, the punishments imposed by the courts vary from the minimum terms of imprisonment for 6 months and the maximum of 91 years.[507] 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.[508] For example, in 2010, it was reported that the EFCC in

[503] Imprisonment for not less than 7 years without option of fine for the offences of obtaining property by false pretence and fraudulent invitation under section 1(3) & 4 of the Act; not less than 5 years without the option of 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 the financial institution who facilitates, contributes or otherwise is involved in failure to exercise due diligence stipulated under section 7(3) of the Act.

[504] See for example the cases of FRN Vs Olasaidi Dare and FRN vs Churchhill Joshua Essien (4 years instead of the 7 years minimum); FRN vs Enejuru Prince Patrick, FRN vs. Akinloye Akintunde, FRN vs. Auwal Ibrahim (3 years instead of the 7 years minium); 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).

[505]See for example the cases of FRN v Auwal Ibrahim, FRN v Nathaniel, FRN v Ugoji T. Ugoji, FRN v Maigari Bello Ibrahim T., and FRN v Bashir Ali & Anor.

[506] 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 Section 7(3) (b) and Section 13 (5) (c) of the AFFA 2006.

[507] See for example, serial Nos: 1,2,5 and 109 of the EFCC Record of Convictions 2013.

[508] See EFCC Partner Australian Police in fighting Internet Fraud. Accessed from http://efccnigeria.org/efcc/index... on 5/2/2015.

collaboration with the Serious Organised Crime Agency (SOCA) of the United Kingdom, made a recovery of N26.5 billion from perpetrators of cybercrimes in 3 years.[509] Within the period, the Commission 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.[510]

The EFCC's cybercrime operations were inhibited due to lack of technical know-how, ICT software and other technical infrastructures. Besides, the EFCC has adopted music as one of its way of combating cybercrimes in Nigeria. This is in reaction to efforts by some musicians at encouraging cybercrimes through the instrumentality of music. Prominent among such musics are Nkem Owoh's "Oyinbo I go Chop Your Dollars,[511] and Olu Maintain's "Yahoozeee.,[512]. Thus, in collaboration with Microsoft company, the EFCC contracted some musicians to sing the song entitled "Maga no need pay!" From the aforestated, it can be seen that the battle for and/or against 419 and cyber related crimes have been taken to the music world. Music, said to be a source of inspiration to some people have been used for the good and/or bad of the society.[513]

19. Nigeria Internet Group (NIG)

Nigeria Internet Group (NIG) was founded in 1995 as non profit, non-governmental organisation principally saddled with the responsibility of

[509] See Amaefule, E.(2010). 'EFCC, SOCA Recover N26.6 billion in 3years.' Accessed from http://home.rica.net/alphae/419coal/news2010.htm. on November 10, 2015.
[510] *Ibid*
[511] Nkem Owoh is a Nigeria renounce actor and comedian, a graduate of Engineering at University of Ilorin. The song "I go chop your dollar" featured in the film " the master " in which Owoh plays a scammer. The EFCC and National Broadcasting Commission (NBC) banned the song , perhaps in response to agitations and pressure from the international communities.
[512] Olu Maintain, in an interview he granted to weekly Trust Newspaper, denied that his music "Yahooze" was meant to celebrate the "Yahoo-Yahoo boys" and their 419 activities. He maintained that yahooze is a music that lift ones spirit. It simply saying when you work from Monday through Friday, you owe yourself the duty to unwind from Friday to Sunday.
[513] Abubakar Is'haq *Op. Cit*

promoting the internet in Nigeria.[514] To achieve its mandate, the Group engages in a number of activities which include; policy advocacy, awareness creation and education through conferences, seminars, exhibitions, workshop and news letter publication. The advocacy activities of the Group let to the licensing of the first set of internet service providers in Nigeria. The Group has made positive and impactful contributions to virtually all government policies and legislation that are related to the internet and the ICT sector in general. Such policies and legislation include; the National IT Policy, the NITDA Act, the EFCC (Amendment) Act, the Cyber Security Bill, the National Policy on Telecoms and the Telecoms Act.[515]

20. Nigeria Computer Society

The Nigeria Computer Society (NCS) is the umbrella organisation of all information technology professionals, interest groups and stakeholders in Nigeria. Formed in 1978 as Computer Association of Nigeria (COAN) and transformed into NCS as a result of harmonisation with other stakeholders and interest groups.[516] The NCS is a national platform for the advancement of information technology science and practice in Nigeria.[517] Part of the NCS strategic objectives include the promotion of the education and training of computer and information scientist, computer engineers, information and communication systems professionals; encourage research in the advancement of computer and information science among others.[518] It is not in doubt that the NCS has contributed to policy formulation with respect to cybercrimes in

[514] See http://www.nig.org.ng/about.php. Accessed on July 5, 2016.
[515] *Ibid*
[516] See http://www.ncs.org.ng/about-ncs. Accessed on May 7, 2016.
[517] *Ibid*
[518] *Ibid*

Nigeria, hence its membership of the Nigeria Cybercrimes Working Group (NCWG).[519]

21. Internet Service Providers Association of Nigeria (ISPAN)

The Internet Service Providers Association of Nigeria (lSPAN) is an independent body and voluntary association acting in the interest of internet service providers and generally dealing with matters related to the provision of internet service in Nigeria. ISPAN's mission is to provide a forum in which internet service providers can address issues of common interest and interface with industry stakeholders so that end users receive world class service and industry participants earned a fair return on their investments.[520] Recently, ISPAN urged cyber cafe operators to join the government in the fight against cybercrimes in Nigeria.[521] In its efforts at combating cybercrimes, ISPAN has blocked many sites because they were used to facilitate internet scams otherwise known as 419. Perhaps, that was why many cyber cafe operators do not want to use the connection of the ISPs hence they own their private connections known as Very Small Aperture Terminal (VSAT)[522] which makes tracking, apprehension and prosecution of offenders more challenging to enforcement institutions. It is submitted that if the ISPs join the government in the fight against such crimes, it will change the image of Nigeria among the comity of nations.

[519] Abubakar Is'haq *Op. Cit.*
[520] See http://www.jidaw.com/comm.htm. Accessed on July 16, 2016 at 2:18pm.
[521] See http://www.news/breakingnews… Accessed on July16, 3016 at 2:38pm.
[522] A type of two-way satellite that transmits both narrow and broadband data to satellites in orbit. The data is then redirected to other remote terminals or hubs around the planet. VSATs are mainly used for wireless transmission of real-time data.

There is therefore, the need for collaboration between and/or among the law enforcement agents, the operators and Nigerians to curb cybercrimes in Nigeria.[523]

22. Department of State Security

The Department of State Security was established by the National Security Agencies Act.[524] Section I 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 the internal security of Nigeria; and such responsibilities affecting internal security within Nigeria as the National Assembly or the President may deem necessary.[525] 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.[526] The main mandates of the Directorate for Cyber Security (A Directorate in the Department of State Security) are to develop and implement a National Cyber Security Policy for Nigeria; drafting

[523] Abubakar Is'haq *Op. Cit*

[524] Cap. N74 LFN 2004.

[525] See Sections 1 & 2 of the Act, it provide for the establishment of other security agencies such as the Defence Intelligence Agency (DIA) and National Intelligence Agency (NIA). The DIA is charged with the responsibility of the prevention and detection of crime of 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 military nature within and outside Nigeria as the President or the Chief of Defence may deem necessary. The NIA on the other hand is charged with the responsibility for the 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.

[526] Adewale, K.S., Isiaka, R.M., and Olayemi, R.T., '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, 2011. Accessed from http://www.ijsat.com. On 14/07/16.

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; and establishing a National Computer Emergency Readiness and Response Mechanism with Early Warning System (EWS) and alerts for all cyber related emergency in the country.

The mandate also includes 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 among others.[527] Like the NCWG, the Directorate for Cyber Security's effort, at combating cybercrimes in Nigeria is unknown to this researcher as less is heard of it. Their activities are highly secretive, restrictive and protective. Attempts by this researcher to secure information on cybercrimes through a contact in the Department of State Security did not yield to fruition.[528]

23. The role of Nigeria Intelligence Agency in fighting cybercrime

In the scope of national security institutions of Nigeria operate the intelligence service that in their focus have the collections of information from persons or members of groups that threat national security by committing cybercrimes. The Nigeria Intelligence Agency (NIA) is a vital part of security section. Its primary role is the collection and analyzing of information for threats against the state and the population. The NIA is established as necessity of obtaining the information on time for intelligence, counter-intelligence, internal and

[527] *Ibid*
[528] *Ibid*

external threats, international and national terrorism, organized crime, cybercrime, sabotage and all other issues related to intelligence and Nigeria security. Apart from its role to gather information, the NIA performs the counter-intelligence activities. This activity covers the encountering and obstruction of cyber espionage and foreign intelligence services that are against the interests of the state.

The agency is responsible of information protection and state information system, dealing with verification of security for all employees of the state institutions that have access to classified information. The essential role of NIA is to protect the state and its population. Preventing various crimes, including cybercrimes, terrorism and other threats against national security, the NIA contributes in the security and welfare of the society. It analyzes foreign and internal information, electronic communication through internet and gathers the information for un-information issues such as, propaganda, terrorism, sabotage, espionage etc. The NIA collects information from persons and members of the groups that threat national security with their incriminatory action including cybercrime.[529]

24. 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. The section is headed by a Commissioner of Police.[530]

However, little is known by this researcher of the efforts made by the Nigeria Police to combat the menace of cybercrimes in Nigeria. Attempts made by the

[529] Abubakar Is'haq *Op. Cit*

[530] See http://www.npf.govs.ng/departments/crime-investigation. Accessed on July14, 2016.

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 seems to [531]have 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 specialized manpower skilled in cybercrimes prevention, detection and prosecution this perhaps, informed the call for an independent agency to handle cyber offences in Nigeria.

The Nigeria Police (NP) applies high standards of preserving the classified information. The data-center of NP is used for creating and functioning of entire service infrastructure such as servers, memory disks, network services etc.

The sector receives considerable number of requests from other states involving various cybercrime cases such as: web-page attacks, unlawful profit though services provided by webpage companies, use of unauthorized credit cards (identity theft) etc. Apart from the mentioned activities of the police regarding the fight against cybercrime, an important role has the co-operation with the prosecution office, the court and internet providers with bank representatives, customs and other institutions, depending on their needs. The close cooperation between relevant institutions is a primary or leading condition that cybercrime be prevented and fought efficiently and effectively. In regard to the international co-operation, we can assess it as positive but with intent to further develop it

[531] *Ibid*

25. **Computer Crime Prosecution Unit, Federal Ministry of Justice**

As part of its commitment to 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.[532] The CCPU is to collaborate with agencies such as the EFCC, the Telecoms and banking sectors in its bids to combat cybercrimes in Nigeria.[533] The CCPU is headed by one T. George-Maria Tyendezwa. Officers of the CCPU are said to have commenced training in basic prosecutor's courses and electronic evidence handling among others, while other modalities for the effective take off of the Unit are being worked out.[534] At best, the CCPU is still in its infancy as such little can be said of its efficacy in combating cybercrimes in Nigeria.

26. **Webb Fontaine Nigeria**

This is a specialist firm in the provision of ICT for trade facilitation and improved revenue has achieved a linkage between the Nigeria Customs Service (NCS), Nigerian ports Authority (NPA) and the Federal Airports Authority of Nigeria (FAAN) for Uniform manifest capable of saving the country over N20 billion annually.[535]

A source at NPA told Daily Trust that Webb Fontaine Nigeria stimulated the seamless manifest interaction between the NPA and NCS for a test period of three weeks before it went live in the fourth week. The new development has the capacity to help the NPA billing process, enhance transparency and increase government revenue by preventing possible leakages caused by

[532] Laura, A., *Op Cit* pp. 211-212
[533] *Ibid*
[534] *Ibid*
[535] Eugene A., (2026) New electronic device saves agencies N 20 Billion annually, *Daily Trust*, Saturday, June, 4, p.53

information on forged manifests.[536] The firm improved uniform manifest regime will also help government generate accurate data for planning and economic purposes like knowing the number of shipping lines, number of vessels and types of cargoes coming into Nigeria. The contribution of webb fontaine to cybercrime cannot be over-emphasised has it worked out a digital certificate for the Standard Organisation of Nigeria (SON) whereby importers do not need a hard copy certificate for processing imports. This SON digital certificate regime had also made it impossible for any two companies to use one certificate number as the number allotted will also be attached to the Tax Identification Number (TIN) of the company that applied for and got it.[537]

27. 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.[538] The 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.[539] Interpol has also established collaborative work with the private sector in countering the

[536] *Ibid*
[537] *Ibid*
[538] See http://eprints.qut.edu.au/43400/l/Ali_Alkaabi_Thesis.pdf;. Accessed on July15, 2016
[539] *Ibid*

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.[540] In Nigeria, the Interpol played a major role in the tracking and apprehension of Prince Rapeal Akpiaifo who defrauded a Nigerian company in the sum of $600,000.00 (Six hundred thousand dollars) equivalent to N75million (Seventy-five million naira).[541]

28. **Financial Action Task Force (FAT F)**

The Financial Action Task Force (FATF) is an intergovernmental body established in 1989 by the ministers of its member jurisdictions.[542] 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.[543] 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. 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.[544] They have capabilities to paralyse large parts of communication networks, cause financial meltdown and socio-economic and political unrest.

---

[540] *Ibid*

[541] See the case of FRN v Prince Rapheal Akpiaifo (Unreported Suit No; K/EFCC/O3/2011.

[542] The membership of FATF consists of Argentina, Australia, Austria, Belgium, Brazil, Canada, 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 State of America.

[543] See FATF Mandate (2012-2020). Accessed from http://www.fatf.gafi.org on July 12, 2016.

[544] 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, router and switches. Although the attacks emanated from Russia, millions of bots from around the world were combined into botnet, forming a giant network used to mount the attack. See Traynor, Russia Accused of Unleashing Cyber war to Disable Estonia.' *The Guardian*, May 17, 2007.Accessed from http://www.guardian.co.uk/russia/article/... On May 18, 2016.

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.[545] Further, to qualify cyber terrorism, an attack should resolve in violence against persons or property or at least cause enough harm to generate fear.[546] In June 2007, an attack originated from China shuts down the unclassified network in the Pentagon for a week.[547] Other targets for cyber attacks include power grids, energy infrastructures, banking and financial services, defence services, defence industry, emergency response networks and telecommunications. It was reported that nine out of ten businesses in the United States were affected by cybercrimes. In a bid to counter multi-national crimes, FA TF 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 and Casinos.

The activities of FATF in this 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

[545] *Ibid*
[546] *Ibid*
[547] See Thornburgh, (2007) 'Inside the Chinese Hack Attack,' *Times.* August 25, Accessed from http://www.times.com/time/nation/printout/... On July 14, 2016.

domestic and international financial institutions. It will not be out of place if it is argued that the EFCC was established as a result of pressure mounted on Nigerian Government by the FATF[548].

In conclusion, challenges, current and future threat related to cybercrime cannot be overemphasized, most of the states like in the case of Nigeria, have internal capacities and sources but they are insufficient to respond to cyber-attacks of major dimensions. The limited knowledge of internet of the users, motivation, the capability and facilitations that the criminals have to commit the criminal acts through internet, made the cyberspace an attractive environment for the criminals. The cybercrime is a phenomenon that touches upon a series of competencies, such as informatics, criminology, economy, justice etc. Therefore the cybercrime is to be considered as a complex phenomenon and the only way to confront it successfully is through a global approach in handling this problem. For this, there is a need for a co-operation between the experts of above mentioned fields in order to avoid partial solutions. The lack of membership of Nigeria in regional and international organizations in field of rule of law, remain the main challenges in fighting organized crime. Based on current assessments, there is no single state immune to the cybercrimes, therefore the local institutions in co-operation with international institutions need to be in alert and observe the activities of groups and organizations that may influence on the recruitment and financing of individuals for different cybercrimes.

[548] Abubakar Is'haq *Op. Cit*

CHAPTER FIVE
SUMMARY AND CONCLUSION

5.1 Summary

Safeguarding the sovereign, independence and territorial integrity of the state was the central pillar of Nigerian national security policy. Other guiding principles were African unity and independence, nonintervention in the internal affairs of other states, and regional economic development and security cooperation. Subordinate goals included military self- sufficiency and regional leadership. In pursuing these goals, Nigeria was diplomatic and flexible, but it employed coercive methods or measured force when necessary. Nigeria was an active participant in the United Nations (UN), African Union (AU), and ECOWAS. Being an issue of national priority in Nigeria, cyber security is now elevated to the level of being handled by the Presidency through the Office of the National Security Adviser (ONSA). A reflection of these could be seen in the presentation of the National Cyber Security Policy and Strategy drafts by the above-mentioned office. From the above postulation, it is observed that national security is not restricted only to weapons and military preparedness but encompasses political, social and economic well-being of the people. As such, any threats to any of these constitute a threat to national security. Nigeria is interestingly at a defining moment in the establishment of a cyber-security policy and strategy framework. This is only an aspect of the numerous processes in their developmental stages concerning national security. Every country should have sufficient legislative and judicial capabilities to combat cybercrime and such laws must be harmonious among different countries; since they protect the common interest. It is the considered view of the researcher, that if the result

of the cybercrime occurs upon more than one country and in case there is an extradition treaty among the criminal's country and the countries on its territories the crime has been committed, then the criminal should be extradited to country more affected by the crime, and in case the extent of damages is equal, then the priority should be given to the country that asked for extradition in an earlier date. Cybercriminal activity has increased dramatically in recent years and can now be considered an omnipresent, even global menace that will continue to affect each and every one of us. Hardly a day goes by without cyber-related incidents hitting the headlines of Nigeria's most renowned newspapers, magazines and blogs. Cybercrime is one of the fastest growing areas of crime and has adopted many carefully crafted disguises to damage information systems. With regards to its impact, cybercrime is known to cause both tangible and intangible damages.

In this work, we highlighted an analysis of international, regional and national regulatory responses to cyber crime and cybersecurity in both developed and developing countries. It highlights the limits and challenges of these regulatory responses in the promotion of cybersecurity and explores several regulatory measures to address the highlighted challenges with a view to promoting global cybercrimes. The research suggests several regulatory measures to enhance global cybersecurity and also emphasizes the need for the collective responsibility of states for global cybersecurity. Proper legislation is the foundation for the investigation and prosecution of cybercrime. The efforts of the government in dealing with cyber-threats must therefore be applauded as a demonstration of its desire to stem the tide of deterioration arising from the effect of such threats on the country's national security, economy of

Nigeria, and individual and corporate of lives of Nigerians. In this connection, it is necessary to stress that the legislative, policy and institutional measures to tackle such crimes as money laundering, cybercrimes, intellectual property violation and other computer related offences which constitute threats to the Nigerian cyberspace have been unearthed.

In a quest to tackle cybercrimes, the Nigerian Cyber Crime Act came into force in May, 2015; this explains why the government of Nigeria has continued to solicit for the active support, participation and contributions of stakeholders from relevant sectors towards achieving increased national cyber security. We also presented a comparative evaluation of the Nigerian Cyber Security Policy and Strategy, Cybercrime Act, 2015 and other regulatory framework with those of selected countries. With Nigeria being at crossroads in cyber security policy formulation, it would also provide necessary information as to the viability of the policy and strategy framework with respect to the Nigerian environment.

There is the need to develop a common platform to address cyber security since cybercrime crosses borders and cannot be fought by one country. As a region, Africa must begin to cooperate to deal with cyber threats at national and regional levels. Africa should establish a body to monitor and report cybercrimes across borders. The approach should also involve governments, industry, civil society organizations and to a large extent security agencies. The fight against cybercrime requires coordinated effort among all stake holders such as government bodies, educational institutions, business organizations and law enforcement authorities. Lawmakers must be well trained and sensitized to help implement legislation that addresses cyber

threats at all levels, Africa needs strong Information and Computer Technology institutions to train cyber security experts with a strong expertise in system administration, security audit, forensic investigation, information security and software development to deal with the future challenges of cybercrime.

In addition, as we have entered the second decade of the new millennium, cybercrime has become an increasingly pervasive threat that cannot easily be linked to only a handful of regions. As noted, in the work, that "Cybercrime has no borders". Not only have cybercriminals developed more sophisticated attack strategies, they have also learned how to blur their traces effectively and complicate the work of those seeking to track them down. Compounding matters even more is the fact that security related laws and regulations vary from country to country (sometimes even from province to province), and thus it comes as no surprise that regions with less strict legislation are prone to a higher degree of cybercrime. Our law enforcement agencies must ensure that the constitutionally guaranteed rights are not eroded and subverted in the course championing reforms, though there is no database hence biometric registration requires fingerprint, the following agencies requires biometric Banks via Bank Verification Number (BVN), Nigeria Communications Commission (NCC Subscribers require biometric) Federal Road Safety Commission (FRSC) to obtain drivers license it require biometric, Independent National Electoral Commission (INEC) and the Nigerian Immigration require biometric all this information may shared internationally but does not appearto be available to our local Law enforcement agencies. Nigeria has no legislation regulating how such data should be stored and

accessed. It is to be noted, that this is the data that is used in many developed countries and societies, to build database for criminal investigation through forensic analysis. In United State of America and United Kingdom, there exist laws centered on data retention and privacy conform to set of principles aimed at protecting personal data and ultimately criminalizes unauthorized access and usage in order to deter perpetrator and compensate victim of same. Note that, there is nothing in the Act[549] expresses authority for the use of biometric data to effectively carryout the functions of banking regulation. Under s. 14-25 of the Act,[550] National Identity Management Commission by virtue of the Act are legally backed at least the NIMC Act contains issue of accountability regarding the capturing, storage and sharing of biometric data. Cybercriminals are often anonymous and ubiquitous, their operations can effectively be carried out across borders. More often than not, the effects of cybercrime ripple across several jurisdictions. In this wise, efforts to tackle and sanction cybercrime viewed on international, regional and national perspective must be enhanced as the enactment of substantive laws to criminalize malevolent activities on the internet, enactment of related Bills to strengthen the cybersecurity framework Completion of the legislative process and establishment of institutional framework should be considered a matter of urgency, as the existing legal framework are inadequate in tackling cybercrime in Nigeria, the liberalization of telecoms and Internet penetration policies of government have yielded unprecedented growth in ICT, leading to increased dependence on technology for the delivery of basic as well as critical services in Nigeria amongst citizens, businesses and governments.

[549]Central Bank of Nigeria Act 2007
[550] National Identity Management Commission Act 2007

Finally, Lawyers and judges must understand the complexity involved in digital technology and its value in scientific analysis as a prelude to advocating effective laws and principles for investigation and admissibility of electronic evidence in pursuit of civil or criminal justice. Because of rudimentary understanding of digital technology credibility of information derived electronically is hardly contested by defense lawyers only its admissibility is challenged, the gap is that the conclusions they produce have yet to be tested for reliability the test of reliability of e-evidence is inevitable once knowledge of how it works becomes widespread. Although the issue of admissibility will still be crucial but so will be the credibility of the technology used. As the law and infrastructure improve judges, lawyers, academics and other experts must be prepared for the scrutiny that digital evidence will require[551].

5.2 Findings

1) It is observed from the research that there exist a conflict between the provisions in sections 38 of the Cybercrime Act and S. 37 of the Constitution of the Federal Republic of Nigeria 1999 which guarantees the right to privacy of citizens. This right must extend to the most private and sensitive data and information of citizens, including biometric data. This raises a two-fold concern. The conflict firstly, relates to the constitutionality of the requirement for personal information under the KYC (Know Your Customer) and BVN (Bank Verification Number) initiatives. This requirement might be considered intrusive and a breach of the constitutionally guaranteed

[551] Prof., Bolaji Owasanoye (2014) Admissibility of Electronic Evidence in Nigeria being a paper presented at the Nigerian Institute of Advanced Legal Studies pp44-45

right to privacy, particularly given the multiplicity of biometric data requests by various regulators in Nigeria. The second implication raised by the constitutional right to privacy is the obligation placed on government and its agencies to safeguard the various data and information banks and their customers. A failure to protect the information of citizens from cyber attacks will constitute a fundamental breach of the constitutionally enshrined right to privacy as the constitutional provision prevail over any other Act.

2) It is our finding that, the lacunae created by provision of section 7 of Cybercrime Act manifested in the area of enforcement, compliance and punishment. On enforcement, S. 7 of the Act mandates the operators of cybercafes to register as business name with Corporate Affairs Commission as well as Computer Professionals Registration Council. Cybercafes shall maintain a register of users through sign-in register, and that the register shall be available to law enforcement personnel whenever needed but made no provision for sanction if the section is violated. S.36 (12) of the constitution of the Federal Republic of Nigeria 1999 provides that, a person shall not be convicted of criminal offence unless that offence is defined and the penalty therefore is prescribed in a written law, and in this subsection, a written law refers to an Act of the National Assembly or a Law of a state, any subsidiary legislation or instrument under the provision of a law. It is therefore settled principle of law that any provision of law that do not prescribed punishment for violation is not law because it serve no purpose, the section mere provided a statement with regards to cybercafé owners by prescribing for registration of cybercafés and maintaining a register of users through sign in register but the Act did not provide punitive measure for anyone who failed to complied with this provision. There is the need to insert the provision for

punishment that reflect the seriousness of the offence in S. 7 of the Act which same calls for amendment.

3) It is also our finding that the Evidence Act as it relates to computer-generated evidence and certification of the generated evidence hamper the smooth adjudication of case relating to internet, the integrity of internet generated evidence is also in issue, while 'public documents' may require certification as a pre-requisite for admissibility, some other form of authentication should be created for 'public devices'. This is the fact that section 104 of the Act is clearly designed or 'documents' and does not in any way envisage 'devices'. Another crucial issue is on the rigidity of the provisions dealing with the requirement for certification of public documents. There is a need to qualify the requirement of certification in certain cases. The blanket requirement of certification for all documents (and devices) emanating from public authorities is bound to occasion hardship and injustice such a certificate must accompany the electronic record like computer printout, Compact Disc (CD), Video Compact Disc (VCD), pen drive, etc., pertaining to which a statement is sought to be given in evidence, when the same is produced in evidence. Electronic records being more susceptible to tampering, alteration, transposition, excision e.t.c., without such safeguards, the whole trial based on proof of electronic records can lead to travesty of justice.

5.3 Recommendations

In view of the inadequacies with the legal response in combating cybercrime, as highlighted in this work, to help safeguard against cybercrime attacks, we recommend as follow:

1) It is recommended that in order to reduce the scourge of cybercrime in the country, financial institutions in the country should establish fraud detection departments. The Evidence Act has become grossly inadequate to cover the present advancement in technology with the concomitant sophistication employed in the commission of economic and financial crimes as it relates to computer-generated evidence should be amended to incorporate medium on how to authenticate an internet public device to ease the admissibility of electronically generated evidence in our court system. There is a need to reconsider the prohibitive aspects of our laws. The inadequacy of our legislation turns out to be even more serious when we consider the lack of analogy between most cyber crimes and their conventional network. There is a need to develop a comprehensive internet legislation to regulate electronic financial transactions and prevent electronic crimes. As long as there is an absence of a centralised electronic databank containing specific information on each individual resident and visitor to Nigeria, exposure of criminal intentions before they are executed and the effective investigation of crimes committed would continue to pose a serious challenge to security agencies.

2) We also called for legislative reforms and amendment of legislation in combating cybercrime and full harmonization with international legislation in order for legislation on cyber crime in Nigeria to keep

pace with e-crime, especially as it becomes more prevalent and sophisticated hence there is the need to develop a common platform to address cyber security since cybercrime crosses borders and cannot be fought by one country. There is need for the National Assembly to amend the cybercrime Act by inserting a provision prescribing punishment under section 7 that relates to operation of cybercafés to make effective and efficient, the law making body should also expedite action to pass necessary Bills, that could help in curbing internet related crimes including the Economic and Financial Crimes Commission Act (Amendment) Bill 2010, Electronic Transactions Bill, 2015 and Payment System Management Bill 2015 all these are yet to become law and it relates to Cybercrimes.

3) Lastly, it is further, recommended that in order to advance the knowledge for applicable laws, the protection of privacy right and intellectual property, with intent to sensibilize the methods and measures to prevent and combat the cybercrimes, there is a need to organize media debates, workshops and seminars with organizations for security and civil society. Education is the most vital weapon for literacy, as such seminars and workshops should be organized from time to time with emphasis on cyber safety so that the individuals, law enforcement agencies and service providers, will learn to keep their personal and customer information safe cybercrime criminals. We therefore, recommends that curriculum which will include courses on cyber crime, cyber management and its prevention should be introduced to both tertiary and secondary schools to take care of the

present social changes. The internet services providers should not just provide broadband connection to their subscribers especially the home users, but they should also monitor effectively what the subscribers are doing on the net, at what time and where. They should provide their customers, especially financial institutions and cyber cafes with well-guided security codes and packages in order to protect their information and soft ware from hackers and publishers.

BIBILIOGRAPHY

TEXT BOOKS

1. Afe Babalola, Law and Practice of Evidence in Nigeria, p. 262
2. Ladan M.T, (2015) Cyberlaw and Policy on Information and Communications Technology in Nigeria Ahmadu Bello University Press Limited p 104.

JOURNALS

3. Agba P.C., (2003) International Communication Principles, Concepts and Issues: In Okunna C.S. (ed) Techniques of Mass Communication: A multi – Dimensional Approach. Enugu: New Generation Books p.9
4. Ehimen O.R & Bola A., (2010) "Cybercrimes in Nigeria*" Business Intelligence Journal*, January, Vol.3, No.1 p.95
5. Folashade B.O. etal, (2013) The Nature, Causes and Consequence of Cyber Crime in Tertiary institution in Zaria-Kaduna state, American International Journal of Contemporary Research, Vol. 3, No. 9, September, p.98
6. Ibikunle F., (2013) Approach to Cyber Security Issues in Nigeria: Challenges and Solution, Publication of Department of Electrical & Information Engineering, Covenant University Nigeria, Vol,1 No1 p1.
7. Longe, O.B & Longe, F.A. (2005). The Nigerian Web Content: *Combating the Pornographic Malaise Using Web Filters. Journal of Information Technology Impact*. Vol. 5, No. 2 Loyola University, United States of America. www.jiti.net
8. Longe, O.B.& Chiemeke, S.C. (2008): Cybercrime and Criminality in Nigeria- *What roles are internet Access Points in Playing. European Journal of Social Sciences,* Volume 6 No 4.

9. Longe, O.B.& Chiemeke, S.C. (2008): Cybercrime and Criminality in Nigeria- *What roles are internet Access Points in Playing. European Journal of Social Sciences,* Volume 6 No 4.
10. Longe,O.B, Mbarika, V, Kourouma, M, Wada, F & Isabalija, R., (2009) Seeing Beyond the Surface: Understanding and Tracking Fraudulent Cyber Activities. *International Journal of Computer Science and Information Security*. Vol. 6 (3) pp. 124-135.
11. Mu'azu A.S & Abubakar M.K., (2014) Cybercrime in Nigeria:*An Overview of Cybercrime Act 2013, Journal of Law, Policy and Globalization*, ISSN 2224-3240 (Paper) ISSN 2224 – 3259 (Online) Vol.32, p.23
12. Nfor, E. S. and Maimusa, H. (2007) "Nigerian National Security and the Challenges of Globalization 1999-2006", M*aiduguri Journal of Peace and Development Studies*, 1, (2), July-December, p. 80.
13. Okeshola F.B & Adeta A.K., (2013) The Nature, Cause and Consequences of Cybercrime in tertiary Institution in Zaria , Kaduna State, American International Journal of Contemporary Research, Vol3. No9, September P1.
14. Okpaga, A. (2007) "Enhancing National Security in Nigeria through Non-Military Perspectives" in Dada, J. P. and Adejo, A. M. (Ed) *Opcit*, p. 84
15. Olanipekun O., (2015) Cybercrimes in the Banking Sector: Facing the new wave of criminals legally p 16
16. Olayemi O.J., (2014) A Socio – Technological Analysis of Cybercrime and Cyber security in Nigeria, International Journal of Sociology and Anthropology Vol 6 (3) March, p.117 Http://www.academic journals.org/ijsa accessed on 03/08/15 at 04:34 pm.

17. Osborn H.Q., e tal, .(2012) Fighting Cybercrime in Africa; *Computer science and Engineering*, 2(6) 118-100 Doi 1-.5923/j computer20/20206.03. p.2 Published online at:http://Journalsapub.org/computer.scientific&Academic publishing 2012.
18. 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.
19. Selma Dilek, e,tal (2015) applications of artificial intelligence techniques to combating cyber crimes: a review, *International Journal of Artificial Intelligence & Applications* (IJAIA), Vol. 6, No. 1, January P.2.
20. Shinder, D.L., (2002) Scene of the Cyber Crime; Computer Forensics handbook, Syngress Publishing Inc. 88 Hingham street, USA. p.1
21. Wada F. & Oduloja G.O., (2012) E-banking and Cybercrime in Nigeria: A Theoretical Policy Perspective on Causation, Afr J. of Comp & ICTs, Vol5, No1 P69.

UNPUBLISHED CONFERENCE/SEMINARS PAPER

22. Chiesa, R., (2011). 'Auditing the Hacker's Mind: The Hacker's Profiling Project. A Presentation by Chiesa Raoul at WINS International Best Practice Conference, Vienna, Austria.
23. Collin, B.C. (1996) The Future of Cyber Terrorism: Where the Physical and Virtual Worlds Converge, 11th Annul International Symposium on Criminal Justice Issues
24. Dasgupta D., (2006) "Computational Intelligence in Cyber Security", IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety (CIHSPS 2006), pp. 2–3

25. Ladan M.T., (2015) Overview of the 2015 Legal and Policy Strategy on Cybercrime and Cybersecurity in Nigeria, M.T Ladan's Law and Policy Review Research working Paper, May – August, p.10.
26. Longe, O.B & Chiemeke, S.C.(2007). Beyond Web Intermediaries: Framework for Protecting Web Contents on Clients Systems. Paper Presented at the International Conference of the International Association of Engineers (IAENG) Imperial
27. Ribadu, E. , (2007) Cyber Crime and Commercial Fraud; A Nigerian Perspective; A Paper Presented at the Modern Law for Global Commerce, Vienna, 9th -12th July,

INTERNET

28. Anah, B.H., Funmi, D.L., & Julius, M., (2012) Cyber Crime in Nigeria: Causes, effects and the way out. ARPN Journal of Science and Technology, 2 (8) 626, http:/www.ejournalofscience.org
29. Brenner,(2004) Cybercrime Metrics: Old Wine Bottles? Virginia Journal of Law and Technology Vol.9, available at www.vjolt.net/Vol9/issue4/v9i4 - a13 - Brenner.pdf.
30. Chawki, M.(2009) Nigeria tackles Advance Fee Fraud*; in Journal of Information, Law and Technology* (JILT), May 28, 2009. Accessed from http://go.warwick.ac.uk/jilt/2009-/chawki on 9/7/2016, p.13
31. Forest, J. J. F. (2012). Confronting the Terrorism of Boko Haram in Nigeria. Retrieved on October 24, *2013 from http://www.jamesforest.com/wp-content/uploads/2012/06/Boko_Haram_JSOU-Report-2012.pdf*

32. Gillespie A., (2007) Cybercrime: *Key Issues and Debates* (Routledge 2016) Chapter 1; I Walden, *Computer Crimes and Digital Investigations* (Oxford University Press).

33. Giordano/Maciag, (2005) Cyber Forensics: *A Military Operations Perspective, International Journal* of Digital Evidence,Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04843F3-99E5-632BFF420389C0633B1B. pdf ; *Reith*, An Examination of Digital Forensic Models, International Journal of Digital Evidence,Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, Vol. 119, page 531.

34. Gordon/Ford, On the Definition and Classification of Cybercrime, *Journal in Computer Virology*, Vol. 2, No. 1, 2006, page 13-20; *Chawki*, Cybercrime in France: An Overview, 2005, available at: www.crimeresearch. org/articles/cybercrime-in-france-overview;

35. Kaspersen Henrik W.K., Cybercrime and internet jurisdiction *Vrrje Universiteit* Amsterdam, Economic crime Division, Directorate General of Human Rights and Legal Affairs, Strasbourg, France Version 5 March (2009) p.12 available at: www.coe.int/cybercrime.

36. Laura A.(2015) Cybercrime and National Security; *the role of the penal and procedural Law,* Research Fellow, Nigerian Institute of Advance Legal Studies p.7. Accessed from http://nials-nigeria.org/pub/lauraani.pdf. On 4/8/15 at 9:45am

37. Lunker Manish : *Cyber Laws: A Global Perspective pg. 2(An article from Internet)*

*See*http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN005

846.pdf.Accessed on; 22 November 2015.

21:52:15.http://www.rediff.com/netguide/index.html accessed on 01.12.2015.

38. Maitanmi Olusola et tal, 'Impact of Cyber Crimes on Nigerian Economy*', the International Journal of Engineering and Sciences (*IJES) Volume 2, Issue 4, p. 47. ISSN 2319-1813. Available at http://www.theijes.com/papers/v2i4/part.%20%284%29/H0244045051.pdf. Accessed on 23/12/2015.
39. Meke E.S.N. (2012), Urbanization and cybercrime in Nigeria : Causes and Consequences: ARPN Journal of Science and Technology , 2 (8) 631, http:/www.ejournalofscience.org.
40. Nojeim, G.T. (2009), Cybersecurity: *Preventing Terrorist Attacks and Protecting Privacy in Cyberspace. Statement Before the Senate Committee on the Judiciary, Subcommittee on Terrorism and Homeland Security.* Oxford Dictionaries (2013, June) online available *at http://oxforddictionaries.com*.www.itu.int/en/ITUT/studygroups/com17/pages/cybersecurity.aspx. accessed on 19/12/2015 at 2:04pm.
41. Olugbodi, K., Fighting Cyber Crime in Nigeria, retrieved 10/08/15 from http//:www.guidenigeria.com/news_articles_about_nigeria, by 5 :35pm
42. Oyesanya., (2025) F. A performance Review of EFCC and the Nigerian Cybercrimes Working Group.' Accessed from http://www.nigeriavillagesquare.com/article/femi-oyesanya/...html on June 6, 2015, p.3
43. Oyesanya., (2025) F. A performance Review of EFCC and the Nigerian Cybercrimes Working Group.' Accessed from

http://www.nigeriavillagesquare.com/article/femi-oyesanya/...html on June 6, 2015, p.3

44. Smith, R.G., Holmes, M.N. & Kaufmann, P. (1999): Nigerian advance fee fraud. *Trends and Issues in Crime and Criminal Justice,* No. 121. Australian Institute of Criminology, Canberra. Available online at *http://www.aic.gov.au* accessed on 20/12/15 at 10:00am.

NEWSPAPERS

45. Abdullahi, T. A., Hamza, I., Yahaya, I., Hamisu, K. M., and Zakariyya, A (2013). *"Cell phone service cut in Borno, Yobe",* Daily Trust Newspaper, May 17, 2013.
46. Adeyemi, K., Joel, D., Tsenzughul, A. (2012). Gunmen Attack MTN, Airtel masts in Kano, Borno, Bauchi, Yobe. The Nation Newspaper. Retrieved September 6, 2012. Retrieved from http://www.thenationonlineng.net/2011/news/60494-gunmen-attack-mtn-airtel-masts-in-kano-borno-bauchi-yobe.html, published in September, 2012.
47. Ahmed, I. (2008) Nigeria: N10 Billion Lost to Bank Fraud in 2007 – *NDIC, Daily Trust,* 28 October 2008
48. Daily Champion Newspaper*, "Nigeria: Representatives Reject Cyber Bill."* Retrieved fromhttp://allafrica.com/stories/201103020802.html, published on March 2, 2011.
49. Muhammed, H., (2009) 'NCC Clamps down on Illegal ISPs, Cyber Cafes, '*Daily Trust*. Monday, February 23, *pp.55*
50. Swire, Peter & Hemmings, Justin. (2015) "Re-Engineering the Mutual Legal Assistance Treaty Process," presented at *Berkeley Center for Law and Technology Privacy Law Scholars Conference*, p. 11.

51. This Day Newspaper, “Non-Passage of Cyber Crime Bill Decried.” Retrieved *fromhttp://www.thisdaylive.com/articles/non-passage*-of-c*yber-crime-bill-decried/88750/, published on March 31, 2011.*

DICTIONARY

52. Garner A. B., (2009) Black’s Law Dictionary 8th ed. p 414.

53. Oxford Dictionary www.oxforddictionaries.com/definition/english/telencies