

**THE LEGAL REGIME OF CYBER SECURITY AND CRIME: ROLE OF LAW  
ENFORCEMENT AGENCIES INNIGERIA**

**BY**

**Sunday Samuel TOKURA  
PhD/LAW/01306/2009-2010**

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

**DEPARTMENT OF PUBLIC LAW  
FACULTY OF LAW  
AHMADU BELLO UNIVERSITY, ZARIA  
NIGERIA**

**DECEMBER, 2016**

## **DECLARATION**

I declare that the work in this thesis titled: **The Legal Regime of Cyber Security and Crime: Role of Law Enforcement Agencies in Nigeria** has been carried out by me in the Faculty of Law. The information derived from the literature has been duly acknowledged in the text and a list of references provided. No part of this dissertation was previously presented for another degree or diploma at this or any other institution.

**Sunday Samuel TOKURA**

\_\_\_\_\_  
**Signature**

\_\_\_\_\_  
**Date**

## CERTIFICATION

This thesis titled: **THE LEGAL REGIME OF CYBER SECURITY AND CRIME: ROLE OF LAW ENFORCEMENT AGENCIES IN NIGERIA** by Sunday Samuel TOKURA meets the regulations governing the award of the degree of Doctor of Philosophy-PhD of the Ahmadu Bello University, and is approved for its contribution to knowledge and literary presentation.

**Prof. M. T. Ladan**  
Chairman, Supervisory Committee

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

**Prof. J.A.M. Audi**  
Member, Supervisory Committee

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

**Dr. I.F. Akande**  
Member, Supervisory Committee

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

**Dr. K.M. Danladi**  
Head, Public Law Department

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

**Prof. S. Z. Abubakar**  
Dean, School of Postgraduate Studies

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

## **DEDICATION**

This work is dedicated to the entire Tokura Family.

## ACKNOWLEDGEMENTS

I am grateful to most of all, our heavenly father, Jesus Christ, for giving me the grace, wisdom and understanding with which I pursued this research and granting me journey mercies to and from my base in Lagos and my school in Zaria, all through the several trips that I made by air and in the high ways that can best be described as the valley of the shadow of death. I bless Him and give praises and honour to His Holy name.

I am highly grateful to my indefatigable supervisory committee with Professor M.T. Ladan as the Chairman, who, in spite of his tight schedule, still found the time to examine this thesis. I really cannot thank him enough.

My appreciation goes to Dr. I.F. Akande, a very visible member of the supervisory committee for her patience and professional guidance at every point that I seemed to be going off track. I thank you Ma.

I remember the kind advice of Professor. J.A.M. Audi also a member of the supervisory committee in the early stage of this thesis that I should always endeavor to read through the chapters one more time before I submit for assessment in order to minimize the errors, I must confess that it was very helpful. I am very grateful Ma.

My unalloyed gratitude goes to my lovely wife, Mrs. Olukemi Fenellia Tokura for her tolerance of my absence from home so many times within the period of this research. Her suggestions and input at some knotty stages of this thesis turned out to be of immense benefit to this research. She is a gracious woman and God bless the day I found her.

I wish to thank the lecturers in the Faculty of Law some of whom were my lecturers since my undergraduate days in this institution. I am humbled and feel honoured that

notwithstanding the distance between us, they still count me worthy as a friend and a brother. I thank you sirs.

Finally, I thank my institution, the prestigious, first generation Ahmadu Bello University Zaria for giving me the opportunity to carry out this research as a student of this revered citadel of learning.

## TABLE OF CASES

Anyaebosi v.R.T Briscoe Ltd (1997) 3 NWLR pt.59 at 84	-	-	-	-	-	-	-	-	280
Amaechi v I NEC (2009) 4 EPR 117	-	-	-	-	-	-	-	-	339
Campania NavieraVascongado v Steamship Cristina (1938) AC, 485	-	-	-	-	-	-	-	-	67
Couch v United States 409 U.S 322, 333 & n.16 (1973) -	-	-	-	-	-	-	-	-	306
Doe v United State 487, U.S. n.a. (1998) -	-	-	-	-	-	-	-	-	306
Ehuwa v OSIEC (2006) 18 NWLR (Pt. 1012) 544 at 568	-	-	-	-	-	-	-	-	339
Ehuwa v INEC (2006) 28 NSCQR 551	-	-	-	-	-	-	-	-	339
Equal opportunity Empl. Comm. v Arabian American Oil Co. (1991) 499 U.S 244,248	-	-	-	-	-	-	-	-	245
FRN v Dr. Bello Muhammad Shallah and another (unreported) Suit no. ZMS/GS/ZC/10	-	-	-	-	-	-	-	-	183
Katz v United States, 389 U.S. 347 (1967)	-	-	-	-	-	-	-	-	320
Miranda v Arizona, 384 U.S. 436 (1996) -	-	-	-	-	-	-	-	-	306
OgolovIMB (Nig) Ltd (1995) 9 NWLR pt. 7 at 317	-	-	-	-	-	-	-	-	280
Oregon v Elstad, 470 U.S. 298, 306 (1985)	-	-	-	-	-	-	-	-	306
R.v Fellow, R.v Arnold (1997) 2 All ER 548	-	-	-	-	-	-	-	-	289
Reno vAmerican Civil Liberties Union 117 Sct. 2329, 2344 (1997)	-	-	-	-	-	-	-	-	302
State vOloketuyi (unreported) FHC/L/346C/15	-	-	-	-	-	-	-	-	184
United States of America vRobert A. Thomas as and Carleen Thomas (1996) 74F. 3d 701, 1996 US. App Lexis 1069, 1996 Fed, App 0032p (6 <sup>th</sup> Cir)	-	-	-	-	-	-	-	-	289
United State vCotton (1973) 471 F. 2 d 744, 750 (9 <sup>th</sup> Cir)	-	-	-	-	-	-	-	-	245
United States vMuench 694 F. 2d 28, 33 (2d Cir) (1982) 694 F.2d 28, 33 (2d cir)-	-	-	-	-	-	-	-	-	246
United States vGuterma, 272f. 2d 344 (2d Cir. 1959)	-	-	-	-	-	-	-	-	306
Wong Sun vUnited States 371 U.S.471 (1963)	-	-	-	-	-	-	-	-	307

## TABLE OF STATUTES

Advance Fee Fraud and Other Related Offences Act, Cap. A6 L.F.N 2004 as amended in 2006 - - - - -	146, 149
African Charter on Human and People’s Rights Adopted in Nairobi June 27, 1981 Entered into force October 21, 1986 - - - - -	212
American Convention on Human Rights. Signed 22 November 1969. Effective: 18 July 1978 - - - - -	209, 212, 215, 218,
Anti Corruption Act, (1999) as amended in (2000) - - - - -	144
The General Assembly of INTERPOL Article 1. adopted the Global Standards in 2002 by its resolution AG-2002-RES-01 at its 71st session in Yaoundé -	285
Lima Declaration, Article 26 (The 6 <sup>th</sup> APEC Ministerial Meeting on the Telecommunications and Information Industry) (TELMING) - -	115
INTERPOL Global Standards, Articles 4.14-4.17 - - - - -	231
Banks and Other Financial Institution Act. (BOFIA)1999 - - - - -	144
General Assembly Resolution 47/133, Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment, the Standard Minimum Rules for the Treatment of Prisoners and the Declaration on the Protection of All Persons from Enforced Disappearance - - - - -	229
United Nation Convention on Bribery of Foreign Public Official in International Business Transactions of 1997 - - - - -	230
California Penal Code,(Section. 502) - - - - -	58
Central Bank of Nigeria Act, (2007) - - - - -	144
Council of Europe Convention on Cybercrime, 2001 - - - - -	5
Child Rights Act, Cap N30 LFN 2004 - - - - -	12
United Nation General Assembly in its Resolution 34/169, Code of Conduct for Law Enforcement Officials - - - - -	221
Computer Fraud and Abuse Act, (USA) 1986 - - - - -	141, 142
Computer Misuse Act, U.K. (1990) - - - - -	132, 133, 288

Constitution of the Federal Republic of Nigeria, 1999 as amended	-	-	196, 302
Constitution of United States of America	-	-	302
UN Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (United Nations, Treaty Series, Vol.1465, No.24841	-	-	221
Convention on Cybercrime Budapest,23.x1, 2001	-	-	165
Convention on the Elimination of All Forms of Discrimination Against Women. (CEDAW) adopted in 1979 by UN	-	-	220
Council of Europe(COE'S), Recommendation No R (81) 20 of the committee of ministers on the Harmonization of laws Relating to the Requirement of written proof and To the Admissibility of Reproductions of Documents And Recordings on Computers(Council of Europe, <i>European Treaty Series</i> , No. 126), Art. 1. More information on the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment is available from <a href="http://www.cpt.coe.int">www.cpt.coe.int</a> .Retrived, December 12, 2014.	-	-	280
Council of Europe Convention for the Protection of Human Right and Fundamental Freedoms (1950)	-	-	90
Council of Europe Convention on Cybercrime, <i>Chart of Signatures and Ratifications</i> , Retrieved June 13, 2015 from <a href="http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&amp;CM=&amp;DF=&amp;CL=ENG">http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&amp;CM=&amp;DF=&amp;CL=ENG</a> .	-	-	250
Council of Europe, (Nov. 8, 2001), C.E.T.S. No. 185, Convention on Cybercrime: Explanatory Report, para. 38. Retrieved December 12, 2014 from <a href="http://conventions.coe.int/Treaty/en/Reports/Html/185.htm">http://conventions.coe.int/Treaty/en/Reports/Html/185.htm</a>	-	-	241
Council of Europe, Recommendation Rec. (2001)10 of the Committee of Ministers to member States on the European Code of Police Ethics, adopted by the Committee of Ministers on 19 September 2001	-	-	205
Council of Europe, Treaty Office	-	-	88
Council of Europe's Convention on Cybercrime Vienna Convention (2001)-			99
Criminal Code Act Cap. C38 Laws of the Federation (LFN) 2004 applicable with few modification in all southern States of Nigeria	-	-	144
Criminal Justice (Miscellaneous Provision) Act, Cap C39, LFN 2004 and the Criminal Procedure Code	-	-	24

Criminal Procedure Act, Cap C41, LFN 2004	-	-	-	-	24
Criminal Procedure Code Operational in the North of Nigeria	-	-	-	-	24
Cybercrime (Prohibition Prevention Etc) Act, 2015	-	-	-	-	7, 22, 33, 184
Economic and Financial Crimes Commission Act, Cap. E1 L.F.N. 2004	-	-	-	-	146
Effective Implementation of the Code of Conduct for Law Enforcement officials adopted by Resolution of 34/169 of the U.N General Assembly on 17th December, 1979	-	-	-	-	224
European Commission Initiative on Combating sexual Exploitation of Children and Child Pornography December 2011	-	-	-	-	96
European Convention on Human Rights, Article 10	-	-	-	-	304
European Convention on Mutual Assistance in Criminal Matters. (1959)	-	-	-	-	89
Evidence Act Cap.E18, LFN 2004, Effectively repealed by Evidence Act, 2011-	-	-	-	-	24
Failed Bank (Recovery of Debt and Financial Malpractice in Bank) Act, No.18 (1994)	-	-	-	-	144
Human Rights and Humanitarian Law for Police and Security Forces (Geneva, International Committee of the Red Cross, 1998) (Cees de Rover, To Serve and to Protect)-	-	-	-	-	205
Independent and Corrupt Practices and other Related Offences Commission Act, 2000	-	-	-	-	150
Inter American Convention Against Corruption of 1996	-	-	-	-	231
International Code of Conduct for Public Officials. January 28, 1997	-	-	-	-	206
International Committee of Red Cross (ICRC) Geneva, (1998) To Serve and To Protect-	-	-	-	-	198, 201, 202
International Convention on the Elimination of all Forms of Racial Discrimination. New York, 7 March 1966	-	-	-	-	220
International Covenant on Civil and Political Rights	-	-	-	-	220
International Strategy for Cyberspace, White house 5 (May, 2011)	-	-	-	-	251

Money Laundry Act, 2011 Cap. M118 LFN 2004, as amended	-	-	144
National Cybersecurity Policy, 2015	-	-	165
National Drugs Law Enforcement Agency (NDLEA) , No 48 (1989)	-		144
National Identity Management Commission Act, No. 23, 2007, (NIMC)	-		149
National Information Technology Development Agency Act, 2007	-		153
Nigerian National Policy for Information Technology, (NPFIT )2001	-		155
OECD Anti-Bribery Convention: National Implementing Legislation, OECD-			249
Organisation for Economic Cooperation and Development Convention on Combating	-	-	71
Penal Code Law Cap.89 Laws of Northern Nigeria 1963 applicable in all Northern States and F.C.T subject to few modifications	-	-	144
Recommendation No R (85) 10 on Letters Rogatory for the Interception of Telecommunications	-	-	280
Recommendation No. R (87) 15 Regulating TheUse of Personal Data in The Police State	-	-	280
Recommendation No. R (89) 9 on Computer- Related Crime	-	-	280
Terrorism (Prevention) Act, 2012	-	-	152
Texas Penal Code	-	-	57
The European Code of Police Ethics	-	-	234
The Torture Convention 1987 (United Nations Declarative and Convention Against Torture)	-	-	257
U.K Data Protection Act, 1998	-	-	319
U.K Financial Services and Market Act, 2000	-	-	320
U.K. Cyber Security Strategy	-	-	191
U.N. Doc A/46/ 654	-	-	163
U.N. Doc. A/65/201 (July 30, 2010)	-	-	238

U.N. DOC. A/RES/49/60	-	-	-	-	-	-	-	163
U.N. DOC. A/RES/50/53	-	-	-	-	-	-	-	163
U.N. Doc. A/RES/60/252 (Apr. 27, 2006)	-	-	-	-	-	-	-	237
U.N. DOC. S/RES/1189 Press Release GA/L/3103 (1998)	-	-	-	-	-	-	-	163
U.N. Economic and Social Council Resolution 1989/61, annex	-	-	-	-	-	-	-	224
U.N. G.A. Res. 57/53, U.N. Doc. A/RES/57/53 (Dec. 30, 2002).	-	-	-	-	-	-	-	237
U.N.G.A. Res. 58/32, <i>at p.4</i> ; G.A. Res. 59/61	-	-	-	-	-	-	-	236
U.N. G.A. Res. 58/32, U.N. Doc. A/RES/58/32 (Dec. 8, 2003);	-	-	-	-	-	-	-	236
U.N. G.A. Res. 60/252	-	-	-	-	-	-	-	237
U.N. G.A. Res. 62/17	-	-	-	-	-	-	-	236
U.N. G.A. Res. 64/211, U.N. Doc. No. A/RES/64/211 (Mar. 17, 2010)	-	-	-	-	-	-	-	237
U.N. General Assembly Resolution 51/59, annex	-	-	-	-	-	-	-	225
U.N. Sec. Council Res. 1189, 13, Aug. 1998	-	-	-	-	-	-	-	163
U.N.Doc. A/RES/51/210: Accord	-	-	-	-	-	-	-	163
U.N.G.A. Res. 51/210, Jan. 16, 1997-	-	-	-	-	-	-	-	163
U.N.G.A. Res. 46/51; 9, Dec. 1991	-	-	-	-	-	-	-	163
U.N.G.A. Res. 49/60; 9, Dec. 1994	-	-	-	-	-	-	-	163
U.N.G.A. Res. 50/53, 11, Dec. 1995-	-	-	-	-	-	-	-	163
U.N.G.A. Res. 58/199, U.N. Doc. No. A/RES/58/199 (Jan. 30, 2004)	-	-	-	-	-	-	-	237
U.N.G.A. Res. 59/61, U.N. Doc. A/RES/59/61 (Dec. 3, 2004)	-	-	-	-	-	-	-	236
U.N.G.A. Res. 60/45	-	-	-	-	-	-	-	163
U.N.G.A. Res. 60/45, U.N. Doc. A/RES/60/45 (Jan. 6, 2006)	-	-	-	-	-	-	-	236
U.N.G.A. Res. 61/54, U.N. Doc. A/RES/61/54 (Dec. 19, 2006)	-	-	-	-	-	-	-	236
U.N.G.A. Res. 62/17, U.N. Doc. A/RES/62/17 (Jan. 8, 2008)	-	-	-	-	-	-	-	236

U.N.G.A. Res. 63/37, U.N. Doc. A/RES/63/37 (Jan. 9, 2009)	-	-	236
U.N.G.A. Res. 64/25, U.N. Doc. A/RES/64/25 (Jan. 14, 2010)	-	-	236
U.S Patriot Act, 2001	-	-	320
U.S.A, Police and Justice Act, 2006	-	-	138
U.S.A. National Security Strategy	-	-	190
UEMOA Treaty of 29 January 2003	-	-	131
U.N. Standard Minimum Rules for the Administration of Juvenile Justice (Beijing Rules)	-	-	213
UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials (Basic Principles 9,10 and 11)	-	-	217
UN Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment (Principles 2, 8,10, 11, 12, 20 and 29),	-	-	210
UN Code of Conduct for Law Enforcement Officials (Article 3), UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials (Principles 4, 5, 6 and 9)	-	-	188, 221
UN Code of Conduct for Law Enforcement Officials (Article 5)	-	-	188, 221
UN Code of Conduct for Law Enforcement Officials (Preamble and Articles 1, 2, 8)	-	-	222
UN Convention on the Rights of the Child (Article 1)	-	-	97
UN Declaration on the Protection of All Persons from Enforced Disappearances (Preamble and Article 6)	-	-	229
UN International Covenant on Civil and Political Rights (Article 10)	-	-	90
UN Standard Minimum Rules for the Treatment of Prisoners (Rule 55)	-	-	227
United Nations Convention on Cybercrime (2001)	-	-	5
United Nations Criminal Justice Standards for United Nations Police	-	-	220
United Nations Declaration of Human Rights 1948	-	-	257

United Nations General Assembly Resolution 55/63 of 2000	-	-	116
United Nations International Covenant on Civil and Political Rights (1966)-			90, 100, 199
United Nations Rules for the Treatment of Women Prisoners and Non-Custodial Measures for Women Offenders	-	-	227
United Nations, <i>Treaty Series</i> , vol. 1249, No. 20378-	-	-	220
Universal Declaration of Human Rights, arts. 19 and 29,(1948)	-	-	209
USA, Fraud and Related Activity in Connection with Computers(Section,1030)-			142
USA, Transportation of Stolen Goods, Securities, Money, Fraudulent State Tax Stampor Articles used in Counterfeiting (Section.2314)	-	-	142

## **ABBREVIATIONS**

APEC	-	Asia Pacific Economic Cooperation
ASEAN	-	Association of Southeast Asian Nations
AU	-	African Union
ACPO	-	Association of Chief Police Officers
AHTCC	-	Australian High Tech Crime Centre
AISI	-	African Information Society Initiative
AMU	-	Arab Maghreb Union
ATU	-	African Telecommunication Union
AICTO	-	Arab Information and Communication Technologies Organization
AREGNET	-	Arab Regulators Network
AGF	-	Attorney General of the Federation n
APCOF	-	African Policing Civilian Oversight Forum
AIGs	-	Assistant Inspector General of Police
BOFIA	-	Bank and Other Financial Institution Act
BUMA	-	Collecting Society for Performing Rights in Musical Works of (Netherlands)
BSA	-	Business Software Alliance
BCR	-	Binding Corporation Rules
C.As	-	Certificate Authorities
C.E.O	-	Chief Executive Officer
CSI	-	Computer Security Institute
COE	-	Council of Europe
EU	-	European Union

COMESA	-	Common Market for Eastern and Southern African
CMA	-	Computer Misuse Act 1990 (U.K)
CCCL	-	Computer Crime and Cyber Laws
CIB	-	Central Intelligence Bureau
CN-CERT	-	China's Computer Emergency Response Team
CDA	-	Communication Decency Act
CD	-	Compact Drive
CSP	-	Cloud Services Provider
DNS	-	Dormain Name System
DOJ	-	Department of Justice (USA)
DSS	-	Department of State Services
DNCR	-	Department for National Civic Registration
DIA	-	Defence Intelligence Agency
DMI	-	Directorate of Military Intelligence
DPO	-	Divisional Police Officer
DHS	-	Department of Homeland Security
DOD	-	Department of Defense
DNA:	-	Deoxyribonucleic Acid
DPA	-	Data Protection Act
ECA	-	Economic Commission for Africa
EFCC	-	Economic and Financial Crime Commission
EU	-	European Union

RESEPTIS	-	Research and Innovation on Security, Privacy and Trustworthiness in the Information Society
ECOWAS	-	Economic Community for West African States
EAC	-	East African Community
ECCAS	-	Central African Economic Community
EMERG	-	Euro-Mediterranean Regulators Group
EEA	-	National Registration Certificate Number for U.K/EU Members
FBI	-	Federal Bureau of Investigation
FNC	-	Federal Networking Council
FRATEL	-	Francophone Telecommunications Regulatory Network
FRSC	-	Federal Road Safety Corps
FIRS	-	Federal Inland Revenue Service
FRN	-	Federal Republic of Nigeria
FTC	-	Federal Trade Commission
FSMA	-	Financial Services and Markets Act
FCMA	-	Financial Services Modernization act
GCA	-	Global Cybercrime Agenda
GUI	-	Graphics User Interface
AAA	-	Affordability, Accessibility and Anonymity
GPEN	-	Global Prosecutors E-crimes Network
CPS	-	United kingdom Crown Prosecution Services.
GILC	-	Global Internet Liberty Campaign
GRECO	-	Group of States Against Corruption

HLEG	-	High- Level Experts Group
HMRC	-	Her Majesty Revenue and Customs
HIPPA	-	Health Insurance Portability and Accountability Act
ITU	-	International Communication Union
ICTs	-	Internet Communication Technology
ITCA	-	Information Technology Centre for Africa
IT	-	Information Technology
ICPC	-	Independent and Corrupt Practices and Other Related Offences Commission
ISP	-	Internet Service Provider
IP	-	Internet Provider
ISDN	-	Integrated Services Digital Network
IDs	-	Users Identities
IGC	-	Institute for Global Communications
IACP	-	International Association of Chiefs of Police
IRC	-	Internet Relay Chat
IAP	-	International Association of Prosecution
INTERPOL	-	International Police Organisaton
ISDN	-	Integrated Services Digital Network
ISOC	-	Internet Society
IGAD	-	Inter-Governmental Authority on Development
ID	-	Use-name or Identifier
ISPAN	-	Internet Services Providers Association of Nigeria

INEC	-	Independent National Electoral Commission
ICRC	-	International Committee of the Red Cross
ICCPR	-	International Covenant on Civil and Political Rights
ICANN	-	Internet Corporation for Assigned Names and Numbers.
ISO	-	International Standard organization
IDC	-	International Data Corporation
ICO	-	Information Commissioners office
LEAs	-	Law Enforcement Agencies
MLATs	-	Mutual Legal Assistant Treaty
MUD	-	Multiple User Dimension, Multiple User Dungeon or Multiple User Dialogue
MS-ISAC	-	Multi-State Information Sharing and Analysis Center
NCSS	-	National Cybersecurity Strategy
NCSR	-	National Cybersecurity Research
NPFIT	-	National Policy For Information Technology
NCTP	-	National Cybercrime Training Partnership
NGOs	-	None Governmental Organisation
NATO	-	North Atlantic Treaty Organisation
NECC	-	National Electronics Commerce Council
NCAFF	-	National Committee on Advance Fee Fraud
NPF	-	Nigeria Police Force
NSA	-	National Security Adviser
NCC	-	Nigerian Communication Commission
NCS	-	Nigeria Computer Society

NIG	-	Nigeria Internet Group
NIMC	-	National Identity Management Commission
NID	-	National Identity Database
NASS	-	National Assembly
NPC	-	National Population Commission
NEPAD	-	New Partnership For Africa's Development
NICI	-	National Information and Communication Infrastructure
NIN	-	National Identification Number
NCWG	-	Nigeria Cybercrime working Group
NIA	-	National Intelligence Agency
NITDA	-	National Information Development Agency
NDLEA	-	National Drug Law Enforcement Agency
NAPTIC	-	National Agency for Prohibition of Traffic In persons
NACA	-	National Agency for the Control of Aids
NAFDAC	-	National Agency for Food and Drugs Administration and Control
NCC	-	National Communication Commission
NPFIT	-	Nigerian National Policy for Information Technology
NCFTA	-	National Cyber forensic and Training Alliances
NASDAQ	-	National Association of Security Dealers Automated Quotation
NFIB	-	National Fraud Intelligence Bureau
O.A.U	-	Organisation of African Unity
O. E.C.D	-	Organisation for Economic Cooperation and Development
O. A.S	-	Organisation of American States

O.F.T	-	Office of Fair Trading
O I F	-	Organisation Internationale de la Francophonie
ONSA	-	Office of the National Security Adviser
OSIEC	-	Ondo State Independent Electoral Commission
PCs	-	Personal Computers
PCeu	-	United Kingdom Metropolitan Police Central e-Crime Unit
PTT	-	Push to Talk
QAKBOT	-	A Multi-Component Worm/Trojan Malware
REMJA	-	Ministers of Justice or of the Ministers or Attorneys General of the Americas
RISDP	-	Regional Indicative Strategic Development Plan
RIDMP	-	Regional Infrastructure Development Master Plan
RCMP	-	Royal Canadian Mounted Police
S.S.S.	-	State Security Service
S.O.C.A	-	Serious Organised Crime Agency
SSA	-	Sub Sahara Africa
SCO	-	Shanghai Cooperation Organisation
SACCWG	-	Strategic Alliance Cybercrime Working Group
SADC	-	Southern African Development Community
SEC	-	Security and exchange Commission
SCC	-	Standard Contractual Clauses
TOR	-	Term of Reference
TEMPEST	-	Transient Electromagnetic Pulse Emanation Standard
TCP	-	Transmission Control Protocol

TRIPS	-	Trade Related Aspect of Intellectual Property Rights
UNCITRAL	-	United Nation Commission on International Trade Law
UN	-	United Nations
U.K	-	United Kingdom
U.S.A	-	United State of America
UNEC	-	United Nation Economics Commission for Africa
UNCTAD	-	United Nations Conference on Trade and Development
UEMOA	-	Comparative Legal Initiative in West Africa Economic and Monetary Union
UDHR	-	Universal Declaration of Human Rights
UNHCR	-	United Nations High Commissioner for Refugees
UNODC	-	United Nation Office on Drug and Crime
VGT	-	Virtual Global Taskforce
VOIP	-	Voice over Internet
WSIS	-	World Submit On the Information Society
WWW	-	World Wide Web
WATRA	-	West African Communication Regulators Assembly
WIMAX	-	Worldwide Interoperability for Microwave Access

## ABSTRACT

*With the advent of computer age, legislatures have been struggling to redefine the law to fit crimes perpetuated by computer criminals. The rise of technology and online communication has not only produced a dramatic increase in the incidence of criminal activity, it has also resulted in the emergence of what appears to be some new varieties of criminal activity. Both the increase in the incidence of criminal activity and the possible emergence of new varieties of criminal activity pose challenges for legal systems, as well as for law enforcement. Successful response to these challenges requires new paradigms. In the light of the fact that a lot of problems have been generated as a result of the “lacuna” in our criminal laws, several issues has brought to the fore the imperativeness for a research of this nature for constructive legal reforms of the Nigerian criminal law and acritical examination of the strengths and weaknesses of the most recent legislation on cybercrime enacted only on 15<sup>th</sup> of May 2015 to tackle the menace of cyber insecurity in Nigeria as is done in other jurisdictions. The research methodology adopted is doctrinal which is a library-based methodology that is, an extensive analysis and review of existing literatures on the subject. The key findings among others, from this study are: Law enforcement authorities, prosecutors, and judiciary in developing countries, require long-term, sustainable, comprehensive technical support and assistance for the investigation and combating of cybercrime, Cybercrime prevention activities in all countries require strengthening, through a holistic approach involving further awareness-raising, public-private partnerships and the integration of cybercrime strategies with a broader cybersecurity perspective and as long as there is an absence of a centralized 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 heavy challenge to law enforcement agencies. This work recommended “seven critical” or top priority needs, some of which are: Public awareness, uniform training and certification courses, steady electric power supply, that the court should play down on the proof of specific intent, because the requirement to proof these specific intents significantly narrows the scope of each offence and also makes proving each offence more difficult, exceptions for law enforcement, military or intelligence activities must be addressed in order to avoid these categories from falling victim of the penal provision of section 14(1) of the cybercrime Act, 2015. This thesis argues that law enforcement officials cannot effectively pursue cybercriminals unless they have the legal tools necessary to do so.*

## TABLE OF CONTENTS

Title page-	-	-	-	-	-	-	-	-	-	-	i
Declaration	-	-	-	-	-	-	-	-	-	-	ii
Certification	-	-	-	-	-	-	-	-	-	-	iii
Dedication	-	-	-	-	-	-	-	-	-	-	iv
Acknowledgments	-	-	-	-	-	-	-	-	-	-	v
Table of Cases-	-	-	-	-	-	-	-	-	-	-	vi
Table of Statutes	-	-	-	-	-	-	-	-	-	-	viii
Abbreviations	-	-	-	-	-	-	-	-	-	-	xix
Abstract	-	-	-	-	-	-	-	-	-	-	xxiii
Table of Contents	-	-	-	-	-	-	-	-	-	-	xxiv

### CHAPTER ONE: GENERAL INTRODUCTION

1.1	Background to the Study-	-	-	-	-	-	-	-	-	-	1
1.2	Statement of Problem	-	-	-	-	-	-	-	-	-	9
1.3	Aim and Objectives of the Research	-	-	-	-	-	-	-	-	-	15
1.4	Justification of the Research	--	-	-	-	-	-	-	-	-	16
1.5	Research Methodology	-	-	-	-	-	-	-	-	-	17
1.6	Scope and Limitation of Research	-	-	-	-	-	-	-	-	-	17
1.7	Literature Review	-	-	-	-	-	-	-	-	-	18
1.8	Organizational Layout	-	-	-	-	-	-	-	-	-	33

### CHAPTER TWO: CONCEPTUAL CLARIFICATION OF KEY TERMS

2.1	Introduction	-	-	-	-	-	-	-	-	-	35
2.2	Nature of Cyber Space	-	-	-	-	-	-	-	-	-	35
	I.Hacking and Related Activities	-	-	-	-	-	-	-	-	-	35
	II.Viruses and Malicious Code	-	-	-	-	-	-	-	-	-	39
	III. Online Fraud	-	-	-	-	-	-	-	-	-	42
	(A) Fraud by Computer Manipulation	-	-	-	-	-	-	-	-	-	42
	(B) Computer Forgery and Desktop Counterfeiting	-	-	-	-	-	-	-	-	-	43
	(C) Modifications of Data or Programmes	-	-	-	-	-	-	-	-	-	43
	(D) Online Auction Fraud	-	-	-	-	-	-	-	-	-	45
	(E) Electronic-Mail Forgery	-	-	-	-	-	-	-	-	-	46

	IV. Cyberstalking, Harassment and Hate Speech	-	-	-	-	-	-	-	48
	V. Cyber-terrorism	-	-	-	-	-	-	-	50
	VI. Cyber theft-	-	-	-	-	-	-	-	51
2.3	Concept of CyberCrime	-	-	-	-	-	-	-	53
2.4	Nature and Scope of Cyber Security and Insecurity	-	-	-	-	-	-	-	59
2.5	Meaning of Cyber Jurisdiction	-	-	-	-	-	-	-	67
2.6	Nature and Scope of Internet	-	-	-	-	-	-	-	73
2.7	Concept of Protection	-	-	-	-	-	-	-	79
2.8	Nature and Scope of Cyber Law	-	-	-	-	-	-	-	81
<b>CHAPTER THREE: THE DEVELOPMENT OF LEGAL AND INSTITUTIONAL REGIMES INCOMBATING CYBER CRIME AND CYBER INSECURITY</b>									
3.1	Introduction	-	-	-	-	-	-	-	84
3.2	Role of Law in Combating Cyber Crime	-	-	-	-	-	-	-	85
3.3	Development of Legal and Institutional Regimes at Global Level	-	-	-	-	-	-	-	87
3.4	Development of Legal and Institutional Mechanisms at Regional Level	-	-	-	-	-	-	-	111
	(i) The Organisation for Economic Co-operation and Development (OECD)-	-	-	-	-	-	-	-	111
	(ii) The North Atlantic Treaty Organisation (NATO)	-	-	-	-	-	-	-	112
	(iii) The Shanghai Cooperation Organisation (SCO)	-	-	-	-	-	-	-	112
	(iv) The Virtual Global Taskforce (VGT)	-	-	-	-	-	-	-	113
	(v) Strategic Alliance Cyber Crime Working Group(SACCCWG)	-	-	-	-	-	-	-	113
	(vi) The Asia-Pacific Economic Cooperation (APEC)	-	-	-	-	-	-	-	114
	(vii) The Council of Europe (COE)	-	-	-	-	-	-	-	116
	(viii) The European Union (EU)	-	-	-	-	-	-	-	119
	(ix) The Organisation of American States (OAS)	-	-	-	-	-	-	-	122
	(x) African Regional Efforts	-	-	-	-	-	-	-	123
	(a) Economic Commission of Africa (ECA)	-	-	-	-	-	-	-	125
	(b) African Information Society Initiative (AISII)	-	-	-	-	-	-	-	126
	(c) The Economic Community for West African States (ECOWAS)	-	-	-	-	-	-	-	127
	(d) East African Community (EAC)	-	-	-	-	-	-	-	129
	(e) Arab Magreb Union	-	-	-	-	-	-	-	130
	(f) South African Development Community (SADC)	-	-	-	-	-	-	-	130

	(g) Comparative Legal Initiatives in West Africa Economic and Monetary Union (UEMOA) - - - - -	131
	(h) Comparative Legal Initiatives in Inter-Governmental Authority on Development (IGAD) - - - - -	132
3.5	Development of Legal and Institutional Frameworks at National Level -	132
	Position in Nigeria - - - - -	133
	(a) The General Statutes for Fighting Criminal Activities - - -	133
	(b) The Genesis of the Cybercrime Act, 2015 - - -	134
	(c) The Economic and financial Crimes Commission (Establishment) Act, 2002 (EFCC) - - - - -	135
	(d) The Nigerian Cybercrime Working Group (NCWG) - - -	136
	(e) Central Bank of Nigeria Guidelines on Electronic Banking - -	138
	(f) The Advance Fee Fraud and Other Related Offences Act, 2006 - -	138
	(g) National Identity Management Commission Act, (NIMC) - -	138
	(h) Terrorism (Prevention) Act, 2012- - - - -	141
	(i) The National Information Technology Development Agency Act, 2007 (NITDA) - - - - -	142
	(j) Criminal Code Act - - - - -	143
	(k) Nigerian National Policy for Information Technology Act, 2001 (NPFIT) - - - - -	144
	(l) Cybercrime Draft Bill 2004 - - - - -	149
	(m) The Cybercrime Draft Bill 2005 - - - - -	150
	(n) Cybercrime Draft Bill 2011 - - - - -	153
	(o) Cybercrime Draft Bill 2013 - - - - -	154
	(p) National Cybersecurity Policy - - - - -	155
	(q) General Overview of Cybercrime Act, 2015 - - - - -	157
	(r) Challenges of the Cybercrime Act, 2015 - - - - -	159

**CHAPTER FOUR: THE ROLE OF LAW ENFORCEMENT AGENCIES  
IN COMBATING CYBER INSECURITY AND CRIME**

4.1	Introduction	-	-	-	-	-	-	-	167
4.2	Nature of Traditional Law Enforcement Functions	-	-	-	-	-	-	-	168
4.3	Prevention and Detection of Crime	-	-	-	-	-	-	-	175
4.4	Powers of Law Enforcement in the Prevention and Control of Crime	-	-	-	-	-	-	-	185
4.5	Ethical and Legal Standards in Law Enforcement on the Prevention and Control of Crime and Insecurity	-	-	-	-	-	-	-	198
4.6	Good Practices (strategies) in Addressing Cyber Insecurity	-	-	-	-	-	-	-	216

**CHAPTER FIVE: PROBLEMS AND CHALLENGES OF LAW ENFORCEMENT AGENCIES IN SECURING AND PROTECTING CYBERSPACE AGAINST CYBERCRIME**

5.1	Introduction	-	-	-	-	-	-	-	238
5.2	Problems of Information Gathering and Sharing in Relation with Cyber Techniques-	-	-	-	-	-	-	-	239
5.3	Human, Technical and Financial/Institutional Capacity to Prevent and Control Cyber Crime-	-	-	-	-	-	-	-	248
	i. Multi-State Information Sharing and Analysis Center (MS-ISAC) v QAKBOT	-	-	-	-	-	-	-	249
	ii. Microsoft v The Rustock Botnet	-	-	-	-	-	-	-	251
	iii. FBI v The Coreflood Botnet	-	-	-	-	-	-	-	252
	iv. The National Cyber Forensic and Training Alliance (NCFTA) v Pump and Dump Scam	-	-	-	-	-	-	-	254
	v. Interpol and Ican, Partnering for Internet Security	-	-	-	-	-	-	-	255
5.4	Evidentiary Problems-	-	-	-	-	-	-	-	257
5.5	Investigative Techniques	-	-	-	-	-	-	-	262
5.6	Prosecutorial Skills and Knowledge	-	-	-	-	-	-	-	266
5.7	Appraisal of the Peel Theory of Community Policing: Whether Applicable in the Context of Cyber Security and Protection	-	-	-	-	-	-	-	268
5.8	Constitutional and Human Rights Issues	-	-	-	-	-	-	-	278
	i) Conflicts between Cybersecurity Law and FreeSpeech	-	-	-	-	-	-	-	286

ii) Data Protection and Privacy Infringement Liability Regimes:										
	Civil and Criminal	-	-	-	-	-	-	-	-	289
a)	Privacy	-	-	-	-	-	-	-	-	292
b)	Data Protection	-	-	-	-	-	-	-	-	293
c)	Duties and Responsibilities of the Cloud Client and the Cloud Service Provider (CSP)	-	-	-	-	-	-	-	-	294
d)	Trans-border Data Transfer Restrictions	-	-	-	-	-	-	-	-	294
e)	Data Security	-	-	-	-	-	-	-	-	296
f)	Applicable Law	-	-	-	-	-	-	-	-	296
g)	Compliance with Data Protection Requirements	-	-	-	-	-	-	-	-	297

## **CHAPTER SIX: SUMMARY AND CONCLUSION**

6.1	Summary	-	-	-	-	-	-	-	-	305
6.2	Findings	-	-	-	-	-	-	-	-	309
6.3	Recommendations	-	-	-	-	-	-	-	-	311
6.3.1	Public Awareness	-	-	-	-	-	-	-	-	311
6.3.2	Uniform Training and Certification Courses	-	-	-	-	-	-	-	-	311
6.3.3	Management Assistance for Onsite Electronic Crime Task Forces	-	-	-	-	-	-	-	-	311
6.3.4	Cooperation with the High-tech Industry	-	-	-	-	-	-	-	-	312
6.3.5	Special Research and Publications	-	-	-	-	-	-	-	-	313
6.3.6	Investigative and Forensic tools	-	-	-	-	-	-	-	-	314
6.3.7	Electric Power Supply-	-	-	-	-	-	-	-	-	315
	Bibliography	-	-	-	-	-	-	-	-	318

## CHAPTER ONE

### GENERAL INTRODUCTION

#### 1.1 Background to the Study

Although only a few would deny that the internet has had a major impact upon criminal behavior, there is much less consensus as to what that impact has been. Even when Nations agree that cybercrimes are a problem there appears to be no overall consensus about how to deal with them collectively<sup>1</sup>. All too often claims about the prevalence of Cybercrimes lack clarification as to what it is that is particularly “cyber” about them.

Indeed, when so called cases of cybercrime are closely examined they often have the familiar ring of the “traditional” rather than the “cyber” about them. These offences typically comprises: hacking<sup>2</sup>, fraud, pornography, pedophilia and the likes. Some of these are already part of existing criminal justice regimes in Nigeria. Perhaps more confusing is the contrast between the many hundreds or thousands of incidents that are supposedly reported each year and the relatively small number of known prosecutions. “Is this a case of the absence of evidence not being evidence”, as per secretary of state, Donald Rumsfeld<sup>3</sup>. “Or should we be asking if there are actually such things as cybercrimes?”<sup>4</sup> Other authors<sup>5</sup> have questioned whether cybercrimes are actually categories of crime in need of new theory, or whether they are understood better by existing theories.

The reason why it is called cyber crime is still not understood. What is clear is that the word cyber crime was first coined by an American writer of Science fiction, William Gibson in

---

<sup>1</sup> Goodman, M and Breaner, S (2002), “The emerging consensus on criminal conduct in cyber” UCLA Journal of Law and Technology,3:28.Retrieved June 2, 2012 from [www.lawtechjournal.com/articles/2002/03-020625\\_goodmambrenner.pdf](http://www.lawtechjournal.com/articles/2002/03-020625_goodmambrenner.pdf).

<sup>2</sup>Hacking- (Criminal act of illegitimate access to computer).

<sup>3</sup> Borone, M (2004, 24 March)“The National interest: absence of evidence is not evidence of absence; US, News & World Report. Retrieved June 2, 2012 from [www.usnews.com/usnews/opinion/baroneweb/mb040324.htm](http://www.usnews.com/usnews/opinion/baroneweb/mb040324.htm).

<sup>4</sup> Brenner, S (2001) “Is there such a thign as “virtual crime””? California Criminal Law Review, 4 (1): 11

<sup>5</sup> Jones, R (2003) “Review of Crime in the Digital Age” by P. Grabosky and R. Smith, International Journal of Law and information Technology, 11: 98

(1982) and then popularized on his 1984 novel 'Necromancer': the term cyberspace became a popular descriptor of the mentally constructed virtual environment within which networked computer activity takes place "cybercrime" broadly describes the crimes that take place within the space and the term has come to symbolize insecurity and risk online.

By itself, cybercrimes is fairly meaningless because it tends to be used metaphorically and emotively rather than scientifically or legally. Usually to signify the occurrence of harmful behavior that is somehow related to the misuse of a networked computer system<sup>6</sup>.

Largely an invention of the media, 'cybercrime' originally had no specific reference point in law in the United Kingdom or United States of America<sup>7</sup>

The offence that did become associated with the term was a rather narrow legal construction based upon concerns about hacking. In fact, many of the so called cybercrimes that have caused concern over the past decade are not necessarily crimes in criminal law.

If we could turn the clock back in time then perhaps the term 'cyberspace crime' would have been a more precise and accurate descriptor. However, regardless of its merit and demerits, the term 'cybercrime' has entered the public parlance and we are stuck with it.<sup>8</sup>

Currently, the internet is so news worthy that a single dramatic incident of cybercrime has the power to shape public opinion and fuel public anxiety, frequently resulting in (political) demands for instant' and simple solutions to extremely complex situations.

"Indeed, media accounts of cybercrimes still frequently invoke a dramatic imagery of a vulnerable society being brought to its knees by forces beyond its control such as an 'Electronic Pearl Harbor'<sup>9</sup> or a 'Cyber Tsunami'<sup>10</sup>.

---

<sup>6</sup> Wall, D.S. (1997) Policing the virtual community: the internet, cybercrimes and the policing of cyberspace. In P.Francis, Davis, P and Jupp, V. (eds), *policing futures*, London Macmillan, Pp.36- 208

<sup>7</sup> There are a few exceptions, such as in Australia, where a cybercrime Act was introduced in 2001 and in Nigeria, where a Draft bill on cybercrime has been proposed since 2005 and an Act enacted only on 15, May, 2015.

<sup>8</sup> Wall, D.S. (2005a) The Internet as a conduit for criminals. In A. Pattavina (ed.) *Information Technology and the Criminal Justice System*, Thousand Oaks, (A : Pp. 77-98)

The now defunct Omni magazine, which was published between 1978 and 1998, was one of a range of contemporary publications that combined articles on science fact with short works of science fiction to form popular technology-related narratives. It was, coincidentally, in the pages of Omni magazine, that William Gibson first coined the word ‘Cyberspace’ in 1982.

As more aspects of people’s life move to digital networks, crime comes with them. People’s lives increasingly depend on the internet and digital networks, but these create new vulnerabilities and new ways for criminal to exploit the digital environment. Not only can many existing crimes be replicated in online environments, but novel crimes that exploit specific features of digital networks have emerged as well, with new crimes, comes new forms of policing and new forms of surveillance and with these comes new dangers for civil liberties.

At the dawn of the computer age, Marshall McLuhan<sup>11</sup> predicted that new electronic media would bring the world closer together into a “global village”. The internet is the fulfillment of his prophecy. People scattered across the globe can now all congregate together in cyber space to share idea and information. Ironically, the global village leads us towards a future that revives part of the past-life in the small village of several centuries ago. With the prevalence of cell phone cameras, people can no longer engage in social infractions without risking being caught in the act. No longer can people hide in obscurity and escape accountability for their actions. People can readily document and record each other’s norm violations, and they can then post them online.

---

<sup>9</sup> Smith, G. (1998) Electronic Pearl Harbor? Not likely Issues in Science and Technology, 15 (3): 68-73, Retrieved June 2, 2012 from [www.nap.edu/issue/15.1/smith.html](http://www.nap.edu/issue/15.1/smith.html). See also, Taylor, P. (2001) Hackitivism: In search of lost ethics? In: D.S Wall (ed.) Crime and the Internet, London Routledge, Pp. 59-73.

<sup>10</sup>Ibid.

<sup>11</sup> Marshall McLuhan, (1962) The new electronic interdependence recreates the world in the image of a global village. The Gutenberg Galaxy p.31, see also Marshall McLuhan & Bruce, (1989). Powers, The Global village: Transformation in world Life and Media in The 21<sup>st</sup> century The Gutenberg Galaxy p.110.

The world today is concerned at the magnitude of insecurity in the cyberspace and this fear is reflected in the several global, regional and national efforts at policy guidelines and control to stamp out the wave of cyber criminality.

At the global level, the International Communication Union (ITU) launched in May 2007, the Global Cybercrime Agenda (GCA) for a framework where the international response to growing challenges to cyber security could be coordinated. In order to assist the ITU in developing strategic proposals, a global High-Level Experts Group (HLEG) was established in October 2007.

This global experts group of almost 100 persons delivered the Chairman's Report in August 2008 with recommendations, including cyber crime legislations. The Global Strategic Report was delivered in November 2008, including strategies in five work areas<sup>12</sup>.

Detailing the content of the report is beyond the scope of this work, however, efforts is made in analyzing the strategies in the five work areas.

Work Area one, "Legal measures", sought to develop advice on how criminal activities committed over ICTs could be dealt with through legislation in an internationally compatible manner.

Work Area two, "Technical and procedural measures", focused on key measures for addressing vulnerabilities in software products, including accreditation schemes, protocols and standards.

Work Area three, "Organizational structures", considered generic frameworks and response strategies for the prevention, detection, response to and crisis management of cyber attacks, including the protection of countries' critical information infrastructure systems.

---

<sup>12</sup> ITU. Retrieved June 2, 2012 from [http://www.itu.int/osg/csd/cybersecurity/gca/global\\_strategic\\_report/](http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/).

Work Area four, “Capacity building”, sought to elaborate strategies for capacity-building mechanisms to raise awareness, transfer Know-how and boost cyber security on the national policy agenda. Finally, Work Area five, “International cooperation” sought to develop a strategy for international cooperation, dialogue and coordination in dealing with cyber threats<sup>13</sup>.

Just like the Council of Europe Convention on Cybercrime in 2001 which is a regional initiative, the African region also made significant efforts and that is briefly discussed infra.

In recognition of the challenges of cyber security, and in other to build an Information Society where key stakeholders can play a pivotal role, Economic Commission for Africa (ECA) upon the request of its Member States launched the Africa Information Society Initiative (AISII). This was the first framework of its kind to concretely prioritize the issue of Information Communication Technology (ICTs) within the socio-economic development agenda. This initiative was approved by the Economic Commission for Africa (ECA) Conference of Finance Ministers in 1996 and adopted the same year by the Summit of Heads of State and Governments of the Organization of African Unity (OAU) and ultimately supported by the then G7+1 as Africa’s major Information Communication Technology (ICT) initiative in its 1997 Denver Summit. The Africa Information Society Initiative’s (AISII) recommendations fed into the World Summit on the Information Society (WSIS) Action Plans and are the cornerstone of the New Partnership for Africa’s Development (NEPAD) ICTs Short Term Action Plan.

Through the implementation of Africa Information Society Initiative (AISII), Economic Commission for Africa (ECA) has supported the formulation of national e-strategies commonly known as National Information and Communication Infrastructure (NICI) plans, in approximately 30 African countries, which promote the formulation and implementation of e-

---

<sup>13</sup>Details and biographies of HLEG Members are listed at and retrieved June 2<sup>nd</sup> 2012 from: <http://www.itu.int/osg/csd/cybersecurity/gca/hleg/members.html>.

strategies. Other Africa Information Initiative (AISI) activities include information and knowledge management activities and projects that include the Information Technology Centre for Africa (ITCA), which is an information and communication technology (ICT) focused exhibition and learning centre to demonstrate to African policy makers and planners the value of Information Communication Technology (ICT) for development.<sup>14</sup>

On the Nigerian scene, the activities of cyber criminals have become a worldwide ugly phenomenon. The government of the Federation in 2001 commissioned a body of experts to design a National Policy on Information Technology. The policy was expected to deal with all emerging issues in the information and communication technology fields. It is however to be noted that the resultant policy does not offer much for the understanding, prevention and eradication of criminal activities in cyberspace.<sup>15</sup>

Significant as the IT policy is, it is noteworthy that the Nigerian state did not take any definite regulatory step on it until 2003, whereas the Information Communication Technology (ICT) media proposed in the Policy had become widely available since 2001. It was not until a murder incident at a Nigerian embassy in 2003, which was connected to an Internet crime<sup>16</sup> that the Federal Government was moved to constitute a cyber crime working group, the Nigeria Cybercrime Working Group (NCWG), to examine all associated problems of cyber-criminality as related to Nigeria and make appropriate submissions to government on how to nip them in the bud. This body was formally launched on 31st March 2004 (by which time the menace of crime on the Internet had become firmly entrenched among a large segment of Nigerian ICT buffs),

---

<sup>14</sup>United Nations Economic and Social Council, (2004, June, 9 - 11 ) Report of Economic Commission for Africa United Nations Conference Centre Addis Ababa, Ethiopia, p.20.

<sup>15</sup>Obada, R, Oke, M, (2012. . May,30)Cyber Capacity without Cyber Security: A Case Study of Nigeria's National Policy for information Technology (NPFIT). The Journal of Philosophy, Science & Law. 12: p.3.

<sup>16</sup>John, W. Retrieved June 3, 2012 from <http://www.crime-research.org/news/22.07.2007>,

sequel to the recommendations of the Presidential Committee on Illegal On-line activities led by the National Security Adviser to Ex-President Olusegun Obasanjo (1999-2007).<sup>17</sup>

The Nigeria Cybercrime Working Group (NCWG) was a high powered Inter-Agency group. Its members were drawn from all the critical law enforcement, security, intelligence, and Information Communication Technology (ICT) agencies of the government. The group also had major organized private ICT sector stakeholders as members. Specifically, the Group had as co-chairpersons the Attorney-General of the Federation and Minister of Justice, and the Minister of Science and Technology. The Inspector General of Police, the Chairperson of the Economic and Financial Crimes Commission (EFCC), the Director-General of the State Security Services (SSS) and the Director-General of the National Intelligence Agency (NIA) were also members of the group. Other members were the Executive Vice-Chairman of National Information Technology Development Agency (NITDA), the President of the Nigerian Computer Society, the President of the Nigerian Internet Group, and the President of the Internet Service Providers Association of Nigeria. The effort of the working group resulted in a draft Cybercrime Bill that is before the National Assembly since 2004. This is the draft bill that the National Assembly has recently enacted as cybercrime (prohibition prevention ETC) Act, 2015.

The commissioning of the policy could be seen as a manifestation of the Nigerian government's awareness of the pivotal role of information and communication technologies in the contemporary world. This awareness of government was well captured in the Policy thus: "Information Technology (IT) is the bedrock for national survival and development in a rapidly changing global environment."<sup>18</sup> Cognate to this governmental awareness, the IT policy focused

---

<sup>17</sup> Abel, E. , (2006), Regulating Internet Banking In Nigeria: Some Success Prescriptions – Part 2, *Journal of Internet Banking and Commerce*.11:33.

<sup>18</sup> "Executive Summary", (2001.March) *Nigerian National Policy on Information Technology (IT)*, Federal Ministry of Science and Technology: Abuja. p. ii.

on some areas that should be covered by appropriate laws. Of particular relevance here is the section of the IT policy on Information Technology Law. This section proposes to:

Criminalize the use of computers and related technologies for the commission of crimes or to facilitate criminal behavior, wrongful access, and deceitful usage; and criminalize the targeting of computers and the data contained within them through an unauthorized access, unlawful copying of information, damage or tampering with such information, and /or depriving the legitimate owner of data of the benefit of such data.<sup>19</sup>

Wide-ranging in its coverage of cybercrimes as this aim of government was, nothing was done towards enacting either an Information Technology Law or a Computer Crime Law until 2004 when the Nigeria Cybercrime Working Group (NCWG) was created. The NCWG, a unit of the National Information Technology Development Agency (NITDA), worked out a foundation for a cybercrime law for Nigeria.<sup>20</sup> As proposed, the envisaged law would include a substantive law that would criminalize the following kinds of conduct: (i) Conducts against information and communication technology (ICT) system, (ii) Conducts using ICT systems as tools for committing crime, and (iii) Legally prohibited conducts that have essential ICT infrastructures as targets.<sup>21</sup> It will also contain some procedural provisions that deal with investigation of crime, collection of evidence relating to cybercrime as well as procedures for searches, seizures and interception of digital communication.<sup>22</sup> The third component of the proposed law is an array of options on infrastructure and institutional arrangement. The details of this component are: (i) promote and develop specialized units to deal specifically with ICT offences, as units of existing law enforcement formations, (ii) facilitate cooperation between industry and law enforcement agencies, (iii) create an advanced ICT centre to collect, collate, analyze, and circulate relevant

---

<sup>19</sup> Ibid, Appendix B; 47.

<sup>20</sup> Basil, U,( 2004.) Challenges of Cybercrime Enforcement in the ECOWAS Sub-Region-Case Study of Nigeria. A paper presented at a seminar organized by NITDA, Held at NITDA Head Quarters Abuja.

<sup>21</sup> *Nigerian National Policy for Information Technology*, (2001) Federal Ministry of Science and Technology, Abuja. p.ii

<sup>22</sup> Ibid,

technical information to and for other relevant Agencies, and (iv) if need be, create an entirely new cybercrime and cyber security agency at par with other specialized agencies like EFCC, ICPC, NDLEA, NAPTIP, NACA and NAFDAC.<sup>23</sup>

The NCWG had a correct perception and apprehension of the enormity of the problem of cybercriminal as reflected in the conclusion of its report thus:

Enforcing cybercrime in Nigeria is a necessary compliment to the great strides the Nigerian Government has made towards transforming Nigeria into an ICT-driven economy. To leave our systems and networks unprotected is to deliberately endanger the same infrastructures we worked so hard and invested so much to build.<sup>24</sup>

The recently enacted cybercrime Act<sup>25</sup> succinctly captured all of the above proposals and provided for penalties for the offences. A general overview of this new Act is discussed in chapter three of this work.

## **1.2 Statement of Problem**

The origin of Cybercrime can be traced back to the interception of Semaphore signals in the eighteenth century, or the wire tap in the nineteenth and early twentieth century<sup>26</sup>.

In both cases, valuable information was intercepted as it was being transmitted across hitherto unparalleled spans of time and space and then sold. However, the true genesis of cybercrimes originates in early computer crimes prior to their subsequent transformation by networking over two further generations. It is useful to explore these milestones because although the notion of “generation invokes the passage of time, each generation is distinctive and the

---

<sup>23</sup> Ibid, at Pp.10 and 16.

<sup>24</sup> Ibid, at. p. 18.

<sup>25</sup> Cybercrime (Prohibition prevention (ETC) Act, 2015. (Signed into Law only on the 15<sup>th</sup> of May 2015 by former President Goodluck Jonathan at the twilit of the last administration).

<sup>26</sup> Standage,T. (1998). The Victorian internet: The remarkable story of the Telegraph and the Nineteenth century’s online pioneers, London: Phoenix, Pp.19-24

conceptual differences between them can be used to explain contemporary differences currently present in the scope of criminal opportunity.

Until the mid-1980s the internet had been the preserve of the military who originally conceived it as an attack-proof communications system. It was subsequently released for government and academic purposes before being opened up for general usage. The internet's massive potential for good and bad was realized following the development and commercial popularity of the graphics user interface (**GUI**) in the early 1990s.

The present generation cybercrimes are mostly 'hybrid'. They are effectively 'traditional' crimes for which entirely new globalized opportunities have arisen. For them, the internet has created a transnational environment with entirely new opportunities for harmful activities that are currently the subject of existing criminal or civil law. Examples of these activities include trading in sexually explicit materials, including child pornography, through interactive hardcore websites, and fraud<sup>27</sup>. The increasing prevalence of deception through internet auctions for example is a vivid example of this level of opportunity<sup>28</sup>.

Networked environments also contributes to the circulation of criminal ideas. News groups and websites circulate information about 'chipping',<sup>29</sup> how to by-pass the security devices in mobile telephones or digital television decoders<sup>30</sup>. They also provide information on

---

<sup>27</sup> Grabosky, P.N, Smith, R.G and Dempsey, G. . (2001) *Electronic Theft: Unlawful Acquisition in cyberspace*. Cambridge University Press. Pp.135-268, See also Levi, M. (2001) *Between the risk and the reality falls the shadow, evidence and urban legend in computer fraud*; In D.S Wall (ed.) *crime and the internet*, London: Routledge. Pp.44-58

<sup>28</sup> Newman, G.R and Clark, R.V. (2003) *Superhighway Robbery: Preventing e-commerce crime*. Cullompton William publication. Pp.86-91

<sup>29</sup> Oxford dictionary of computing fourth eds (1996) U.K Oxford University Press "An illegal act of avoiding security measures on chip cards formerly called smart card".

<sup>30</sup> Mann, D and Sutton, M. *Netcrime: (1998), More change in the organization of thieving: British Journal of Criminology*, 38 (2): 210-229. see also Wall, D.S. (2000) *The theft of electronics services: telecommunication and teleservices*, Essay on the C.D-Rom annex to DTI, *Turning the corner* London: Department of Trade and Industry. p.47

how to take to manufacture and distribute synthetic drugs<sup>31</sup>. Take away the internet and the offensive behavior remains but the new opportunities for committing of offence disappear and the behavior continues by other means, though not in such great numbers or across such a wide span. Consequently, hybrid cybercrimes are examples of the modernization of modernity<sup>32</sup> perhaps the major problem lies in the fact that the problems that arise tend to relate to matters of trans-Jurisdictional procedure rather than substantive law. This creates difficulties for the enforcement of law where the responsibilities of each country are not so clearly defined.

During the past decade, the growth in the use of the internet and the cyberspace it has created has developed from science fiction into a socially constructed reality. Cyberspace possesses some unique qualities which creates a series of challenges for our existing laws. These qualities are: Its lack of respect for jurisdictional boundaries, the sheer volume of traffic that it can handle virtually instantaneously, its openness to participation, the potential for anonymity of members of the virtual community, its apparent economic efficiency. All these are summarized by the popular acronym “3A’s” in cyber circle which stands for Affordability, Accessibility and Anonymity’. When these qualities are combined with the rather ironic fact that the internet was originally designed by the United States of America military so as to resist thermonuclear attack<sup>33</sup>, then the internet has an innate ability to undermine attempts by nation states and commercial institutions to monopolize its political and commercial potentials. As a consequence, many of existing models of legal regulation have difficulties coping with the new medium of cyberspace. At one level, some old laws simply do not apply anymore and new laws need to be developed, for example, to deal with the use of pseudo-photographs in obscenity cases involving

---

<sup>31</sup> Scheiner J.L. (2003) iding in plain sight: on Exploration of the illegal (?) activities of a drug newsgroup. The Howard Journal of Criminal Justice, 42 (4): 374-389

<sup>32</sup> Beck,U. (1992).Risk society, London sage. p.22. See also Finnemann. N. (2002) perspectives on the internet and modernity; late modernity, postmodernity or mordenity modernized? In N. Brugger and H. Bodker (eds.) The Internet and society? Papers from centre for Internet Rresearch, University of Aarhus, Denmark Pp, 29-37.

<sup>33</sup> “Cyber Law Research Unit, (1999) University of Leeds, U.K. (college brochure). P.3.

children. In such cases, prosecutors have traditionally based their arguments upon the fact that in order to create the obscene picture, a child had to be abused. This presupposes the intention of section 30 (2) (e) of the Child Rights Act<sup>34</sup> which provides that: “any person who procures, uses or offers any person for, - - - or the production of pornography, or for pornographic performances - - - commits an offence and is liable on conviction to 14 years imprisonment without option of fine”.

However, the development of graphics software that enables the advanced manipulation of images now means that obscene photographs can be created with the same effect as before but without the abuse of a child. Hence the need for existing law to adapt. It is noteworthy however, that the United Kingdom has already promulgated an Act on Pseudo photograph<sup>35</sup>. The recent Nigeria cybercrime Act<sup>36</sup> has also adequately provided for this.

At another level, the special qualities of cyberspace which are outlined above create such serious problems for the application of law to the point that focus of the debate shifts from legal regulation to governance. Quite simply, many traditional laws and legal mechanisms have become outmoded, being replaced by a variety of regulatory and normative strategies and techniques which transcend the public/private divide.

To this extent, Cyber-law refers to the legal regime, relating to issues that arise within the newly emerging area that is increasingly becoming known as cyberspace. More specifically, it relates to the interaction of law with information communications technologies and computer mediated communications system. It therefore has a different agenda to that of either computer law or law of the internet which respectively often show little difference from the law relating to contract or patents or publishing or broadcasting law.

---

<sup>34</sup> Section 30 (2) (e), Child Rights Acts cap. N30. L.F.N. 2004

<sup>35</sup> Computer Misuse Act, 1990, ch.18ss.1-3 (England)

<sup>36</sup> Section.23, Cybercrime (prohibition Prevention ETC) Act, 2015

Although the application of both areas of law raises some fascinating issues. Whilst there is some overlap with the law of the internet and to a lesser extent with computer law, cyber law nevertheless has separate identity. The distinctions between the three relate not just to subject areas but, importantly to the qualitatively different levels with which each engage with the study of law. Cyber law exists at the (cutting) edge of law where the ability of the existing law to achieve its goals is challenged. In this sense the “law” in cyber law is a much broader concept; it is “law in action” as opposed to “law in books” as it applies to situations where law cannot cope. It therefore takes as its subject the wider range of regulatory responses and strategies of governance that subsequently arise.

Unfortunately, the legal regime on the offences of cyber crime and cyber insecurity, prior to the enactment of the Nigeria cybercrime Act on 15<sup>th</sup> of May 2015 “is not only moribund but anachronistic. The Criminal and Penal Codes that made provisions for offences in Nigeria pre-dated Nigeria’s independence by which time the modern technology was yet to be in place”<sup>37</sup>.

It is obvious that the criminal statutes such as the police Act, the criminal procedure Act and other statutes in this category as they were today, did not envisage crime as cyber crime and cyber insecurity. This deficiency has created a gap in the law to the extent that it did not empower the law enforcement agencies to prevent and control cyber crime and insecurity and especially determine cyber jurisdiction.

The negative impact of cyber crime on National economy, national security and sustainable development of the nation was vividly captured during a public hearing on the

---

<sup>37</sup> The pre-existing Legal regime in our criminal law statutes covers the following offences, stealing, see. Section 383, Criminal Code and 286 Penal Code; forgery, see. Section 465 Criminal Code and 362 Penal Code; obtaining by false pretence, see. Section 419 Of the Criminal Code and fraudulent false Accounting. See. Section 435 (2) and 438 Of the Criminal Code. See also Robbery as provided in Section 401 Criminal Code and Section 296 of the Penal Code.

Computer Security and Critical Information Bill 2005 organized by the Senate Committee on Science and Technology, the then Senate president, Ken Nnamani said:

For Nigeria to be super power in Information and Communication Technology (ICT), Nigerians must shun all Internet crimes and malpractices capable of giving the country a bad name. He said Nigerians must not use the Information Communication Technology revolution to damage our cultural values and international credits'. He further added; 'Advances in Information Communication Technology are blessing to mankind but they could become curse - - -. If we intended to be globally competitive, we must remake Nigeria as an attractive destination for international capital. This cannot be achieved if we are branded a nation of 'scammers' and 'anything goes'<sup>38</sup>

It has been argued that organized crime<sup>39</sup> weakens the very foundation of democracy, as there can be no good governance without rule of law .This observation is very applicable to the situation in Nigeria. As the nation faces the challenges of nurturing a stable democracy, after many years of military dictatorship, organized crime poses a great threat to the survival of the country. Therefore, the Nigerian government has mapped out policies and strategies to deal decisively with crimes that are transnational in nature and scope. The detail of this is discussed in chapter 3.4 of this work infra.

In the light of the fact that a lot of problems have been generated as a result of the "lacuna" in our criminal laws, several issues will agitate the basis of a research in cyber security and protection. Prominent but not limited to such issues for determinations are:

- (1) Is the issue of cybercrime overhyped?
- (2) What is the role of law enforcement agencies in combating this emerging crime?

---

<sup>38</sup> Ken Nnamani. Senate President, as he then was ( 2006. Sept.12,) Daily Trust News paper. at p.5

<sup>39</sup> M. Lyman, M and Porter, G, Organized Crime (New Jersey:Prenhall); Sieber, U (1998), Legal Aspects of Computer Related Crime, (European Commission), 25. (cited by Chawki, M. (2009) 'Nigeria Tackles Advance Fee Fraud', Journal of Information, Law & Technology (JILT) (1):7.The involvement of organised crime groups in the field of computer fraud was illustrated when a Russian group attacked one of the known US banks in New York via data networks in 1994. Operating from St. Petersburg, the group succeeded in causing the American bank to transfer over US\$ 10 million to foreign accounts. The arrested perpetrators possessed false Greek and Israeli passports which were forged in a quality which could be produced in Russia only by members of the former Russian secret service KGB. Retrieved June 4, 2012 from <[http://go.warwick.ac.uk/jilt/2009\\_1/chawki](http://go.warwick.ac.uk/jilt/2009_1/chawki)>

(3) What are the problems and challenges of law enforcement agencies in the prevention and control of cybercrime?

(4) Nigeria now has a cybercrime “specific” Act, but the concern is what is the implementation strategy for the newly promulgated cybercrime Act 2015 and the National Policy on Cybercrime?

Above questions are the core research questions related to the problems which have brought to the fore the imperativeness for a research of this nature for constructive legal reforms of the Nigerian criminal law.

### **1.3 Aim and Objectives of the Research**

This study aims at providing responses to the above mentioned research questions by:

- a) Critically examining the legal and institutional frameworks at global, regional and national level to ascertain the gravity of cybercrime in the society.
- b) Appraising critically, the role of law enforcement agencies in the prevention and control of cyber insecurity in Nigeria and selected jurisdictions of Britain and USA not because the law in Britain and USA is applicable in Nigeria, but because these two countries are more technologically advanced countries than Nigeria, and their experiences can serve as a point of lesson for Nigeria.
- c) Identifying the problems and challenges in the strategies for the prevention and control of cyber insecurity and develop viable options to address the identified problems and challenges relating to the prevention and control of cyber insecurity in Nigeria.
- d) Propounding recommendations on implementation strategy for the newly promulgated cybercrime Act, 2015 and to critically examine the strengths and

weaknesses of the most recent legislation on cybercrime enacted only on 15<sup>th</sup> of May 2015 to tackle the menace of cyber insecurity in Nigeria as is done in other jurisdictions.

#### **1.4 Justification of the Research**

Today, the routing infrastructure of the Internet is based on relationships between network operators around the globe. As the Internet evolves and the number of network operators expands, a more standardized and automated model of routing security is needed. Research such as this is required to investigate this need and to produce standards to enable a more secure Internet routing infrastructure, including cyber security and protection.

Though Internet routing has worked well over the years, there have been instances of errors that caused routing stability issues. There is also opportunity for malicious activities that could damage the routing infrastructure in the future. To prevent future errors and malicious activity, it is only research such as this that can reveal the reasons why it is important to increase the security of the Internet's routing infrastructure through the deployment of secure routing protocols.

In the light of the above, this research is justified for the following reasons:

1. It will provide additional literature and research output that will contribute to knowledge and enhance greater understanding on the effective strategies for the prevention and control of cyber insecurity.
2. It will assist in the adoption of an appropriate legal and regulatory framework through introduction of a whole legal system supportive and free from legal barrier for the development of a knowledge economy.

3. It will help in the creation of an environment which offers basic assurances such as security, integrity, authenticity, confidentiality and data protection and privacy.
4. It will provide a basis for review of the performance of the law enforcement agencies in Nigeria with a view to enhancing their human, technical, material and investigative capacity in cybercrime and factors responsible for cyber insecurity.

### **1.5 Research Methodology**

The research methodology adopted is doctrinal which is a library-based methodology that is, an extensive analysis and review of existing literatures on the subject.

Accordingly, all library based materials such as books, journals, law reports, internet references and material consulted are duly acknowledged.

### **1.6 Scope and Limitation of Research**

Although the challenges of cyber security and protection are a global phenomenon, there are some countries that are more vulnerable to cyber crime due to the fact that every facet of their daily social life and economic endeavor is woven around Internet services.

Territorially therefore, this research will focus on Nigeria. However, experiences of other countries such as United States of America and Britain will be discussed where such will help for a further clarification and good practice.

The research covers efforts made at global, regional and national levels to proffer solutions to the worrisome and growing factors responsible for cyber insecurity activities of cybercriminals in the world today as well as the impact on global, regional and national economies, peace and security.

In relation to the world position on the drive towards a lasting solution to the problems and challenges facing law enforcement agencies in cyber security and protection, this study will

be territorially, limited in scope to the above mentioned countries and the developments on the subject from 1970 to date.

## **1.7 Literature Review**

Daniel, J.S's.<sup>40</sup> contribution is overabundant with example of online gossip, rumor, and shaming. It is an engrossing book that explores the profound implications of personal information on the Internet. The author argues that unless we establish a balance between privacy and free speech, we may discover that the freedom of the Internet makes us less free.

He reveals that as the Internet is erasing the distinction between spoken and gossip, the future of personal reputation is one of our most vexing social challenges. This illuminating contribution, filled with memorable cautionary tales is of invaluable help to this research. The gap not covered as to incisively analyze the technological and legal challenges and offer a moderate, sensible solutions for navigating the shoals of the blogosphere, are what this research intends to fill.

On his part, Samuel, C.M.<sup>41</sup> provides the insights into what victims of cybercrime experience and must endure after they, their computer systems, or their organization are attacked. He further explains the importance of research for understanding and managing cybercrime related issues and attendant problems. He emphasize that in the real world, policy making and development of sound investigation and security practices cannot wait for additional research into the nature and extent of cybercrime. The author is of the opinion that professionals must do what they can with existing knowledge to develop needed information assurance technologies, protect information systems from attacks, investigate and prosecute cybercrimes and ameliorate harm caused by computer abuse and illegal use of computers, other Information Technology (IT)

---

<sup>40</sup> Daniel J.S. (2007). *The future of Reputation Gossip, Rumor, and Privacy on the Internet*. Yale University press. New Haven & London Pp.97-183

<sup>41</sup> Samuel, C.M. (2006) *Understanding and Managing Cybercrime*. Library of congress cataloging in publication data. Pp.1-187.

devices and information systems. His contribution is inspirational to this research to the extent that it provides an overview of cybercrime and its legal, social, and technical issues. His view is very helpful for the fact that he focuses on the challenges having to do with emergence, prevention, and control of high-tech crime. However he did not reveal, to a large extent the prospect to take a multidisciplinary perspective by trying together various disciplines information technology, the social and anthropology of cyberspace, computer security, deviance, law, criminal justice, risk management and strategic thinking. This work will strive to cover these areas.

David S.W's.<sup>42</sup> approach to this issue gives a refreshing look at new forms of crime. He "decent" desperate nineteenth century street crime that sends minorities to prison, cybercrime is virtually new, a risky frontier for the middle classes. He shows how these new forms find the Police ill suited and untrained for their investigation, he ex-rays cybercrime as a rapidly changing Landscape and he provides an impressive overview of the varieties of contemporary cybercrime, and the many institutions in the public, private, and voluntary sectors that work toward its prevention and control. His line of thought will provide for this research a stimulating, thoughtful and an ideal review of the way that electronic communications have changed (and yet in many ways have not changed) the world of crime and its control. His ideas will assist this research to a fresh thinking and critical perspective on how the Internet has transformed criminal behavior. The main drawback is that he did not touch on what is different about cybercrime with traditional criminal activity, what new criminal opportunities have arisen and in the final analysis, what impact cybercrime might have on public security. This work will fill in the gaps.

---

<sup>42</sup> David, S.W. (2008) Cybercrime: The Transformation of Crime in the Information Age. Polity press. 2<sup>nd</sup> ed. U.K. Pp25-202

Sue, T.<sup>43</sup> writes on an overview of criminal law in a slim, accessible and affordable format. His efforts will provide for this research an ideal resource to supplement other available research material without overwhelming the study, but his conclusion did not reflect the burgeoning threat posed by cyber crime and information terrorism. This research will address this vacuum.

Daniel, E.G.<sup>44</sup> examine in a collection of article on cybercrime and it exposes how Internet has dramatically altered the landscape of crime and national security, creating new threats, such as identity theft, computer viruses, and cyber attacks. He reveals that because cybercrimes are often not limited to single site or nation, crime scenes themselves have changed; consequently, law enforcement must confront these new dangers and embrace novel method of preventions, as well as produce new tools for digital surveillance which can jeopardize privacy and civil liberties. His analysis will provide for this research, a wealth of new insight about the legal and policy implication of Internet. On the whole, he presents a state of the art vision for how to detect and prevent digital crime, creating the blueprint for how to police the dangerous back alleys of the global Internet. Daniel's contributions did not explore the description of crime prevention and security protection in the electronic age. Ranging from new government requirements that facilitate spying to new methods of digital proof. This is going to be the efforts of this research in addition to essentially broaden the horizon of understanding how criminal law and crimes itself have been transformed in our net worked world.

Ladan, M.T, in his book,<sup>45</sup> although not wholly dedicated to cybercrime, the section devoted to Law, Information and Communications Technology in Nigeria is very explicit on

---

<sup>43</sup> Sue, T.R. (2009). Criminal Law the Essentials. oxford University press. New York. Pp.32-160.

<sup>44</sup> Daniel, E.G. (2006) The physics of Digital law: Searching for counter intuitive analogies. In: Balkin M, etal. (ed.) Cybercrime Digital Cops in a Networked Environment. New York University Press. p.13

<sup>45</sup> Ladan M. T (2006) Introduction to Jurisprudence: Classical and Islamic. Faith printers and Publishers Limited, Zaria. Pp.13-16

evidentiary problems. It echoed with the aid of cases the reluctance of our courts to admit electronic documents as evidence and the fact that courts had in most situations regarded such document as secondary evidence. This has reaffirmed the knowledge of this research in this area. However, the recent amendment as it relate to electronics evidence in the Evidence Act, 2011 which is not covered by the author, will be fully discussed in this work. In his most recent book on cybercrime, Ladan, M.T,<sup>46</sup> carefully but in details analyzed the legal and policy responses to ICT and Cybercrime in Nigeria and Ecowas. His efforts clearly explained the International and Regional Initiatives on Cybercrime, Cybersecurity and ICT. This book can be described as a compendium of cyber laws and policies at international, regional and national levels. The authors approach to the issue of definitional problem of cybercrime is of immense benefit to this research to the extent that he revealed that instead of bi-labouring on the definition of cybercrime a topology-related approach could be adopted to achieve the same goal. The author however, did not touch on the problems and challenges of law enforcement agencies in securing and protecting cyberspace against cybercrime. This work will make efforts to vividly discuss this aspect.

Chukkol, K.S,<sup>47</sup> on his part had domesticated the whole issue of cybercrime and critically examined the application of the hitherto existing criminal statutes in Nigeria, to manage cyber insecurity. He revealed how very inadequate the Nigeria criminal law is, in tackling some aspects of cybercrime. He concluded: “The above three important new forms of computer offences, do require special legislation to handle them. Nigerian Penal Statutes i.e. traditional ones have not made provisions for them. There is the need for new laws to address them in specific terms as is

---

<sup>46</sup> Ladan M.T. (2015) Cyber-law and Policy on Information and Communications Technology in Nigeria and Ecowas. Ahmadu Bello University Press Limited Zaria. Pp.34-35

<sup>47</sup> Chukkol K.S (2010) The Law of Crimes in Nigeria. Ahmadu Bello University, Zaria. (Revised Edition)p.517

done in other jurisdictions”.<sup>48</sup> This text provided insights to this research that no matter how hard prosecution tries, the old Statutes may constitute an arm string in a case of cybercrime. This fear is however, now allayed by the enactment of the Cybercrime (Prohibition Prevention ETC) Act, 2015. This is perhaps, an answer to the prayers of the author and this work shall give an overview of this Act in chapter three ahead.

Chubey, R. K,<sup>49</sup> expressed concern in his book that enormous amount of money is being earned by the cybercriminals, either by causing huge damage to the computer systems or by stealing information which is marketable or by way of some foul play through the network. He asks the question of what constitutes a computer crime and how it can be distinguished from routine crime. He, by himself, provided the answer that the query has no legal answer because neither the IT Act 2000 nor the Indian Penal Code gives any precise or concise definition for same. His analysis is more of an overview of Indian laws as it relate to control and punishment of cyber criminality. This is of significance to this research to the extent that it reveals that the challenges are of similarity all over different countries. The fact not mentioned in his book is that the threat of cybercrime is not from the intelligence of the criminals but from the ignorance of the society and the will to fight it. This research will deal with this gap.

Rodney D. Ryder’s<sup>50</sup> book is a compendium containing evolution of law in Cyberspace. His direction is a perspective on Internet related legal issues. This book is of immense benefit to this research for creating easy access to cyberspace law, expanding the understanding of concepts and legal determination and provided an insight into the India’s rules and regulations with the United Nations Commission on International Trade Law (UNCITRAL) model law and

---

<sup>48</sup> Ibid at p.536

<sup>49</sup> Chubey, R. (2009) An Introduction to Cyber Crime and Cyber Law. Kamal Law House, Kolkata India. p.6

<sup>50</sup> Rodney, D. (2007) Guide to Cyber Laws (information Technology Act, 2000 E-Commerce, Data Protection & internet) 3<sup>rd</sup> edition, Wadhwa and Company Law publisher, Agra Nagpur New Delhi, India . p.1

related foreign legislation including intellectual property. This research will strive to explore the latest development in this area after the publication of this book.

The origins of the internet and its associated information technologies are well documented from its Military origins through to educational, commercial and later social use by Castells, M,<sup>51</sup> from this literature comes the clear message that the Internet has radically changed aspects of people's lives, but to determine the extent is difficult. It is arguable that it has only had a marginal effect, while on the other hand, mostly the post-modernist, believe that the information society has contributed to the rupturing of traditional links across time and space and has caused the demise of modernity. Yet, authors such as Castell, M.<sup>52</sup> and Giddens, A.<sup>53</sup> have steadfastly maintained that the shift towards post, late or high modernity (depending upon author) was already occurring well before the popularization of the Internet in the early 1990s.

Ashaolu, David, stated in his papers<sup>54</sup> that Nigeria's notoriety in cybercrimes worldwide is an open secret. He argued that there is hardly any crime which is not perpetrated by Nigerians more for gain than for play. He further argued that Nigeria, being Africa's most populated nation and power house, the behavior of Nigerians come under the spot light as role models and as a model of African behavior. He opined that Nigeria should therefore be at the fore of cyberspace policing in Africa. He contended that it will be pretentious to assume that with the few cybercrime prosecutions and convictions achieved by the EFCC to date, Nigeria is achieving much in the fight against cybercrimes. When compared with what obtains in other countries around the world, Nigeria is nowhere near where she should be. His explanations on the reason

---

<sup>51</sup> Castells, M. ,(1997b) *The Information Age: Economy, Society and Culture*. In: Oxford, B. (ed) *The power of identity*. (2):19. see also, Castells, M. (2000a) *Materials for an explanatory theory of the network society*: *British Journal of Sociology*, 51 (1): 5-24

<sup>52</sup> Ibid.

<sup>53</sup> Giddens, A. (1990). *The Consequences of Modernity*, Cambridge: Polity, (press) London. p.19.

<sup>54</sup> Ashaolu D ( 2011 December, 24 & 27) *Combating Cybercrimes in Nigeria I & II*. [ Web log post]. Retrieved August 8, 2015 from <http://blogs.McAsh'sThoughts>.

that the rate of convictions recorded is inversely proportional to the number of trials executed as the backward state of Nigeria's criminal justice system, while he listed the two legislations which are responsible for that aspect of Nigeria law as the criminal procedure Act<sup>55</sup> and the Evidence Act<sup>56</sup> is very revealing and helpful to this research. However, his analysis did not cover the cybercrime Act, 2015 and that area will be adequately looked into by this work.

In a United Nations General Assembly Press Release.<sup>57</sup> The nuclear disarmament committee assessing new technologies and their impact on disarmament considered as examples, information warfare, satellite technology and laser technology. To achieve a multi-dimensional strategy in addressing one weapon system, the committee is addressing questions on the potential new weapons and future forms of warfare. This Disarmament Committee opens general debate on 12 Oct, 1998 with focus on Nuclear Non- Proliferation and Small Arms. This press release provided insights to this research work to the extent that computer is not only manipulated for fraudulent making of money, but to the fact that it could also be used as a means of warfare. However, this press release did not suggest an effective law enforcement approach to tackling the problem of cyber criminality. This research will direct its efforts towards this direction.

With Richard Aldrich,<sup>58</sup> he expresses his fear over multinational corporations in the United States of America (some with annual earnings that dwarf the gross domestic product of the entire nations). In his opinion, non-governmental organization and other large groups may be able to exert significant political clout even if they are unwilling or unable to exert military might. He further explain that some or all of these organizations could additionally perpetrate harm tantamount to that of a war by using only computer and phone lines, and in ways which do

---

<sup>55</sup> Cap C41, LFN 2004. See also, Criminal Justice (Misc. Provision) Act, Cap C39, LFN 2004 and the Criminal Procedure Code.

<sup>56</sup> Cap E18, LFN 2004 effectively repealed by the Evidence Act, 2011.

<sup>57</sup> U.N. GA/DIS/3106, (9 Oct, 1998) Retrieved June 5, 2012 from [www.un.org/disarmament/WMD/Nuclear/](http://www.un.org/disarmament/WMD/Nuclear/).

<sup>58</sup> Richard, A. (1999) How Do You Know You Are at War in the Information Age?" *Houston Journal of International Law*, (fall). p. 88.

not cleanly fall within current proscriptions against the unlawful use of force. The author's fear is inspirational to this research work for the fact that it highlighted the need for a legislation which is specifically based on computer-related crime. This is to avoid a situation where a person or group of persons could conduct operations which would intrinsically seem criminal yet not violate the criminal laws of the states in which they perpetrated the conduct, and may be unreachable under existing international law. Beyond the conclusion of his study, this research will go further from his position to show that collaborative efforts of countries otherwise called Mutual Legal Assistance Treaty (MLATs) can help in this regard.

Steven Rinaldi's<sup>59</sup> paper addresses the context surrounding the question of how the United States military responds to the cyber threat facing the America military and society today. Rinaldi examines the issues of partnering and sharing sensitive information across private and governmental sectors as a central requirement of a national risk reduction and management effort in the face of the threat of cyber attack. This paper will provide for this research, fresh thinking and critical perspective on a security threat arena that increasingly captivates the headlines. This research will however discuss the trans-border or jurisdictional challenges which the paper did not mention.

Roger Molander, Peter Wilson, David Mussington and Richard Mesic<sup>60</sup>, did a draft random study prepared for the office of the Secretary of Defense of United States of America. This report revealed to a great extent that the increasing openness of cyber crime is largely attributable to the growth of interconnectedness afforded by the ever-expanding Internet. Of course, the United States of America is not the only country to be so threatened. All countries

---

<sup>59</sup> Steven, R. (2003, April) Sharing the knowledge: Government – private Sector Partnerships to Enhance Information Security. occasional paper series of the United States of America's Air Force Institute for National Security Studies. (INSS). Presented at the US air force base, Washington DC, USA.

<sup>60</sup> Roger M, Peter W. David M and Richard M. (1998) Strategic Information Warfare Rising. A draft random study prepared for the office of the Secretary of Defense of United States of America. Retrieved September 11, 2012 from <http://lumbungbuku.com>listbuku>.

that make use of computer technology and especially those connected to the Internet are vulnerable, though the level to which the United States of America has incorporated new technologies and highly networked nature of its infrastructure makes her the most vulnerable.

Although this report is a study based on the disruptions attributed to the “Chernobyl” computer virus, it is of invaluable help to this research, to the extent of its findings that better publicity about virus and the widespread use of anti-viral software, can help to reduce the vulnerability to strategic information warfare. This research will address the efforts at the global, regional and national levels at effective control of this cyber crime which the study did not discuss.

Urs, Gasser. et-al,<sup>61</sup> presented a paper and decisively dealt with the issue of young persons in today’s digital age. The paper seeks to map and explore what is known about the ways in which young users of age 18 and under search for information online, how they evaluate information, and how their related practices of content creation, levels of new literacy, general digital media usage and social patterns affects these activities. The paper reveals patterns in youth’s information seeking behavior, but also highlights the importance of contextual and demographic factors both for research and evaluation. This paper is of great assistance to this research to the extent of its revelation of the behaviors of youths as another group of users of Internet that needs to be paid attention in the development of law or control measures of cyber space misuse. This research shall however show that thus far, educational initiatives to educate youth about search, evaluation, or creation have depended greatly on the local circumstances for their success or failure. This is one area not touched by the authors.

---

<sup>61</sup> Gasser, U; Cortesi, S; Malik, M. and Lee, A. (2012. February 16,) Youth and Digital Media: From Credibility to Information Quality. Harvard Law School, Berkman Center Research Publication No. 2012-1. Retrieved June 5, 2012 from SSRN: <http://ssrn.com/abstract=2005272> or <http://dx.doi.org/10.2139/ssrn.2005272>.

In the report of the National Cyber Security Research Agenda of Netherlands, the editors, Herbert Bos, Sandro Etalle and Erik Poll<sup>62</sup> exhibited brilliance in the research work on critical aspects of cyber security and protection. This document is the result of a series of discussions about the best shape, form and content of a national research agenda in line with the National Cyber Security Strategy (NCSS). It formulates, in concrete terms, common thoughts and promising directions for a research agenda in cyber security. While all contributors firmly believe that a realization of the agenda requires ambitious funding, as well as solid governance and embedding, this document addresses only the research directions. This document proposes an ambitious National Cyber Security Research Agenda (NCSR) to boost ICT security expertise in the Netherlands through research at universities and knowledge centers, government agencies and companies active in ICT security, and to foster partnerships between these domains. The NCSR Agenda positions itself alongside the NCSS and complementary activities focused on more short-term and operational goals, such as the establishment of legal and law-enforcement frameworks to deal with cyber crime, response teams to handle cyber security incidents, threat analyses and protection of existing ICT infrastructure, awareness campaigns, and the likes. This fits well with the term of reference (TOR) of the Nigeria Cyber Working Group (NCWG) which was formally launched on 31<sup>st</sup> March 2004 by ex-president Olusegun Obasanjo. Moreover, it is in line with the recommendations of the European Union (EU) advisory board on Research & Innovation on Security, Privacy, and Trustworthiness in the Information Society (RISEPTIS, 2008). By this report, this research is enriched with the fact that there is a potential for tremendous benefits by bringing together the different sectors and stake-holders like, government, industry, knowledge centers, interest groups and universities. It also reveal that a

---

<sup>62</sup> Herbert, B; Sandro, E and Erik. P. .(2010). Trust and Security for our Digital Life. In: Report of the Committee on .National Cyber Security Research Agenda of Netherlands Published by the Netherlands home Holland. at Pp.1-4

stimulating research will also have a big impact on higher education and help in training the next generations of security experts, including PhD students trained as part of research projects, and many more Bachelor and Master students that come into contact with the field. More fundamentally, the report has expanded the horizon of this research to understand that highly visible research projects and groups help to attract students to the area. However a very important issue that the report did not mention is the fact that, Cyber security issues are no longer limited to traditional computer systems, such as personal computers (PCs) and laptops. Rather, they surface everywhere, from electricity and water supply systems to the health service, from public transport to smart cars, from implants to supply chains, and from banking and logistics to the emergency services. Addressing cyber security involves many domains of expertise, or disciplines. One do not just need technical expertise to detect and stop attacks or better still, prevent them. There is also the need for laws and regulations that better fit computer crime, and there is the need to better understand the forms and causes of cyber crime, the effectiveness of measures, including law enforcement, the underground economy, and see where economic drivers for implementing security measures are lacking and regulation may be needed. This research will substantially address this omission.

Wu, K.C's<sup>63</sup> seminar paper reveals a clear picture on the nature of cyber crimes and how to investigate such crimes by new technology and procedure. In his opinion, since new cyber crimes arise by the leap development of telecommunication and information technologies, investigators must face such challenges with a totally different thought and technical skills. He also provide case study on the methodology to break such cyber crimes in real environment by

---

<sup>63</sup> Wu, K. (2012. Monday, April, 23, ) Cyber Crime: New Challenge to Mankind Society, Introduction to the Nature of Cyber Crime and its Investigation Process. A paper presented at a course on Cyber Crime Investigation organized by Network Forensics and Law Interception Total Solution Provider ( E- Detective Solutions), held in Digital Education Institute, for Information Industry, Taiwan. atp.19.

investigators. He emphasized that the most distinct nature of cyber crime from traditional one is that it is borderless, anonymous and by the help of pervasive network technology, cyber crime is ramping over areas, regions, and countries. He opined that, for investigators, it is really hard to get the true picture of the whole crime process because of dispersed elements in different places. He presented the true profile of cyber crime in terms of process, technology behind, behavior model and mind set. He further stated the fact that Cyber Fraud is the most common and significant type of crime, and cover versatile of facets, such as fraud in cyber auction, VoIP phishing, identity stealing and many more. In this lesson note, He presented different type of real cyber crime cases, and how it happened, including criminal profiling. This paper will influence the thinking of this research to the extent of its revelations on the basic of cyber crime, and effective ways to investigate it, and, most important, it has shown a firsthand lesson from real cases that have happened as fine example. The most important point of this seminar paper to this research is that, it has provided a better understanding of these cyber frauds and their weakness. Now, the research may easily distinguish the crime model when dealing with cyber fraud and offer suggestions on how to investigate it and keep all valid legal evidence. With seminar paper, the scope of this research is now broaden to understand that even after investigating cyber crimes, with all evidence collected and are ready to be submitted to court. It is still necessary to be sure that all evidence at hand is valid and legal for the endured lawsuit process. It is in the clear view of this research now that without a legal procedure on cyber crime investigation, a law enforcement agent's hardworking effort will be fruitless. From this paper, this research is sufficiently schooled to understand the formal investigation procedure on cyber crime, difference from the legacy one, and legal requirement of evidence in the court. Revealing as Wu, K.C's presentation is, where he covered cyber crime in many different aspects, most of his emphasis is

cyber crimes from external threats. As for cyber crime from internal threat, this research will present it in depth. Traditionally this kind of cyber crime is usually neglected by the public. This work will highlight it with many case studies and show how to deal with it. It will also give a detail understanding on its nature, how to prevent it and how to lawsuit it in the court in the viewpoint of lawful enforcement agency.

In Ezeoha Abel's paper on the regulation of internet banking in Nigeria<sup>64</sup> he argues that for internet banking to assume a developmental dimension in Nigeria and for the country to be fully integrated in the global financial environment, the prevalent level of frauds in Nigeria and among Nigerians must first be addressed. It suggests that the way to do this are first to get the relevant local laws in place and in consonance with international laws and conventions, get the citizens well educated on the intricacies of internet usage and frauds, as well as the regulatory implications of wrong/fraudulent uses of the Internet, ensure that all the major background problems such as poverty, corruption and bad governance are addressed and ensure adequate interface and collaboration between Nigeria local law enforcement agents and the various international agencies that are presently pursuing the course for safe internet community. His paper is contributory to the knowledge of this work to the extent of his revelation that generally, regulating Internet banking encompasses three major issues, i.e. how bank customers are to be protected, how banks are to be protected and how the country would be protected against the negative publicity associated with the spread of Internet frauds. It is noted that the author's discussion is limited to Internet operations in banking industries alone. The scope of this work covers more extensive area beyond the limit of this paper.

---

<sup>64</sup> Ezeoha Abel (2006, April) Regulating Internet Banking in Nigeria: Some Success Prescriptions-part 2. Journal of Internet Banking and Commerce. 11(1):1-17

Rosemary Obada and Moses-Oke<sup>65</sup> clearly expressed their view in their joint paper that prior to the year 2001, the phenomenon of Internet criminal fraud was not globally associated with Nigeria. Since then, however, the country had acquired a world-wide notoriety in criminal activities, especially financial scams, facilitated through the use of the Internet. In their opinion, it is not to say that computer-related crimes were alien to the country. It is, however, remarkable that the perpetration of cyber crimes involving Nigerians and traceable to Nigeria became so rampant that questions might be legitimately raised as to why the problem became so pronounced from around that year.” It is further remarkable that the attempt to launch Nigeria into the digital age coincided with the unprecedented rise in computer-related financial crimes in the country.”<sup>66</sup> In this paper, it is argued that the problem arose as a direct consequence of the lapses in the 2001 National Policy for Information Technology (NPFIT). The argument is based on an analysis of the various provisions of the Policy, with specific focus on the lack of proactive security provisions in it and in its subsequent implementation, in the wider context of global experiences of, and efforts to deal with, cyber security breaches as at the time of the formulation and implementation of the NPFIT. The paper is of the view that in a knowledge-powered world, every individual or collective activity, including policy designs and implementations, should be guided by all the available relevant information. As such, the paper seeks to see how much Nigeria’s entry into the world of the Internet, via the *National Policy for Information Technology*<sup>67</sup>, has been guided by the available relevant information as at 2001, and how this has impacted on the country’s presence in cyber space since then, with a view to providing some insight into the ultimate cause of cyber crime in Nigeria, and consequently, how

---

<sup>65</sup> Obada R, Oke M. (2012 May) Cyber Capacity Without Cyber Security: A case study of Nigeria’s National Policy for Information Technology NPFIT) *The Journal of Philosophy, Science and Law* 12: 1-11

<sup>66</sup> Ibid at p.1

<sup>67</sup> *Nigerian National Policy for Information Technology*, (NPFIT) (2001) Federal Ministry of Science and Technology Abuja.

best to address the situation. The critical analysis of this policy by these authors is an eye opener for this work to the extent that it reveals the policy's weakness in dealing with the menace of cyber criminality. The author's argument is centered on the Nigeria's NPFIT, 2001 only, while this research will discuss many more cybercrime laws and policies of different jurisdictions but will be guided by the scope of this work.

In the submission of some scholars,<sup>68</sup> they contended in their joint paper that:

They quite disagree with the research carried out by [G. O, Odulaja and F.Wada, *Assessing Cyber crime and its Impact on E-Banking In Nigeria Using Social Theories* (2012) ] who taught that Nigeria has no legislation against these crimes, this was actually what gave birth to this research work. But further reading testifies that it is not actually true. In reference to the paper quoted earlier by Ribadu where he mentioned as the chairman of Economic and Financial Crime Commission (EFCC) that cyber crime and its vices are under the jurisdiction of EFCC. Also supported by [O.B.Longe, S.C. Chiemekwe, S. Fashola, F.Longe, and A. Omilabu, "Internet ServiceProviders and Cyber crime in Nigeria Balancing Services and ICT Development (2007) that Economic and Financial Crimes Commission (EFCC) is the body empowered by government to fight all forms of financial crimes including cyber crimes in Nigeria. They are working together with the cyber crime prevention working group. Therefore, the above expression by Wada Odulaja would better be restructured as to believe that it is not the state of absolute lawless but perhaps rarely mentioned and practiced by EFCC [Criminal Code Act Chapter 77, Laws of the Federation of Nigeria. (1990) ] which is charged with the responsibility of investigating and prosecuting of all economic and financial crimes.

This paper has shown to this research that cybercrime as a subject is truly controversial and that even up till now there is a misunderstanding among writers/scholars on this issue. This work has strived to bridge the gap in understanding by making a conceptual clarification of the term 'cybercrime'.

---

<sup>68</sup> Matanmi O, Ogunlere S, Ayinde S, Adekunle Y. (2013 May) Cyber Crimes and Cyber Laws in Nigeria. *The International Journal Of Engineering And Science (IJES)* 2 ( 4):19-25

In analyzing the above literature, efforts has been made to state, immediately after each review, the importance of the material to this research, the shortfall identified in the material and how this study seeks to fill in such gaps.

## **1.8 Organizational Layout**

This thesis is organized into six chapters. Chapter one is the general introduction of the research which covers the following aspects: Background of the study, Statement of Problem, Objective of the Research, Justification for the research, the Research Methodology, Scope and Limitation of Research, Literature Review and Organizational Layout.

Chapter two covers conceptual clarification of key terms such as: Nature of Cyber Space, Concept of Cyber Crime and Nature and Scope of Cyber Security and Insecurity. Also discussed here is Meaning of Cyber Jurisdiction, Nature and Scope of Internet and Concept of Protection while Nature and Scope of Cyber Law, finally close this chapter. In chapter three, the Role of Law in Combating Cyber Crime is highlighted along with the Development of Legal and Institutional Regimes at Global Level. The Development of Legal and Institutional Mechanisms at Regional Level are considered in detail in this chapter. Also looked at here is the Development of Legal and Institutional Frameworks at National Level where the recent Nigeria cybercrime (prohibition prevention etc) Act, 2015 including the policy and strategy is analyzed.

Chapter four exhaustively discusses the Nature of Traditional Law Enforcement Functions, the Prevention and Detection of Crime. Within this chapter, the Powers of Law Enforcement in the Prevention and Control of Crime is highlighted including the Ethical and Legal Standards in Law Enforcement on the Prevention and Control of Crime and Insecurity it concluded with Good practices (Strategies) in addressing cyber insecurity. Chapter five addresses: Problems of Information Gathering and Sharing as it relate to Cyber Techniques. It

mirrors Human, Technical and Financial/Institutional Capacity to Prevent and Control Cyber Crime. The various issues associated with Evidentiary Problems are discussed here with details on Investigative Techniques, Prosecutorial Skills and Knowledge. Also given prominence is an appraisal of the Peel Theory of Community Policing: Whether Applicable in the Context of Cyber Security and Protection. The Constitutional and Human Rights Issues as it relate to: (i) Conflicts between Law of Privacy and Free Speech (ii) Data Protection and Privacy Infringement and finally, Liability Regimes: civil and criminal are closely examined.

Chapter six is the last and concluding chapter of this research. It presents the findings, and anchors on recommendations.

## CHAPTER TWO

### CONCEPTUAL CLARIFICATION OF KEY TERMS

#### 2.1 Introduction

In order to establish criminal offences for the protection of information and communication in Cyberspace, provisions must be enacted with as much clarity and specificity as possible, and not rely on vague interpretations in the existing laws. With the new cybercrime prohibition prevention etc Act, 2015, perpetrators will be convicted for their explicit acts and not by existing provisions stretched in the interpretations, or by provisions enacted for other purposes covering only incidental or peripheral acts. In the light of the above, this chapter presents a conceptual clarification of the key terms in cyber insecurity and crime.

#### 2.2 Nature of Cyberspace

Cyberspace is complex and sometimes elusive phenomena; there is no comprehensive, globally accepted definition that separates the sensational from the sensible and scientific. Thus, the following scenarios – all of which are quit real and take place frequently in cyberspace, illustrate the range of activities that can best describe the nature of cyberspace:

##### I. Hacking and Related Activities

To some extent, the definition of hacking depends on what is asked<sup>1</sup>.

Recent studies of actual hacker crimes reveal that there are many misconceptions about hackers? In one instance, members of the United State military, testifying before the U.S. Armed Services Committee in Congress in 1994, described a ‘master spy’ that posted a major threat to U.S. security. The military chiefs feared that an East European spy ring had successfully hacked into American Ai Defence systems and learned some of its most well-guarded intelligence secrets. A 13- month investigation however, revealed that a 16 year old British music student was responsible for the break-ins. The culprit, known as the Data-stream Cowboy,

---

<sup>1</sup>Parker D. (1998.September) Fighting Computer Crime: A New Framework For Protecting Information. John Wiley & sons. Inc. Publishers.U.S.A. p.164

had downloaded dozens of military files, including details of ballistic missile research and development, and had used a company's network in California for more than 200 logged security breaches-all using a \$ 1,200 computer and modem. He was tried and convicted in 1997, and fined \$ 1,915 by a London court. After his conviction, the media offered the musical hacker considerable sums for the book and film rights to his story, but he declined, preferring to continue his musical studies and concentrate on winning a place in a leading London orchestra.<sup>2</sup>

Generally speaking, a 'hack' used to be a clever solution to a restriction.<sup>3</sup> A hack was an ingenious, but temporary, fix or 'make-do' rather than an attack on a computer system.<sup>4</sup> However, in 1960s malicious hacking started with compromising telephone systems and stealing telephone services.<sup>5</sup> It soon spread to computers and networks. When this term is extended to the individuals who practice the art of hacking, however, the definitions become murkier. The Oxford English Dictionary (1998) defines hacker as "a person who or thing that hacks or cuts roughly" or "a person who uses computers for a hobby, especially to gain unauthorized access to data".

In his book *The Hacker Crackdown*, Brice Sterling takes a rather positive view of the activity, explaining that the term *hack* 'can signify the free-wheeling intellectual exploration of the highest and deepest potential of computer systems.'<sup>6</sup> Hacking can involve the heartfelt conviction that beauty be found in computers, that the fine aesthetic in a perfect program can liberate the mind and spirit'.<sup>7</sup> This is hacking as it was defined in Steven Levy's much praised history of the pioneer computer milieu, *Hackers* published in 1994.

---

<sup>2</sup> Ibid

<sup>3</sup> Ibid p.158.

<sup>4</sup> Ibid.

<sup>5</sup> Chirillo, J. (2001) *Hack Attacks Encyclopedia: A Complete History of Hacks, Cracks, Phreaks and Spies*. John Wiley & sons. Inc. publishers. U.S.A .p. 1.

<sup>6</sup> Sterling B. (1993 November 1,) *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. Batman Publishers. Pp. 50-51.

<sup>7</sup> Ibid.

Hacking or gaining unauthorized access to computer system, programs, or data, open a broad playing field for inflicting damage.<sup>8</sup> The *New Hackers Dictionary*<sup>9</sup> offers six definitions for hacking and hacker:

(a) A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to many users, who prefer to learn only the minimum necessary; (b) A person who enjoys the intellectual challenge of overcoming or circumventing limitations; (c) A person good at programming quickly; (d) An expert in a particular language; (e) A person who programs enthusiastically; (f) A malicious meddler who tries to discover sensitive information by poking around.<sup>10</sup> On such a base hacking can manifest itself in many ugly forms including “cyber murders”. A British hacker hacked into a Liverpool hospital in 1994 and changed the medical prescriptions for the patients.<sup>11</sup> A nine-year old patient who was ‘prescribed’ a highly toxic mixture survived only because a nurse decided to re-check his prescription<sup>12</sup>. The hacker’s motive is simply that he wanted to know ‘what kind of chaos could be caused by penetrating the hospital computer. Unfortunately other patients have not been so lucky. An underworld don who was only injured in a shootout was killed by an overdose of penicillin after a hacker broke into the hospital computers and altered his prescription.<sup>13</sup>

Hacking is facilitated by many technologies, the major ones being first, packet sniffing<sup>14</sup> In fact, when information is sent over computer networks, it gets converted into hex and broken into lots of packets. Each packet is identified by a header, which contains the source, destination, size of packet, total number of packets, serial number of that packet, and more. If a hacker wants

---

<sup>8</sup>Goodman M. and Brenner S. (2000) The Emerging Consensus on Criminal Conduct in Cyberspace Oxford International Journal of Law and Information Technology 10(2): 146.

<sup>9</sup>Raymond E (1991)*The New Hacker’s Dictionary*. The MIT Press. U.S.A

<sup>10</sup>Parker, *Dop cit*. p35.

<sup>11</sup>Nagpal A. (2001, September) *Cyberterrorism in the Context of Globalisation*. Paper presented at the National Seminar on Globalization and Human Rights) sponsored by India UGC, held in India.

<sup>12</sup>Ibid.

<sup>13</sup>Ibid.

<sup>14</sup> Ibid

to see this information, he uses Packet Sniffing technology that reconverts the data from hex to the original. This technology is like putting the equivalent of a phone tap on a computer. Sniffing can be committed when a packet leaves the source or just before it reaches the destination. For this, the hacker would need to know only the internet provider's (IP) Address (the unique number that identifies each computer on a network). A packet sniffer can log all the files coming from a computer. It can also be programmed to give only a certain type of information, for example, only passwords. Second, is tempest attack,<sup>15</sup> Transient Electromagnetic Pulse Emanation Standard (TEMPEST) technology allows someone not in the vicinity to capture the electromagnetic emissions from a computer and thus view whatever is on the monitor. A properly equipped car can park near the target area and pick up everything shown on the screen. There are some fonts that remove the high-frequency emissions, and thus severely reduce the ability to view the text on the screen from a remote location. This attack can be avoided by shielding computer equipment and cabling. Third is the password cracking.<sup>16</sup> A password is a type of secret authentication word or phrase used to gain access. Passwords have been used since Roman times. Internal to the computer, passwords have to be checked constantly. So, all computers try to "cache" passwords in memory so that each time a password is needed the user does not need to be asked. If someone hacks into the memory of a computer, he can sift the memory or page files for passwords. Passwordcrackers are utilities that try to 'guess' passwords.

One way, the dictionary attack, involves trying out all the words contained in a predefined dictionary of words. Readymade dictionaries of millions of commonly used passwords can be freely downloaded from the Internet. Another form of password cracking attack is 'brute force' attack. In this attack, all possible combinations of letters, numbers and

---

<sup>15</sup> Ibid.

<sup>16</sup> Ibid

symbols are tried out one by one till the password is found out. The fourth is the buffer overflow.<sup>17</sup> This is also known as buffer overrun, input overflow and unchecked buffer overflow, this is probably the simplest way of hacking a computer. It involves input of excessive data into a computer. The excess data "overflows" into other areas of the computer's memory. This allows the hacker to insert executable code along with the input, thus enabling the hacker to break into the computer. Due to recent developments in the field of telephone and telecommunications technology such as integrated services digital network (ISDN), hacking does not only affect classic computer systems but also increasingly telephone lines, *answer-phones* and voice-mail-systems.<sup>18</sup> "Telephone hackers" dial themselves into the telephone company's local phone exchanges and are thus able to eavesdrop on the digitally led conversations in a respective part of town. In the United State of America, besides other confidential information, especially the numbers of telephone access cards (so-called calling cards) are eavesdropped on, which are then resold.<sup>19</sup>

## II. Viruses and Malicious Codes

As earlier mentioned, computers are the subjects of crime in computer virus distribution in cyber space. Trojan horse attacks, logic bombs use, and *data diddling* – the term used by Donn Parker to refer to the act of putting false data into computers.<sup>20</sup> Malicious code is any software program designed to move from computer to computer and network to network, in order to intentionally modify computer systems without the consent of the owner or operator.<sup>21</sup> It includes viruses, Trojan horses, worms, script attacks and rogue Internet code.<sup>22</sup> Computer

---

<sup>17</sup> Ibid

<sup>18</sup> Sieber U. (1998). Legal Aspects of Computer Related Crime in Information Society. European Commission. S.S. Wimbledon U.K.p.43.

<sup>19</sup> Ibid.

<sup>20</sup> Parker, D. Op.cit, p.35, at, 82

<sup>21</sup> Grimes R. (2001. August) *Malicious Mobile Code, Virus Protection for Windows*. O'Reilly Media publishers. U.S.A. p. 2.

<sup>22</sup> Ibid.

viruses have been around for almost as long as computers.<sup>23</sup> The term *computer virus* was formally defined by Fred Cohen 1984, while he was performing academic experiments on a Digital Equipment Corporation VAX computer system.<sup>24</sup> Fred Cohen is best known as the inventor of computer viruses and virus defence techniques.<sup>25</sup> Actually, a computer virus is a specific type of malicious code that replicates itself and inserts copies or new versions of itself in other programmes, when it is executed with the infected program.<sup>26</sup> It replaces an instruction in the target program with an instruction to transfer control to the virus which is stored in the memory.<sup>27</sup> Whenever the program transfer instruction is executed, it dutifully transfers control to the virus program, which then executes the replaced instructions and performs its work of inserting itself in other programs.<sup>28</sup> There are presently more than 10, 000 identified viruses that affect the personal computer (PC) and Apple operating systems. In addition, a few viruses affect other operating systems such as UNIX. There are, however, no known viruses that attack the large-scale mainframe computer operating systems.<sup>29</sup> This is probably because the virus makers have easy access to the desk top and laptop computing environments and because of the proliferation and casual exchange of software for these environments.<sup>30</sup> On such basis, a calamitous virus may delete files or permanently damage systems. A Trojan horse masquerading as a utility or animation may copy user's identities (IDs) and passwords, erase files, or release viruses.<sup>31</sup> The program may also be used for blackmail, with activation of a virus or detonation

---

<sup>23</sup>Schweitzer D.Cited by Chawki, M. (2005. April ) A Critical Look at The Regulation of Cyber Crime. A Comparative analysis with suggestions for Legal Policy, Droit-tic, 11 P.20. Available on Mohamed [chawki@hotmail.com](mailto:chawki@hotmail.com). Retrieved, June 2<sup>nd</sup>, 2012.

<sup>24</sup> Experiments with computer virus. Retrieved June 2, 2012 from. <http://all.net/books/virus/part5.html>.

<sup>25</sup>Chawki, M. Op cit,14 at 20

<sup>26</sup>Skoudis ,E. (2003. November) Malware, Fighting Malicious Code. Prentice Hall publisher, U.K. p.25.

<sup>27</sup>Parker,D.Op.cit.p.335, at, 84

<sup>28</sup>Ibid. p.83

<sup>29</sup>Ibid.

<sup>30</sup>Ibid.

<sup>31</sup>Goodman M and Brenner S.p.37, at,146.

of a digital bomb threatened unless demands are met.<sup>32</sup> A virus might cause a minor annoyance, or tremendous losses in money and productivity, or human lives, if it changes or destroys such crucial data as medical records at a hospital.<sup>33</sup> In some cases, the original software which was issued by the producing company was already infected with a virus. While viruses only spread in “host programs”, worm programs attack other computer systems independently.<sup>34</sup> An illustrative example for the possible dangers is the American “Internet worm”-case. In this case a young computer scientist created an extremely complex virus which consisted of several programs. The virus was injected into a Department of Defence research computer system. Due to a design error it replicated wildly in a similar manner as a worm, ultimately jamming more than 6,000 computers. Although the virus caused no actual damage to any files, it cost many thousands of employee hours to locate and erase this virus.<sup>35</sup>

The most famous viruses over the years are Melissa, This virus, when it was first noticed on 26th March 1999 was the fastest spreading virus the world over. The virus by itself was quite harmless. It merely inserted some text into a document at a specified time of the day. What caused the maximum harm was that the virus would send itself to all the email addresses in the victim's address book. This generated enormous volume of traffic making servers all over the world to crash. Explore-Zip, in its activities it was similar to Melissa, but there was one major difference.

Explore Zip was first discovered in June 1999, not as a virus but a Trojan. This means that it was incapable of replicating itself. Thus, the Melissa virus had more far reaching presence. Also, Explore Zip was more active. It not only hijacked Microsoft Outlook but also selected

---

<sup>32</sup> Ibid

<sup>33</sup> Ibid

<sup>34</sup> Sieber U. Op.cit. p. 39, at,49.

<sup>35</sup> Ibid.

certain files and made their file size zero subsequently reducing their data to nothing. Those files were then of no use to the user and they could not be recovered.

The Chernobyl, or PE CIH, virus activates every year on the 26th of April - on the anniversary of the Chernobyl, Ukraine's nuclear power plant tragedy. The virus wipes out the first megabyte of data from the hard disk of a personal computer thus making the rest of the files of no use. Also, it also deletes the data on the computer's Basic Input-Output System (BIOS) chip so that the computer cannot function till a new chip is fitted or the data on the old one is restored. Fortunately, only those BIOSes, which can be changed or updated, face a threat from this virus. "I Love you" virus, Pakistani Brain, Stoned-Marijuana, this virus was originally written in New Zealand and would regularly display a message, which said, 'YourPC is stoned. Legalize Marijuana. As for Cascade virus which is also called 'Falling Letters' or '1701'. It initially appeared as a Trojan horse in the form of a program designed to turn off the Num-Lock light on the user's keyboard. In fact, what it did was to make the characters on the screen drop in a heap to the bottom of the screen. And finally, Michelangelo virus is titled after famous Italian Renaissance artist Michelangelo Buonarroti. It gets activated every year on the artist's birthday - 6th March.

### **III. Online Fraud**

All stages of computer operations are susceptible to criminal activity, either as the target of the fraud, the instrument of the fraud, or both.<sup>36</sup> Input operations, data processing, output operations and communications have all been utilized for illicit purposes.<sup>37</sup> The more common types of computer fraud are:<sup>38</sup>

---

<sup>36</sup>Wells, J. [2002] Cybercrime ranges from computer fraud, theft and forgery. The Computer and Internet Fraud Manual (Annual) publication. Austin, Texas, p. 3.

<sup>37</sup> Retrieved June 6, 2012. From <<http://www.fraud.org/internet/lt00totstats.htm>>

<sup>38</sup>Ibid p. 8.

### **(A) Fraud by Computer Manipulation**

Intangible assets that are represented in data format, such as money-on-deposit, or hours of work, are the most common targets of computer related fraud. Modern business is replacing cash with deposits transacted on computer systems, creating an enormous potential for computer fraud. The organized criminal community has targeted credit card information, as well as personal and financial information about clients. The sale of this information to counterfeiters of credit cards and travel documents has proven to be extremely lucrative.<sup>39</sup>

On such a base, improved remote access to databases allows the cybercriminals to commit several types of fraud such as: (a) Input manipulation; (b) Program manipulation; (c) Output manipulation.<sup>40</sup>

### **(B) Computer Forgery and Desktop Counterfeiting**

When a criminal alters data stored in a computer system, the crime committed may be forgery. In this case computer systems are the target of criminal activity. However, computers can also be used as tools with which to commit forgery. A new generation of fraudulent alteration emerged when computerized colour laser copies became available. These copies are capable of high resolution copying-modifying of documents, and even the creation of false documents without benefit of an original.<sup>41</sup> Moreover, they produce documents whose quality is indistinguishable from that of authentic documents except by an expert.<sup>42</sup>

### **(C) Modifications of Data or Programmes**

This category of criminal activity involves either direct or covert unauthorized access to a computer system by the introduction of malicious software.<sup>43</sup> The unauthorized modification of

---

<sup>39</sup>Ibid

<sup>40</sup>Ibid

<sup>41</sup>Chawki, M. Op. cit. p. 14, at, 23

<sup>42</sup> Ibid

<sup>43</sup>Wells, J. p. 42, at, Pp. 9-10

computer data or functions, with the intent to hinder normal functioning of the system, is clearly criminal activity and is commonly referred to as computer sabotage.<sup>44</sup> It can be the tool for gaining economic advantage over a competitor, or promoting the illegal activities of ideologically motivated terrorists or for stealing data or programmes for extortion purposes.<sup>45</sup>

In a case,<sup>46</sup> a computer operations supervisor at a bank in New Jersey used a utility program to increase the balances of several friends' accounts. The friends withdraw the money as it arrived, and the supervisor destroyed the withdrawal slips. His plan was to stop the thefts before the end of the current audit period to avoid detection. His friends, however, were too greedy to stop and forced him to proceed further. When the auditors found the logged fraudulent transactions in the balance computer system (which the supervisor did not know about), they investigated to see who had the ability to cause the discrepancies. The supervisor was the only one to pick the bill.

In another case<sup>47</sup> in Germany, a complex invoice manipulation was committed as early as 1974 by a programmer who carried out salary manipulations worth over DM 193,000 through changes of the salary data as well as the book-keeping and balance sheet programs of his company. Using a program written especially for this purpose, he entered the information on the salaries of fictitious people into the data memories containing company salary information and entered his own account as the account to which the fictitious salaries should be transferred.

These salary manipulations would have been discovered by the company because normally, the computer prepared wage-slips, checklists, account summaries, and balances sheets which were carefully checked. In order to prevent discovery by these control printouts, the

---

<sup>44</sup> Ibid

<sup>45</sup> Ibid

<sup>46</sup> Parker, D.Opcit,p.35, at.52

<sup>47</sup> Sieber U.Opcit, p.39,at 45.

offender first made adjustments in the salary payments program to ensure that no pay-slips were printed for payments to the fictitious employees so that the payment did not appear in the checklists produced by the computer. By further manipulation of the program which produced the company's accounting summaries and balance sheets, the perpetrator finally succeeded in having the embezzled amounts deducted from the income tax to be paid to the tax office. Thus, the sums did not appear as deficient amounts in the company's accounting summaries and balance sheet.

#### **(D) Online Auction Fraud**

Many Internet marketplaces conduct transactions by using methods of auctions or exchanges in order to make potential buyers and sellers meet and conclude a deal.<sup>48</sup> However, one of the most types of cyber fraud is online 'auction' fraud.<sup>49</sup> Normally when thinking about the term, the English auction comes to mind. This is an auction initiated by a seller where higher and higher bids are made orally by bidders. When no further bids are heard the auctioneer lets the hammer fall and the highest acquires the item offered. As we see nowadays in the cyberspace, there are many types of transactions that in different ways resemble this English auction.

There are actually many examples of Internet marketplaces which may be operated by an independent intermediary or be set up by the party taking the initiative in the transaction. The vendor may be describing the products in a false or misleading manner, or may take orders and money, but fail to deliver the goods.<sup>50</sup> Or he may supply counterfeit goods instead of legitimate ones.<sup>51</sup> One of the most famous types of fraud is investment fraud.<sup>52</sup> Thousands of online

---

<sup>48</sup>Ramberg C. [2002] *Internet Marketplaces, The Law of Auctions and Exchanges Online*. Oxford University Press U.K. p. 36.

<sup>49</sup> See, Oxford Dictionary of Computing (Fourth Edition (1996) Clays Ltd. U.K. (Example of interesting change sites are: eBay, Bid let, Goindustry.com, Metalsite, and Autodaq.)

<sup>50</sup>Goodman M and Brenner S.Opcit, p.37, at 147.

<sup>51</sup>Ibid

investment e-mails have appeared on the Internet in recent years. Many offer investors seemingly unbiased information free of charge about featured companies or recommending ‘stock picks of the month.’ While legitimate online e-mails can help investors gather valuable information, some e-mails are tools for fraud<sup>53</sup>.

In fact, some companies pay the persons who send online e-mails cash or securities to ‘tout’ or recommend their stocks. While this is against the law, the federal securities laws in United States require the e-mails to disclose who paid them, the amount, and the type of this payment.<sup>54</sup>

However, many fraudsters fail to do so. Instead, they’ll lie about the payments they received, their independence, their so-called research, and their track records.<sup>55</sup> The emails masquerade as sources of unbiased information, when they stand to profit handsomely if they convince investors to buy or sell particular goods.<sup>56</sup>

#### **(E) Electronic-Mail Forgery**

E-mail spoofing or forgery is the term applied to the counterfeiting and forging of e-mail messages, but the euphemism doesn’t fully convey the insidious nature of the crime.<sup>57</sup> The sheer size and anonymity of cyberspace demand the information passing through the Internet be subjected to both authentication and accountability controls.

The most effective way to invoke these controls is through the use of independent trusted third parties called *certificate authorities* (CAs), which provide digital signatures and encrypted communication of electronic authentication certificates. CAs authenticates the identities of users

---

<sup>52</sup>Ibid.

<sup>53</sup>Internet Fraud, How to Avoid Internet Investment Scams, Retrieved, June 5, 2012. From <<http://www.sec.gov/investor/pubs/cyberfraud.htm>>

<sup>54</sup> Ibid

<sup>55</sup>Ibid

<sup>56</sup>Ibid

<sup>57</sup>Parker D.Op.cit, p.35, at.123

by exchanging personal information known only to be the communicating parties.<sup>58</sup> CAs log messages for later audit, and they use investigative software to trace the source of messages. In addition, they initiate criminal and civil litigation for wrongdoing.<sup>59</sup>

A famous case of e-mail forgery occurred in California in 1996.<sup>60</sup> The spurned girlfriend of the chief executive officer (CEO) of a large software firm won a wrongful termination suit against the company and collected a \$ 100,000 settlement. Until she was fired, she was the girlfriend of an executive assistant to a vice president in the company. Among other things, she was responsible for changing her supervisor's passwords, providing him with new codes, and managing his e-mail account. A key piece of evidence in the termination suit was copies of an e-mail message her supervisor, the vice president, allegedly sent to the CEO that said, "I have terminated Adelyn per your request." The CEO denied that he had fired the woman because she refused to have a relation with him, maintaining that the e-mail message was a spoof. In 1997, the company challenged the veracity of the e-mail messages.

The district attorney subsequently indicated, creating false documents, and perjury in a superior court. The company found a computer audit records showing back and forth between the vice president's and another employee's e-mail accounts on the day and time that the questionable e-mail message was sent. The vice president proved that he was driving his car and talking on his cellular phone at the time the e-mail message was sent. Even though investigators were unable to retrieve the last numbers dialed from the woman's home computer, she was convicted and sentenced to one year in prison and fined \$100,000.

---

<sup>58</sup> Ibid

<sup>59</sup> Ibid

<sup>60</sup> *Ibid at*, p. 124.

#### IV. Cyberstalking, Harassment and Hate Speech

The neologism “*stalking*,” In fact, the word stalk has the meaning of both the act of following one’s prey and walking stealthily. To label someone a stalker has been, at least from the sixteenth century, to imply he or she is a prowler or a poacher. When the media appropriated the word to describe those who pestered and harassed others they provided a new focus for this ancient indictment. Stalking is now a part of the culture language. It has become a category with which people describe and understand the experiences.

If someone is repeatedly followed by a stranger, or is distressed at receiving numerous unwanted letters from an estranged partner, in today’s world, they are likely to describe themselves as being stalked. Looking back over their life they may now recall having been stalked in the past. In California, a 50-year-old former guard...used the Internet to solicit the rape of a women who rejected his romantic advances...[He] terrorized his 28year old-victim by impersonating her in various Internet chat rooms and online bulletin boards , where he posted , along with her telephone number and address, messages that she fantasized of being raped. On six occasions, sometimes in the middle of the night men knocked on the woman’s door saying they wanted to rape her.

Cyberstalking has entered the English lexicon, connotating a paranoid tinged world of malicious and instructive activity on the Internet.<sup>61</sup> As US Attorney General Janet Reno noted in the report prepared by the Department of Justice in 1999, many of the attributes of the Internet – low cost, ease of use and anonymous nature- make it an attractive medium forfraudulent scams, child sexual exploitation and cyber stalking. She also noted that some conduct involving annoying, menacing behaviour may be a prelude to stalking and violence and should be treated

---

<sup>61</sup>Boon J. [2002.April] *Stalking and Psychosexual Obsession: Psychological Perspectives for Prevention, Policing and Treatment* John Wiley& sons, Ltd. U.K. p. 206.

seriously.<sup>62</sup> Meloy and Gothard defined it, or as they prefer to call it obsessional toll owing, as ‘an abnormal or long term pattern of threat or harassment directed toward a specific individual’.<sup>63</sup>

The pattern of threat or harassment was further clarified as being ‘more than one overt act of unwanted pursuit of the victim as being harassing’, although more than one may seem generous rendering of a long term pattern.<sup>64</sup> Meloy further states that in distinction to legal definitions, it was designed to further scientific investigation and clinical understanding.<sup>65</sup> Cyber stalking also called online stalking or online victimisation, shares important characteristics with offline stalking.<sup>66</sup>

The similarities are that, first, the majority of cases involve stalking by former intimates, although stranger stalking certainly occurs in the real world and in cyberspace; second, most victims are women and most stalkers are men.<sup>67</sup> And third, stalkers are believed to be motivated by the desire to control the victim. Major differences include, first, offline stalking requires the stalker and victim to be located in the same geographic area whereas cyber stalkers may be located in the same city or across the country; second, technologies make it easier for a cyber stalker to encourage third parties to harass and/or threaten a victim; and third, technologies lower the barriers to harassment and threats, and a cyber stalker does not need to physically confront the victim.<sup>68</sup>

---

<sup>62</sup> Ibid

<sup>63</sup> Mullen P. (2000. April 27). *Stalkers and their Victims (First edition)* Cambridge University Press. U.K , p. 7

<sup>64</sup> Ibid

<sup>65</sup> Ibid

<sup>66</sup> Boon J. Op.cit, p.48, at. 218.

<sup>67</sup> Ibid

<sup>68</sup> Ibid

Cyber staking, harassment, hate and racist speech perpetrated over computer networks may or may not be criminal activities, depending on the jurisdiction.<sup>69</sup>

## **V. Cyberterrorism**

Cyberterrorism is the convergence of terrorism and cyberspace. It has been defined as ‘premeditated, politically, motivated attack against information, computer systems, computer programs, and data which result in violence against non combatant targets by sub national groups or clandestine agents.’<sup>70</sup>

Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Cyberspace is constantly under assault.<sup>71</sup> Cyber spies, thieves, saboteurs, and thrill seekers break into computer systems, steal personal data and trade secrets, vandalize Web sites, disrupt service, sabotage data and systems, launch computer viruses and worms, conduct fraudulent transactions, and harass individuals and companies.<sup>72</sup> These attacks are facilitated with increasingly powerful and easy-to-use software tools, which are readily available for free from thousands of Web sites on the Internet.<sup>73</sup>

Many of the attacks are serious and costly. In 1998,<sup>74</sup> Spanish protestors bombarded the Institute for Global Communications (IGC) with thousands of bogus e-mail messages. E-mail

---

<sup>69</sup>Goodman, M and Brenner, S. Op.cit.p.37, at.149

<sup>70</sup>Ibid

<sup>71</sup>Denning D. [2000. May 23,] Cyberterrorism ( U.S.A, Special Oversight Panel on Terrorism), P.2 Retrieved August 8, 2012, from <http://www.stealth-iss.com>>documents.

<sup>72</sup> Ibid

<sup>73</sup> Ibid

<sup>74</sup>Defining cyberterrorism, Retrieved August 8, 2012 from <[http://www.asianlaws.org/cyberlaw/library/cc/def\\_ct.htm](http://www.asianlaws.org/cyberlaw/library/cc/def_ct.htm)>

was tied up and undeliverable to the internet service providers (ISP's) users, and support lines were tied up with people who couldn't get their mail. The protestors also spammed IGC staff and member accounts, clogged their Web page with bogus credit card orders, and threatened to employ the same tactics against organizations using IGC services.<sup>75</sup> In the same year a 12-year-old boy successfully hacked into the controls for the huge Roosevelt Dam on the Salt River in Arizona, USA.<sup>76</sup> He might have released floodwaters that would have inundated Mesa and Tempe, endangering at least 1 million people.<sup>77</sup> And finally in 2002, numerous prominent Indian web sites were defaced.<sup>78</sup> Messages relating to the Kashmir issue were pasted on the home pages of these web sites.<sup>79</sup> The Pakistani Hackers Club, led by “Doctor Neukar” is believed to be behind this attack.

## **VI. Cyber theft**

There are many different types of cyber theft, or ways of using ICTs to steal information, money, or other valuables. The offences include:<sup>80</sup>

*Embezzlement*, which involves misappropriating money or property for the own use of the perpetrator, that has been entrusted to him by someone else. For example an employee who uses his or her legitimate access to the company's computerized payroll system to change the data so that he is paid extra, or who move funds out of company bank accounts into his own personal account. Some of the sharp practices on the cyberspace are:

---

<sup>75</sup> Ibid

<sup>76</sup> Nagpal A. [2001 September]. *Cyberterrorism in the Context of Globalisation*. A Paper presented at the National Seminar on Globalization and Human Rights) sponsored by India, UGC, held in India.

<sup>77</sup> Ibid

<sup>78</sup> Ibid

<sup>79</sup> Ibid

<sup>80</sup> Shinder D. *Find Phone & Address information, medical practice...Retrieved July 23, 2012. From [www.healthgrades.com](http://www.healthgrades.com)>.> Philadelphia.*

- a. *Domain Name System (DNS) cache poisoning*, a form of unauthorized interception in which intruders manipulate the contents of a computer's DNS cache to redirect network transmissions to their own servers.
- b. *Unlawful appropriation*, which differs from the embezzlement in that the criminal was never entrusted with the valuables but gains access from outside to company and transfer funds or modifies documents.
- c. *Plagiarism*, which is the theft of someone else's original writing with the intent of passing it off as one's own.
- d. *Piracy*, which is the unauthorized copying of copyrighted software, music, movies, art, books, and so on, resulting in loss of revenue to the legitimate owner of the copyright.<sup>81</sup>

In fact, the unauthorised copying and use of *computer programs* – often called theft of software or software is also inclusive in this practice.

Piracy – at first involved, in accordance with the historic development of computer technology, the copying of individual software which frequently contains important internal company know-how. Therefore software theft overlaps with computer espionage in many cases. For instance, the German “debit collection program case” is an example for the copying of individual software which led to the first decision of the Bundesgerichtshof concerning the possibility of copyright protection: Because of the copying of its central computer program and the following low price sale by the perpetrator, the victimized “debt collection company got into a situation that threatened its existence”<sup>82</sup>

Identify theft, is the practice in which the cyberspace is used to obtain a victim's personal information, such as Social Security and driver's numbers, in order to assume that person's

---

<sup>81</sup>Sieber, U. Op.cit,p. 39, at,45

<sup>82</sup> Ibid

identity to commit criminal acts or to obtain money or property or to use credit cards or bank accounts belonging to the victim.<sup>83</sup> In March 2002, Federal agents arrested a Jacksonville, Florida man for identify theft in connection with stealing personnel records of 60,000 Prudential Insurance Company employees from a computer database. The man was a former IT employee for Prudential, and he attempted to sell the database information over the Internet for the purpose of obtaining fraudulent credit cards using the stolen identities.<sup>84</sup>

### 2.3 Concept of Cybercrime

Generally speaking, computers play four roles in crimes: They serve as objects, subjects, tools, and symbols.<sup>85</sup> Computers are the objects of crime when they are sabotaged or stolen. There are numerous cases of computers being shot, blown up, burned, beaten with blunt instruments, kicked, crushed and contaminated.<sup>86</sup> In one such case in San Francisco, an electrical transformer in the basement of a building exploded, causing a poisonous liquid coolant to be released. The computers in the building continued to operate, but the fire department would not allow anybody to enter the building to tend to them, which rendered the information unavailable.<sup>87</sup> The damage may be intentional, as in the case of an irate taxpayer who shot a computer four times through the window of the local tax office.<sup>88</sup> Or unintentional, as in the case of a couple who engaged in sexual intercourse while sitting on computer.

Sabotage destroys information, or at least makes it unavailable.<sup>89</sup> 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 subjects

---

<sup>83</sup>, U.S. Department of Justice (2002. march) The Foreign Born Population in the United States. Press Release. Retrieved May 26, 2012 from <https://books.google.com.ng>

<sup>84</sup> Ibid

<sup>85</sup> Johnson D and Post D. [1996] *Law and Borders: The Rise of Law in Cyberspace*. Stanford Law Review n (1378):16

<sup>86</sup> Ibid

<sup>87</sup> Ibid

<sup>88</sup> Ibid

<sup>89</sup> Ibid

of attacks. The third role of computers in crime is as tools-enabling criminals to produce false information or plan and control crimes. In fact criminals may use computers, graphics software, and colour printers to forge documents. Criminals who create automated crime software and those who purchase and use the software will be using their computers as tools to commit crimes. Finally, computers are also used as symbols to deceive victims. In a \$ 50 million securities-investment fraud case in Florida, a stock broker deceived his victims by falsely claiming that he possessed a giant computer and secret software to engage in high-profit arbitrage. In reality, the man had only a desktop computer that he used to print false investment statements. He deceived new investors by paying false profits to early investors with money invested by the new ones.<sup>90</sup>

In the United States of America, police departments are establishing computer crimes units, and cybercrime makes up a large proportion of the offences investigated by these units. The National Cybercrime training Partnership (NCTP) encompasses Local, State, and Federal law enforcement agencies in the United States.<sup>91</sup> The International Association of Chiefs of Police (IACP) hosts an annual Law Enforcement Information Management training conference that focuses on IT security and cybercrime.<sup>92</sup> The European Union has created a body called the forum on Cybercrime, and a number of European states have signed the Council of Europe's Convention on Cybercrime treaty, which seeks to standardize European laws concerning cybercrime. From this perspective, each organization and the authors of each piece of legislation have their own ideas of what cybercrime is-and is-not. These definitions may vary a little or a lot. To effectively discuss concept of cybercrime, however, there is need for a working

---

<sup>90</sup> Denning, D.Op.cit, p.52, *at*.16.

<sup>91</sup> Jody R. (2003) International Guide to Combating Cybercrime. Retrieved June 8, 2012. From <<http://www.nctp.org>>.

<sup>92</sup> IACP Newsletter Retrieved June 8, 2012 from <http://www.theiacp.org/>

definition. This work will therefore start with a broad, general definition and then define specific one.

When speaking about concept of cybercrime, it is usual to speak about two major categories of offences: In one, a computer connected to a network is the target of the offence; this is the case of attacks on network confidentiality, integrity and/ or availability.<sup>93</sup>The main goal of Internet security is to keep proprietary information confidential, to preserve its integrity, and to maintain its availability for those authorized to view that information. When information is accessed and examined by unauthorized individuals, it is no longer confidential.

By connecting to the Internet organizations, they will have made their information assets far more vulnerable to unauthorized access and breaches of confidentiality. If data are tampered with, modified, or corrupted by intruders there is a loss of information integrity. Sometimes this can happen inadvertently, but most often it is the intentional act of a hacker or a disgruntled employee seeking revenge.

Finally, if information is deleted or becomes inaccessible to authorized users, there is a loss of availability.<sup>94</sup>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.<sup>95</sup>Cybercrime ranges from computer fraud, theft and forgery to infringements of privacy, the propagation of harmful content, the falsification of prostitution, and organized crime.<sup>96</sup>

---

<sup>93</sup>Spinello R. [2002. June 30] *Regulating Cyberspace: The Policies and Technologies of Control* Praeger Publishing .U.S.A. p. 107.

<sup>94</sup> Ibid

<sup>95</sup> Goodman M and Brenner S. *Op.cit*, p.38

<sup>96</sup> Ibid

In many instances, specific pieces of legislation contain definitions of terms. However legislators don't always do a good job of defining terms.<sup>97</sup> Sometimes they don't define them at all, leaving it up to law enforcement agencies to guess, until the courts ultimately make a decision.<sup>98</sup> One of the biggest criticisms to the definition of computer crime conducted by the U.S Department of Justice (DOJ) is of its overly broad concept. The (DOJ) defines computer crime as 'any violation of criminal law that involved the knowledge of computer technology for its perpetration, investigation, or prosecution.'<sup>99</sup> Under this definition, virtually any crime could be classified as a computer crime, simply because a detective searched a computer data base as part of conducting an investigation.

One of the factors that make a hard-and-fast definition of cybercrime difficult is the jurisdictional dilemma.<sup>100</sup> Laws in different jurisdictions define terms differently, and it is important for law enforcement officers who investigate crimes, as well as network administrators who want to become involved in prosecuting cybercrime that are committed against networks, to become familiar with the applicable laws.<sup>101</sup>

Also, one of the major problems with adequately defining cybercrime is the lack of concrete statistical data on these offences. In fact, reporting crimes are voluntary.<sup>102</sup> David Garland argues that 'today's world of crime control and criminal justice was not brought into being by rising crime rates or by a loss of faith in penal welfarism, or at least not by these alone.

---

<sup>97</sup>Ibid

<sup>98</sup>Shinder D. (2002) *Scene of the Cybercrime*. Retrieved July 9, 2012 from <http://www.store.elsevier.com>.

<sup>99</sup>Ibid

<sup>100</sup>Chawki M. A Critical Look at the Regulation of Cybercrime-Computer Crime Retrieved June 9, 2012.

<[http://www.findarticles.com/p/articles/mi\\_m2194/is\\_8\\_70/ai\\_78413303](http://www.findarticles.com/p/articles/mi_m2194/is_8_70/ai_78413303)>

<sup>101</sup>Shinder.D,Op cit,p.55,at, 6.

<sup>102</sup>Garland D. ), [2001].*The Culture of Control: Crime and Social Order in Contemporary Society*. The University of Chicago Press.Pp.64-88

These were proximate causes rather than the fundamental processes at work. It was created instead by a series of adaptive responses to the cultural and criminological conditions of late modernity conditions which included new problems of crime and insecurity, and new attitudes towards the welfare State. But these responses did not occur outside of the political process, or in a political and cultural vacuum.

On the contrary, they were deeply marked by the cultural formation that he describes as ‘crime complex’; by the reactionary politics that have dominated Britain and America during the last twenty years; and by the new social relations that have grown up around the changing structures of work, welfare and market exchange in these two late modern societies. This means that the figures are almost certainly much lower than the actual occurrence of networked-related crime.<sup>103</sup>

In many cases, crimes that legislators would call cybercrimes are just the ‘same old stuff’, except that a computer network is somehow involved. The computer network gives criminals a new way to commit the same old crimes. For example, the Internet is a non secure network with more than one hundred million users around the world. One of the Internet’s greatest strengths is its open anonymous nature which is also its greatest weakness, making it ripe for abuse and attracting attention from an array of unsavoury individuals and advocacy groups including terrorists, neo-Nazis, pornographers, and pedophiles. Fraudsters of every stripe engage in securities boiler room operations, illegal gambling, Ponzi pyramid schemes, credit card fraud, and a variety of other illicit activities.<sup>104</sup> Existing statutes that prohibit these acts can be applied

---

<sup>103</sup>Shinder D, Op.cit, p.55,at 6.

<sup>104</sup>Parker, D. Op.cit, p.35 at,114

to people who use a computer to commit them as well as to those who commit them without the use of a computer or network.<sup>105</sup>

In other cases, the crime is unique and came into existence with the advent of the network. Hacking into computer systems is an example; while it might be linked to breaking and entering a home or business building, the elements that comprise unauthorized computer access and physical breaking and entering are different.

Most U.S states have laws pertaining to computer crime. These statutes are generally enforced by state and local police and might contain their own definitions of terms. Texas Penal Code's Computer Crime section, defines only one offence which is breach of Computer Security as: '(a) A person commits an offence if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner'.<sup>106</sup>

California Penal Code, on the other hand, defines a list of eight acts that constitute computer crime, including altering, damaging, deleting, or otherwise using computer data to execute a scheme to defraud, deceiving, extorting, or wrongfully controlling or obtaining money, property, or data using computer services without permission, disrupting computer services, assisting another in unlawfully accessing a computer, or introducing contaminates into a system or network.<sup>107</sup> Thus, the definition of cybercrime under state law differs, depending on the state. Perhaps, one should look to international organizations to provide a standard definition of cybercrime.

---

<sup>105</sup>Ibid

<sup>106</sup>Texas Penal Code. Retrieved June 9, 2012 from <<http://www.capitol.state.tx.us/statutes/docs/PE/content/word/pe.007.00.000033.00.doc> >

<sup>107</sup>Section 502. California Penal Code

At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined thus:<sup>108</sup>

‘(a) Cybercrime in a narrow sense: Any illegal behaviour directed by means of electronic operations that targets the security of computers systems and the data processed by them.

(b) Cybercrime in a broader sense: 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 disturbing information by means of a computer system or network’.

These definitions, although not completely definitive, do give a good starting point to the extent that it has some international recognition and agreement for determining just what is meant by the term “*cybercrime*”. Cybercrime, by these definitions, involves computers and networks. In cybercrime, the “cyber” component usually refers to perpetrating qualitatively new offences enabled by information technology or integrating cyberspace into more traditional activities.<sup>109</sup>

## **2.4 Nature and Scope of Cybersecurity and Insecurity**

In order to understand the changes that ICTs introduces into criminal activity, it is important to consider a hypothetical situation: One can analogize a denial of service attack to using the telephone to shut down a supermarket business, by calling the business’ telephone number repeatedly, persistently without remorse. Thereby preventing any other caller from getting through to place their orders. On such a base, the nature of cyberspace lets someone carry

---

<sup>108</sup>Tenth United Nation Congress on the Prevention of Crime and the Treatment of Offenders, (2000. April)Vienna. Retrieved June 12, 2012. From <<http://www.uncjin.org/Documents/congr10/4r3e.pdf>>

<sup>109</sup>Goodman M.and Brenner S.Op.cit, p.37 at 145.

out an attack such as this easily and with very little risk of apprehension, so easy, in fact, that a 13 year-old hacker used a denial of service attack to shut down a computer company.<sup>110</sup>

In addition to the increased scale of criminal activity the cybercrime offers, it also has a tendency to evade traditional offence categories. While some of its categories consist of using ICTs to commit traditional crimes, it also manifests itself as new varieties of activity that cannot be prosecuted using traditional offence categories.<sup>111</sup> The dissemination of the “Love Bug” virus illustrates this. Virus experts quickly traced this virus to the Philippines. Using Information supplied by an Internet service provider, agents from the Philippines’ National Bureau of Investigation and from the Federal Bureau of Investigation (FBI) identified individuals suspected of creating and disseminating the ‘Love Bug’.<sup>112</sup>

However, they ran into problems with their investigation: The Philippines had no ICTs laws, so creating and disseminating a virus was not a crime.<sup>113</sup> Therefore, the law enforcement officers had hard time convincing a magistrate to issue a warrant to search the suspects’ apartment.<sup>114</sup> Later on the suspected author of the virus could not be prosecuted under the repertoire of offences defined by the Philippines criminal code.<sup>115</sup>

On such a basis cybercrime’s ability to morph into new and different forms of antisocial activity that evade the reach of existing penal law creates challenges for legislations around the world.<sup>116</sup> Studies of cyber criminals reveals seven significant profiles. Unfortunately, however, no criminal fits exclusively in any one profile. Instead, the profiles overlap one another in fuzzy relationships. (A) Pranksters; (b) Hackers; (c) Malicious hackers; (d) Personal problem solvers;

---

<sup>110</sup>Gibson S. *The Strange Tale of the Denial of Service*. Retrieved June 6, 2012 from <<http://grc.com/dos/grcdos.htm>>

<sup>111</sup>Bicknell C. [,2000 August], *Sex.Com : It Wasn't Stolen*. Retrieved June 10, 2012. From <<http://www.mediaesq.com/new31857.php>>

<sup>112</sup>Schweitzer D.Op.cit,p.40

<sup>113</sup>Leyden J. *Love Bug Suspect Released* [2000. May], Retrieved June 10, 2012 from <<http://www.vnunet.com/news/1101024>>

<sup>114</sup>Goodman M and Brenner S.Op.cit, p,37 at, 153.

<sup>115</sup>Ibid

<sup>116</sup>Ibid

(e) career criminals; (f) extreme advocates; (g) malcontents, addicts, and irrational and incompetent people.<sup>117</sup> Criminals have the ability of exploiting gaps in their own country's penal law in order to victimize their fellow citizens with impunity.<sup>118</sup> Also, cybercriminals can exploit gaps in penal laws of other countries in order to victimize the citizens of those, and other, nations; as the 'Love Bug' episode demonstrated, cybercrime is global crime.<sup>119</sup>

To determine the scope of cyber insecurity, it is important to know how much crime is committed as this might help to decide how much to spend on security. Estimates by security experts of annual losses from computer crime range from \$555 million to more than \$13 billion,<sup>120</sup> but there are actually no valid statistics on the losses from this type of crime, because no one knows how many cases go unreported.<sup>121</sup> Even when the victims of computer crimes are aware of the crimes, they are usually reluctant to report their losses, especially if those losses can be easily hidden.<sup>122</sup>

Victims can lose more from reporting crimes than they lose from the crimes themselves. Embarrassment, key staff diverted to prepare evidence and testify, legal fees, increased insurance premiums, and exposure of vulnerabilities and security failures can all result from reporting computer crime incidents.<sup>123</sup>

However, the results of national surveys in the U.S.A, bear out the picture that cybercrime is consistently and dramatically on the increase. In fact, some surveys don't focus on the incidence of cybercrime, but on the extent to which the public is concerned about cybercrime.

---

<sup>117</sup>Chawki, M. Op.cit. p.14, at, 13

<sup>118</sup>US Department of Justice. [ 1999] *Report on Cybertalking*. Retrieved June 12, 2012 from <<http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm>>

<sup>119</sup>Goodman M and Brenner S. Op.cit. p.38,at,154

<sup>120</sup>ParkerD. Op.cit, p.35, at,10.

<sup>121</sup>McConnell International E-Lert, [2001. Feb.] *Combating Cybercrime : A Proactive Approach*. Retrieved June 12, 2012,from <<http://www.mcconnellinternational.com/pressroom/elert.cfm>>

<sup>122</sup>UNESCO [2000]. *Les Dimensions Internationales du Droit du Cyberspace* (Paris, Economica), Cited by Chawki, M. Op.cit. at.13

<sup>123</sup>Parker D. Op.cit.p.35, at, 10

This may be due to the theory that public opinion is an important driver of national policy. In a February 2001 survey of Americans, two contradictory views emerged: The first is that many Americans do not trust their government and its agencies very much. Yet the second strong strain of opinion is that Americans are quite willing to grant to law enforcement agencies and the Federal Bureau of Investigation (FBI) the right to intercept the email of criminal suspects, perhaps because Americans are concerned about crime, especially new ways to perpetrate crime using the Internet.

While a majority of Americans approve of email interception to fight crime, only 21% of all Americans have heard about Carnivore, the FBI's digital surveillance tool.<sup>124</sup> One of the famous cited national surveys for the United States is the 'Computer Crime and Security Survey' conducted by the Computer Security Institute<sup>125</sup> with the participation of the San Francisco branch of the Federal Bureau of Investigation's Computer Intrusion Squad.<sup>126</sup> The CSI/FBI survey which has been conducted in 2004, reports the results of questionnaire administered to 494 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities. One area the survey explores is security breaches; the questionnaire asks the respondents if they have experienced breaches of information security in the last year.<sup>127</sup>

The percentage of the respondents answering that their organization experienced unauthorized use of computer systems in the last 12 months declined to 53 percent, the smallest percentage since this question first appeared in the survey in 1999. Moreover, the percentage of

---

<sup>124</sup>Pew Internet and American Life Project, Retrieved June 6, 2012 from <[http://www.pewinternet.org/pdfs/PIP\\_Fear\\_of\\_crime.pdf](http://www.pewinternet.org/pdfs/PIP_Fear_of_crime.pdf)>

<sup>125</sup>Ibid

<sup>126</sup>Retrieved June 12, 2012 <<http://www.emergency.com/fbi-nccs.htm>>.

<sup>127</sup>Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson (2004 .8-10 November) CSI/FBI Computer Crime and Security Survey computer security institute publications, Retrieved June 6, 2012 from <[http://i.cmpnet.com/gocsi/db\\_area/pdfs/fbi/FBI2004.pdf](http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf)>

respondents answering that there was no unauthorized use of their organization's computer systems increased to 35 percent as the respondents not knowing if such unauthorized use occurred dropped to as low as 11 percent. The year 2004 showed the lowest percentage (12 percent) of respondents estimating that organization experienced more than ten computer security incidents during the past year. The survey provides a visual demonstration that attacks of computer systems or misuse of these systems has been slowly, but fairly steadily decreasing over many years in nearly all categories.

In fact, there has been a dramatic drop in reports of system penetrations, insider abuse and theft of proprietary information. Data from other countries reveal similar trends. According to a November 2000 report from the United Kingdom:<sup>128</sup> Cybercrime accounted for half of all fraud committed in the UK in the first six months of this year, according to a legal expert. Steven Philippsohn,<sup>129</sup> said this figure would rise as it becomes easier for criminals to break online security. Speaking at the computer security conference (Compsec) in London, he said:

The internet is a criminal's charter. There is an increasing number of targets and despite what people say, buying online is not the same as giving your credit card to someone in a restaurant. In that scenario, maybe 10 people will see your credit card details. The minute you put those details on to a website and that site is hacked, the information can be accessed by millions if not billions around the world.

Philippsohn said it is cheap for fraudsters to set up an online scam. They don't need premises, and they can set up a website claiming anything they like and give a very good impression of what can be an absolute scam. He said there has been a 56 per cent increase in hacking in the UK over the past 12 months, with most hackers seeking financial gain, for

---

<sup>128</sup> *Cybercrime Soars in the UK*. Retrieved June 12, 2012 from <<http://www.vnunet.com/news/1113497>>

<sup>129</sup> *Ibid.* (Philippsohn is the senior litigation partner at the law firm of Philippsohn, Crawfords, Berwald,)

example by using their hack to demand money, or for political reasons such as posting messages for a certain cause on a company's website'<sup>130</sup>.

In Japan and china, studies showed high increases in cybercrime.<sup>131</sup> From its part, the Australian version of the CSI/FBI survey 2004 found that: 'more respondents organizations experienced electronic attacks that harmed the confidentiality integrity or availability of network data or systems (49% in 2004 compared to 42% in 2003)'.<sup>132</sup> It also remarked that: 'Most of these attacks were again sourced externally (88%) compared to internally (only 36%), but fewer respondents experienced external attacks compared to 2003 (91%)'.<sup>133</sup> The survey showed that: 'Infections from viruses, worms or Trojans were the most common form of electronic attack reported by respondents for the third consecutive year. They were the greatest cause of financial losses and accounted for 45% of total losses for 2004.'<sup>134</sup>

In 1999, the Australian survey found that the attacks perpetuated appear to be random, 'spur of the moment' attacks, with no discernible pattern detected in more than 70% of the cases. According to respondents, the most likely motivation for an attack was curiosity (71%). The attacker was most likely to be a disgruntled employee or an independent hacker.<sup>135</sup> In fact, the value of these surveys is perhaps more anecdotal than scientific.<sup>136</sup> As almost everyone concedes, it is difficult to gather accurate cybercrime statistics.<sup>137</sup> On such a basis Parker states:

In reality, we have no valid statistics on cybercrime frequency or size of loss. Even if there were valid statistics on cybercrime, beyond helping with actuarial insurance rate structures and legislation, they would be of little use to a particular organization

---

<sup>130</sup>Ibid

<sup>131</sup>Kabay M [2001], *Studies and Surveys of Computer Crime*. Retrieved June 6, 2012 from <[http://www.securitystats.com/reports/Studies\\_and\\_Surveys\\_of\\_Computer\\_Crime.pdf#search='studies%20and%20surveys%20of%20computer%20crime'](http://www.securitystats.com/reports/Studies_and_Surveys_of_Computer_Crime.pdf#search='studies%20and%20surveys%20of%20computer%20crime')>

<sup>132</sup>Deloitte and Victoria Police Computer Crime Survey [2004], p. 3.(cited by Chawki M. op cit. at,15

<sup>133</sup>Ibid

<sup>134</sup>Goodman M and Brenner S. Op.cit .p.387 at,156.

<sup>135</sup> Ibid

<sup>136</sup>Ibid

<sup>137</sup>Ibid

for its own risk assessment. Each organization's circumstances differ significantly from the average incident represented in the statistics. Unfortunately, the limited surveys that are conducted on cybercrime are often conducted by individuals who are unfamiliar with cybercrime. Each survey respondent has a different definition of cybercrime and may be unaware of what actually happened, how it happened, or what the actual losses were. In addition, many victims do everything they can to avoid revealing their actual losses.<sup>138</sup>

Confirming this, Kabay states that's 'a commonly held view within the information security community is that only one-tenth or so of all the crimes committed against and using computer systems are detected'.<sup>139</sup> He also declares that:

Even if attacks are detected, it seems that few are reported in a way that allows systematic data collection. This belief is based in part on the un-quantified experience of information security professionals who have conducted interviews of their clients; it turns out that only about ten percent of the attacks against computer systems revealed in such interviews were ever reported to any kind of authority or to the public. The Department of Defence studies mentioned above were consistent with this belief; of the few penetrations detected, only a fraction of one percent were reported to appropriate authorities.<sup>140</sup>

Most experts believe that common forms of computer related crime are significantly underreported because 'victims may not realize that they have been victimized, may not realize that the conduct involved in a crime, or may decide not to complain for reasons of embarrassment or corporate credibility'.<sup>141</sup> Other reasons for the under reporting of cybercrime are that 'further problems arise with the mass victimization caused by offences such as virus propagation, because the number of victims are simply too large to identify and count, and

---

<sup>138</sup>Parker D.Op.cit, p.35, at, 74.

<sup>139</sup>Kabay M.Op.cit, p. 63

<sup>140</sup>Ibid

<sup>141</sup>*U.N (2001) Commission on Crime Prevention and Criminal Justice, 10 th session, Item 4 at 10, Conclusion of the Study on Effective Measures to Prevent and Control High-Technology and Computer Related Crime. Retrieved June 9, 2012.from <[http://www.unodc.org/pdf/crime/10\\_commission/4e.pdf](http://www.unodc.org/pdf/crime/10_commission/4e.pdf)>*

because such programs can continue creating new victims long after the offenders have been caught and punished'.<sup>142</sup>

Finally, a factor complicating the gathering and comparison of national crime statistics will be the fact that transnational computer related crimes are, by definition committed in or have effects in at least two States risking multiple reporting or no reporting at all.<sup>143</sup> "Thus, much of the information we have on cybercrimes is the product of studies and surveys addressed to individuals working in information security."<sup>144</sup> On such a basis the obvious problem that survey results include only the respondents of people who agreed to participate.<sup>145</sup> Before basing critical decisions on survey information, it is important to find out what the response rate was; although there are no absolutes. In general, people aim to trust survey results more when the response rate is high.<sup>146</sup>

However, response rates for telephone surveys are often less than 10%; response rates for mail and e-mail surveys can be less than 1%.<sup>147</sup> It is not easy to make any case for random sampling under such circumstances, and all results from such low response rate surveys should be viewed as indicating the range of problems or experiences of the respondents rather than as indicators of population statistics.<sup>148</sup> As to the problems noted above, a research firm estimated in 2001 that 'Cybercrime today is focused on corporate espionage and financial gain.

There are no guns or violence and the perpetrator is nowhere near the scene: in fact, most of the time they aren't even in the same country! Gartner Group already predicted that the

---

<sup>142</sup> Ibid

<sup>143</sup> Ibid

<sup>144</sup> Kaybay M. Op.cit, p.63

<sup>145</sup> Ibid

<sup>146</sup> Ibid

<sup>147</sup> Ibid

<sup>148</sup> Ibid

financial damage caused by cybercrime will increase by between 1000 and 10,000 per cent by 2004'.<sup>149</sup>

Also, at a Berlin conference of 100 Internet experts from the G8 group of industrialized nations in October 2000, J. Fischer German Foreign Minister declared that cybercrime losses have reached 100 billion German marks for the eight major countries including the U.S.<sup>150</sup> As to the effects of cybercrime, it is, at the very least, safe to agree with the position the European Commission took in launching a cybercrime initiative:<sup>151</sup>

While conceding that 'there is a little doubt that these offences constitute a threat to industry investment and assets, and to safety and confidence in the information society'.<sup>152</sup> The Commission states 'it is necessary that substantive law in the area of high tech crime is approximated'.<sup>153</sup> European leaders called during the special EU-summit in Tampere (1999) for common definitions, incriminations and sanctions in the area of high tech crime'.

---

<sup>149</sup>Miles A. (2001. April 20) Bug Watch: The Fight Against Cybercrime. Retrieved June 6, 2012 from <<http://www.pcw.co.uk/print/it/1120814>>

<sup>150</sup>F. Cilluffo [2001 May]. *Cyber Threats and Information Security* (CSIS), For full study.cited by Chawki, M. Op.cit. p.at,14

<sup>151</sup>Goodman M and Brenner S. Op.cit p.37, at,160.

<sup>152</sup>Burren J. (2001) *European Commission Wants to Tackle Cybercrime*. Retrieved June 19, 2012 from <<http://www.heise.de/tp/r4/artikel/4/4658/1.html>>

<sup>153</sup> Ibid

## 2.5 Meaning of Cyber Jurisdiction

Jurisdiction is the authority by which court take cognizance of and decide cases. The word ‘jurisdiction’ is of large and comprehensive import and embraces every kind of judicial action, jurisdiction is the authority of a court to hear a case and resolve a dispute involving persons, property and subject matter. These principles of jurisdiction are enshrined in the constitution of a country and part of its jurisdictional sovereignty.<sup>154</sup>

All sovereign independent countries possess jurisdiction over all persons and things within its territorial limits and all causes, civil and criminal, arisen within these limits<sup>155</sup>. One of the significant issues that must be addressed when assessing the legal means of combating information terrorism or cyber crime is the jurisdictional issue. Indeed two commentators on the field have stated, “of greatest significance [to the prevention of internet crime], however, is the credibility of law enforcement agencies’ capabilities to detect, investigate and prosecute”.<sup>156</sup>

The scope of this dissertation does not permit extensive analysis of all jurisdictional issues. Therefore, the discussion in this subhead shall be limited to the subject matter as it relate to cyber insecurity.

A number of important jurisdictional issues stem from the cross border nature of cybercrime. These include limited law enforcement capacity in the face of rapid globalization and technological change, tensions from the conflict between national sovereignties, and the importance of international cooperation.<sup>157</sup> The following is a list of key jurisdictional issues associated with the complexities of cyber-fraud: First, jurisdiction (whether jurisdiction exists

---

<sup>154</sup> -Apart from judicial activity, a state’s administrative, executive and legislative activity is also part of its jurisdictional sovereignty.

<sup>155</sup> Lord Macmillan in *Campania Naviera Vascongado v Steamship ‘Cristina’* (1938) AC 485

<sup>156</sup> Roger Clarke, Gillian Demsey & Robert F.O. Connor (1998. 16-17 Feb.) Technological Aspect of Internet Crime Prevention. A Paper Presented at the Australian Institute for criminology’s Conference on “Internet Crime”, Melbourne University. Retrieved June 20, 2012 from <http://www.anu.edu.au/people/Roger.Clark/II/CrimePrev.html>.

<sup>157</sup> Grabosky, P. (2006) Editor’s Postscript, *Crime, Law and Social Change*. Retrieved June 18, 2012 from <https://researchchrs.anu.edu.au/researchers>. Pp.275-276.

and the problem of concurrent jurisdiction); Second, legislative difficulties associated with differing criminal law regimes (the requirement of dual criminality), Third, managing strategic alliances and partnerships and ensuring the confidentiality and flexibility of responses (particularly in relation to the private sector);<sup>158</sup> Fourth, dealing with differing privacy regimes; Fifth, achieving mutual assistance and strategic intelligence in a timely manner; Sixth, the need to secure the cooperation and assistance of internet service providers (ISPs); Seventh, the need for the trans-national search of computer data banks and the interception of communications; and eighth, difficulties with managing and coordinating extraditions.<sup>159</sup>

The transnational nature of cybercrime challenges traditional conceptions of criminal jurisdiction because conduct no longer necessarily occurs entirely within the territory of a single sovereign.<sup>160</sup> For example, in 2000, the Love Bug virus, which was launched from the Philippines, infected computers in at least twenty countries<sup>161</sup>. The person who was alleged to have released the 'ILove You' virus was never prosecuted for that act because the mischief was not defined under Philippine law at the time that it occurred, although it was prohibited in a number of countries impacted by the virus<sup>162</sup>.

Since cybercrime can transcend national borders and given that the activities of an offender often result in the commission of a crime in multiple countries simultaneously, it is necessary to note that it is capable of escaping the substantive computer offences in national legislation and the procedural provisions relating to the investigation and prosecution of computer crimes. This defect could be cured if, the goal for the establishment of cooperative

---

<sup>158</sup>Subsequently, this model for the enactment of cybercrime legislation was adopted by a number of states and territories.

<sup>159</sup>Urbas G and Choo K. (2008). Resource Materials on Technology-Enabled Crime: Technical and Background Paper No.28. Canberra: Australian Institute of Criminology. p8

<sup>160</sup> Brenner, S. (2002)Organized Crime? How Cyberspace May Affect the Structure of Criminal Relationships. *North Carolina Journal of Law and Technology* 4(1):1-50.

<sup>161</sup> Ibid

<sup>162</sup>Grabosky, P.Op.cit p.10, at, 186

measures to facilitating the exchange of evidence, information and the extradition of suspects is achieved on international basis.<sup>163</sup>

It is encouraging that the global threat of cybercrime has triggered the response of international agencies and law enforcement agents around the globe. Indeed, there have been new coalitions formed by law enforcement, government agencies, non governmental organizations (NGOs,) and private sector actors, to address the transnational nature of cybercrime.

Nigeria is yet to be an active participant in a number of international organizations, such as the G8 Group of Senior Experts on Transnational Organized Crime, the Committee of Experts on Crime in Cyberspace of the Council of Europe, and the Organization of American States Group of Government Experts on Cybercrime. The Government of most of this participating countries hosts global summits, conducts international studies, and helped draft the Council of Europe's *Convention on Cybercrime*. For instance, the Canadian Association of Internet Providers is currently sharing information with European Internet Service Providers (ISPs) and working with other countries to develop international solutions.

Interpol, which is an international law-enforcement organization with 188 members, has been at the forefront of an organized international response to online fraud for many years.

The General Secretariat continues to offer specialized assistance to national law enforcement authorities in its member countries through a range of operational support, database services and police training. Interpol is also engaged in developing strategic partnerships with other international law enforcement organizations and public sector bodies. For example, the Interpol Counterfeit Payment Cards Database was specifically created to promote successful

---

<sup>163</sup>Schjolberg, S.(2008). The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva. p.1. Retrieved June 20, 2012 from [http://www.cybercrimelaw.net/documents/cybercrime\\_history.pdf](http://www.cybercrimelaw.net/documents/cybercrime_history.pdf).

collaboration on a global scale. Interpol regularly hosts meetings of its Advisory Group on Payment Card Fraud, which is comprised of senior investigators and forensic experts from many member countries, as well as major credit card companies such as Visa, American Express and MasterCard.

In recent years, there have been a number of milestones that address the challenges of combating transnational cybercrime. One of the most significant of these was the Council of Europe's *Convention on Cybercrime* whose efforts to harmonize substantive and procedural law serves as a model for nations around the world. This was the first multilateral treaty aimed at facilitating international cooperation in the prosecution of computer crimes. It was signed in Budapest on November 23, 2001, by member states of the Council of Europe and by several non member states, including Canada, Japan, South Africa and the US, that participated in its development<sup>164</sup>. The Convention entered into force on July 1, 2004.

As of March 16, 2011, there were 47 signatory states.<sup>165</sup> Of the 47 countries that signed the Convention, 30 countries have ratified it and entered it into force, including the United States of America. The Convention requires each signatory state to make it an offence to commit certain crimes using computer systems (including computer related fraud and forgery, offences related to child pornography and the infringement of copyright) and to grant new powers of search and seizure to its law enforcement officials, including the expedited preservation of stored computer data, search and seizure of stored computer data and the real time collection of computer data. Article 25 requires law enforcement officials in each signatory state to assist those in other participating states by cooperating with "mutual assistance requests" from police "to the widest extent possible."

---

<sup>164</sup> Huey L. and Rosenberg R.S. (2004). Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention. *Canadian Journal of Criminology and Criminal Justice* 46: 597-631.

<sup>165</sup> Council of Europe Treaty Office. Retrieved June 20, 2012 from <http://www.conventions.coe.int>.

Elsewhere in the world, regional organizations have begun to address the important unresolved issues relating to transnational cybercrime. Beginning in the late 1990s, the G8 subgroup on high-tech crime established a 24hour network of experts to assist in high-tech crime investigation to ensure that no criminal receives a safe haven anywhere in the world.<sup>166</sup>The G8 also negotiated principles and an action plan to combat high tech crime, as well as better practices documents, including guides for security of computer networks, international requests for assistance, legislative drafting, and tracing networked communications across borders.<sup>167</sup>In addition, the G8 has worked on training conferences for cybercrime agencies from every continent (except Antarctica) and conferences for law enforcement and industry on improved cooperation and tracing online criminal communications.

Similar steps have also been taken by the Organization for Economic Cooperation and Development (OECD). In 2002, the OECD published its *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, which were developed with the following aims: promote a culture of security among all participants as a means of protecting information systems and networks; raise awareness about the risk to information systems and networks, as well as the policies, practices, measures and the need for their adoption and implementation; foster greater confidence among all participants in information systems and networks and the way in which they are provided and used; and create a general frame of reference that will help participants understand security issues and procedures for the security of information systems and networks.<sup>168</sup>

The European Union (EU) adopted a Framework Decision and entered it into force in 2005, which provides that states will criminalize illegal system interference and illegal data

---

<sup>166</sup>Schjolberg S.Op.cit, p.69, at,13

<sup>167</sup>Urbas G. and Choo K.Op.cit. p,68 at,12

<sup>168</sup> Ibid at p.10

interference, and illegal access to information systems<sup>169</sup>. Similarly, the Asia Pacific Economic Cooperation (APEC) has committed to encouraging its member states to enact a comprehensive set of laws relating to cybercrime, as well as a policy framework that addresses substantive, procedural and mutual legal assistance measures, consistent with international legal instruments<sup>170</sup> APEC has conducted a capacity building project on cybercrime for its members in relation to legislation and investigative capabilities, whereby the advanced APEC economies support the less advanced in training law enforcement personnel.<sup>171</sup> Similar commitments were also made by the Association of Southeast Asian Nations (ASEAN) in 2006, and the League of Arab States, as well as some members of the African Union. As well, in 2008, North Atlantic Treaty Organization (NATO) opened a centre for excellence on cyber defense in Estonia, in order to conduct research on cyber warfare. The Organization of American States (OAS) has also taken steps to combat threats to cyber-security, including urging member states to adopt cybercrime laws and to facilitate international cooperation.

The connection between organized crime and cybercrime was one of the focuses of the 11th United Nation Crime Congress in 2005. The United Nations General Assembly has also adopted a number of resolutions on combating the misuse of information technologies. A UN Working Group on Internet Governance was established to contribute to the World Summit on the Information Society which was held in Tunisia in November 2005<sup>172</sup> a Global Cyber security Agenda was also launched in May 2007 by the Secretary General as a global framework for dialogue and international cooperation in the development of strategies and solutions to enhance information security. Additionally, the International Telecommunications Union (ITU) in

---

<sup>169</sup> Ibid at p.15

<sup>170</sup> Ibid at p.16

<sup>171</sup> Li, X. (2007). International Actions Against Cybercrime: Networking Legal Systems in the Networked Crime Scene. *Weblog*,4(3):1-45. cited by Smyth S and Carleton R.(2011. August) Measuring the Extent of Cyber-Fraud: A Discussion Paper on Potential Methods and Data Sources. Report NO.020,2011 at p.31

<sup>172</sup>Schjolberg.S. Op.cit, p.69, at, 10.

Geneva has become the most active United Nation organization aimed at reaching harmonization on global cybercrime legislation and it has been looking at how to promote international cooperation and build on existing international agreements in this area, particularly the Council of Europe's *Convention on Cybercrime*.<sup>173</sup>

## 2.6 Nature and Scope of Internet

There are many networks<sup>174</sup> that exist in the world, often with different hardware<sup>175</sup> and software.<sup>176</sup> People connected to one network often want to communicate with people attached to a different one. This desire require connecting together different, and frequently incompatible networks, to make the connection and provide the necessary translation, both in terms of hardware and software. A connection of interconnected networks is called an Internetwork or just Internet. An internetwork is formed when distinct networks are connected together. On October 24, 1995, the Federal Networking Council (FNC) of U.S.A. unanimously passed a resolution defining the term internet. This definition was developed in consultation with members of the internet and intellectual property rights communities. The following language reflects the definition of the term "Internet"<sup>177</sup>.

"Internet" refers to the global information system that: (i) is logically linked together by a globally unique address space based on the Internet protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communications using the transmission control protocol/Internet protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses or make accessible, either publicly or privately,

---

<sup>173</sup> Ibid at p.20

<sup>174</sup> Oxford Dictionary of Computing. Op.cit p. 10, (A Computer Network is a group of two or more computer systems linked together; it is used to connect two or more computers together with the ability to communicate with each other.)

<sup>175</sup> Oxford Dictionary of Computing. Op.cit. p.10 ,(Hardware is the physical aspect of computers, telecommunications and other devices. Hardware is a collective term, it include not only the computer proper but also the cables, connector, power supply units, and peripheral devices such as the keyboard, mouse, audio speakers, and printers.)

<sup>176</sup> Software is a general term used to describe a collection of computer programs, procedures and documentation that perform some task on a computer system. In simple terms, software is a computer instruction or data and include anything that can be stored electronically, Available at: <http://www.wordreference.com/definition/software>. Accessed, 20/6/12

<sup>177</sup> Adopted with the unanimous resolution by Federal Networking Council, on October 24, 1995. Retrieved June 20, 2012 from [http://www.livinginternet.com/How\\_The\\_Internet\\_Works.htm](http://www.livinginternet.com/How_The_Internet_Works.htm).

high level services layered on the communications and related infrastructure described herein.

The Internet is a network of networks, linking computers to computers sharing the TCP/IP protocol.<sup>178</sup> Each runs software to provide information and access to view information. The Internet is the transport vehicle for the information stored in files or documents on another computer. It can be compared to an international communications utility servicing computers. The Internet itself does not contain information. It is a slight misstatement to say a “document was found on the Internet.” It would be more correct to say it was found through or using the Internet.<sup>179</sup> The Internet is revolutionizing and enhancing the way we as humans communicate, both locally and around the globe. Simply put the Internet is a network of linked computers allowing participants to share information on those computers.<sup>180</sup>

Internet and on line services sometimes, called “new media” services is in many respect similar to the traditional media as it also includes production oriented material such as music, audio, video, graphics, text and games. It performs communication function also like, messaging, conferencing, research and the conduct of commerce. The Internet’s root can be traced to the 1950s with the launch of sputnik, the ensuing space race, the cold war and the development of ARPANet (Department of Defence Advance Research Projects Agency), but it really took off in 1980s when the National Science Foundation used ARPANet to link its five regional supercomputer<sup>181</sup> centers. From there evolved a high-speed backbone of Internet access for many other types of networks, universities, institutions, bulletin board systems and commercial online

---

<sup>178</sup> Transmission control protocol/Internet protocol, the suite of communication protocols used to connect host on the internet. TCP/IP uses several protocols, the two main ones being TCP and IP. It is the de facto standard for transmitting data over networks. Retrieved June 20, 2012 from <http://www.Searchnetworking.techtarget.com>TCP-IP>

<sup>179</sup> Chaubey R. (2009 ) An Introduction to Cyber Crime and Cyber Law. Kamal Law House Kolkata Indian. p.56

<sup>180</sup> Douglas E, Ralph E. Computer Network and Internets, Fourth Edition prentice Hall. U.K ( cited by Chaubay. R. Ibid)

<sup>181</sup>Chaubay, R. Op.cit .P.74, at p. 56. (Super computers are the fastest type of computer. They are very expensive and are employed for specialized applications that require immense amount of mathematical calculation. For example, weather forecasting requires a supercomputer. Other uses of supercomputers include animated graphics, fluid dynamic calculations, nuclear energy research, and petroleum exploration.)

services. The end of the decade saw the emergence of the World Wide Web, (www) which heralded a platform independent means of communication enhanced with a pleasant and relatively easy to use graphical interface.<sup>182</sup>

The Internet is on like any previous human invention in both scale and effect, and is now a global resource important to all of the people in the world. This unprecedentedly rapid growth and impact is largely due to its incorporation of a number of deeply powerful features that continue to accelerate its success, some of these key features of Internet which propels its concept are described below;<sup>183</sup>

**a. Geographic Distribution**

A key attribute of the Internet is that once you have connected to any part of it, you can communicate with all of it. All of the Internet's technologies- web, newsgroup, email, mailinglist, IRC.<sup>184</sup>MUD's<sup>185</sup> enables geographically distributed groups of people to communicate who otherwise couldn't do so. Largely because the basic architecture of internet is open and in concept, it is fundamentally designed to connect new networks, this powerful communication medium has spread rapidly to interconnect the world and turned it into a true multi way electronic global village.<sup>186</sup>

**b. Strong Architecture**

The Internet is the most robust communication system ever designed, able to adapt itself almost instantaneously to damage or outages to individual sections. The Internet has no irreplaceable central control, administration, or authority. It can't be bought, hijacked, or

---

<sup>182</sup> Tyrone A, Sharon S. (2005) Internet Effectively: A Beginner's Guide to the World Wide Web. Addison Wesley.U.K

<sup>183</sup> Retrieved June 22, 2012 from [http://www.livinginternet.com/tindex\\_p.htm](http://www.livinginternet.com/tindex_p.htm).

<sup>184</sup>Chaubay, R.Op.cit, p.74, at p. 62 (Internet Relay Chat (IRC) is a form of real-time Internet chat. It is mainly designed for group communication in discussion forums, but also allows one-to-one communication and data transfers via private message.)

<sup>185</sup> Ibid (A MUD (Multiple User Dimension, Multiple User Dungeon, or Multiple Users Dialogue) is a computer program which users can log into and explore. Each user takes control of a computerized character. He can walk around, chat with other characters, solve puzzles, and eves create his very own rooms, description and items.

<sup>186</sup> Retrieved June 22, 2013.from [http://www.linginternet.com/ip\\_geo.htm](http://www.linginternet.com/ip_geo.htm).

monopolized. The loss of individual computers and networks does not affect its overall reliability. The Internet perfectly realizes its original intent, it is actively robust, and cannot be completely deactivated without bringing down every single connection. The Internet is robust over time, too. Many people alive today were born before the internet was invented. If the birth of its concept is to be marked from 1969, one can safely assume that it is now effectively immortal, and will continue to exist in some form for the rest of human history.

### **c. High Speed**

The Internet operates at near light speed, which on a planet the size of earth often practically amounts to near real-time. Digital information such as Internet packets travel at 2/3 of the speed of light on copper wire and on fiber optic cables. Since light speed is about 300,000 kilometers a second, this means digital communications travel at about 200,000 kilometers a second, slowing down only because copper and fiber optic materials are about one-third thicker than a vacuum.<sup>187</sup> At this speed and neglecting switching delays, two computers have to be more than ten thousand kilometers apart, or almost half way around the world, before they experience a tenth of a second in communication delay. Internet routers are getting faster and faster with switching speeds nearing instantaneous, while fiber optics<sup>188</sup> and wireless technologies<sup>189</sup> are enabling networks to send much larger numbers of bits at once. The Internet is getting even faster.<sup>190</sup>

### **d. Accessibility**

---

<sup>187</sup>Chaubey, R. Op.cit, p.74, at, 63

<sup>188</sup>Oxford Dictionary of Computing,Op.cit .p.10, (Fiber Optics is technology that uses glass (or plastic) threads (fibers) to transmit data. A fiber optic cable consist of a bundle of glass threads, each of which is capable of transmitting messages modulated onto light waves.)

<sup>189</sup> The term wireless is normally used to refer to any type of electrical or electronic operation which is accomplished without the use of a “hard wired” connection. Wireless communication is the transfer of information over a distance without the use of electrical conductors or “wires”. Retrieved, June 22, 2012. From [http://www.sintef.no/content/page\\_11881.aspx](http://www.sintef.no/content/page_11881.aspx).

<sup>190</sup> Retrieved June 22, 2012 from [http://www.livinginternet.com/i/ip\\_speed.htm](http://www.livinginternet.com/i/ip_speed.htm).

The Internet provides universal access, giving the same powerful capability to everyone who has access to the network no matter where they are. The internet is based on a common standard, the **TCP/IP** network protocol, which provides all computers with access to the network with the same technical interface and capabilities. This common foundation makes the entire internet technologies equally available to anyone connected to the Internet. You should feel free to approach the Internet with the spirit of exploration, and don't need to have a task or a question to answer, you can surf from link to link or try random searches just to see what turns up like exploring a new city. If you feel moved to set up a web site about your favourite hobby, you can go ahead. The Internet is universally empowering to the extent that everyone can participate.<sup>191</sup>

**e. Growth**

The growth rate of the Internet exceeds that of any previous technology. Measured by users and band-width, Internet has been growing at a rapid rate since its conception, on a curve geometric and sometime exponential. Today, the Internet is growing exponentially in three different directions size, processing power, and software sophistication, making it fastest growing technology humankind has ever developed.<sup>192</sup>

**f. Technical Advantage**

Digital communications has the D4 advantage "Digital data doesn't degrade". Analog systems and digital systems are like mirror images of each other. Analog systems are usually controlled by physical mechanisms that can be in an infinite number of continuous positions. In contrast to approximate, analog systems, the Internet is a digital medium based on data made up of discrete 1's and 0's. a bit of computer data is not infinitely adjustable, and only has one or two

---

<sup>191</sup> Retrieved June 22, 2012 from [http://www.livinginternet.com/i/ip\\_access.htm](http://www.livinginternet.com/i/ip_access.htm).

<sup>192</sup> Retrieved June 22, 2012 from [http://www.livinginternet.com/i/ip\\_growth.htm](http://www.livinginternet.com/i/ip_growth.htm).

unambiguous states, it is either ‘a 1’, or ‘a 0’. This limitation has a very important compensating advantage; there is no “drift” that can introduce error. The Internet, like all computer systems, is based on digital data,<sup>193</sup> so that information never changes or become distorted over time or in transmission between sites. This is the key feature that makes it possible to construct the very complex software systems that run the Internet, so that a web site doesn’t age and become fuzzy or garbled over time, and the character in an e-mail don’t get transposed or mixed up when they are sent over long distances. One of the most important strengths of the Internet is that it’s based on one of the simplest concept which is digital 1’s and 0’s.<sup>194</sup>

#### **g. Freedom of Speech**

The Internet is a common area, a public space like any village square, except that it is the largest common area that has ever existed. Anything that anybody wishes to say can be heard by anyone else with access to the Internet and this world-wide community is as large and diverse as humanity itself. Therefore, from a practical point of view, no one community’s standards can govern the type of speech permissible on the internet. Information wants to be free, and the Internet fosters freedom of speech on a global scale. If is believed that there is an inherent value in truth, that human being on average and overtime recognized and value truth, and that truth is best decided in a free market place of ideas, then the ability of the Internet to promote freedom of speech is very important indeed.<sup>195</sup>

### **2.7 Concept of Protection**

At this point, one may conclude that cyber protection and cybercrime control are different but inter-related and intersecting concepts (at least in the way they are understood and applied so

---

<sup>193</sup> Digital data are the data transmitted or stored with digital technology, it is expressed as a string of zeroes and ones. Each of these state digits is referred to as a bit. A string of bits that a computer can address individually as a group is a byte. Retrieved June, 22, 2012 from <http://www.itrainonline.org/itranonline/english/glossery.shtml>.

<sup>194</sup> Retrieved June 22, 2012 from [http://www.livinginternet.com/i/ip\\_digital.htm](http://www.livinginternet.com/i/ip_digital.htm).

<sup>195</sup> Retrieved June 22, 2012 from [http://www.livinginternet.com/i/ip\\_speech.htm](http://www.livinginternet.com/i/ip_speech.htm).

far). Cyber protection and cybercrime control measures complement each other. The primary interest of the concept of cyber protection is to ensure the confidentiality, integrity and availability (“c-i-a”) of Information Communication Technology (ICT) (in particular critical information infrastructure) and the services built on it. They are covering non-intentional ICT security incidents and, more importantly, intentional attacks by state and non-state actor, including criminals and terrorists. In terms of measures, the focus is on technical, administrative and procedural measures to protect systems, in particular critical information infrastructure, to increase their resilience, to prevent, detect and manage incidents, to ensure coordinated responses to incidents and recovery, as well as building confidence and trust in ICT and the digital economy, and finally on national security and defence. Given the reliance of societies on ICT, concept of cyber protection are contributing to larger political, security, economic and social interests of countries. Cyber protection concept is thus interdisciplinary and comprises multiple stakeholders.<sup>196</sup>

The primary interest of cybercrime strategies is crime prevention and criminal justice that is to ensure that the rule of law applies also in the ICT and borderless online environment. Like concepts of cyber protection, they cover attacks against the confidentiality, integrity and availability against ICT by state and non-state actors. However, cybercrime strategies –while also covering preventive and not excluding technical measures – would focus primarily on the investigation, prosecution and adjudication of offenders. This means that cybercrime strategies and measures put emphasis on rule of law and human rights principles, including safeguards and conditions regarding investigative and other procedural measures. It is indicative that public authorities responsible for the rule of law (ministries of justice and interior, prosecution services,

---

<sup>196</sup>Markko Künnapu. (2011. October 14)Cited in global project on cybercrime, version, Strasbourg, France.p.17. Retrieved, June 22, 2012 from [www.coe.int/cybercrime](http://www.coe.int/cybercrime).

law enforcement agencies) have primary responsibilities for cybercrime matters but play only a secondary role in the concept of cyber protection.

Concept of protection goes beyond attacks against ICT and addresses offences also by means of ICT. This is particularly true for offences that have acquired a new scope and quality in cyberspace such as the sexual exploitation of children, fraud, the terrorist use of the Internet, infringements of intellectual property rights and other offences. Offences by means of ICT would normally not be covered by concept of protection.

Moreover, cybercrime strategies may need to address the fact that any offence may involve electronic evidence which entails a large scale effort to enhance criminal justice capabilities.<sup>197</sup>

Nevertheless, cyber protection and cybercrime strategies complement and reinforce each other cross-wise and at different levels. The complementarities is obvious with respect to the response to “c-i-a” attacks: While concept of protection covers a wide range of technical and procedural measures to respond to intentional attacks against ICT and to ensure the confidentiality, integrity and availability of ICT (ranging from prevention to protection and recovery), cybercrime strategies focus on the criminal justice response to “c-i-a” attacks.

Or to develop Vinton Cerf’s metaphor further, if the concept of protection is about “fire brigades” (‘when a house is on fire, the priority is to put down the fire to mitigate the damage, to repair the house and make it functioning again. Cyber protection is about efficient fire brigades’)<sup>198</sup>, then a cybercrime strategy is about criminal justice: if somebody puts one house after the other on fire it is necessary and effective to investigate and prosecute the offender and put him or her behind bars to prevent further damage.

---

<sup>197</sup> Ibid, (In this sense, cybercrime strategies would need address a challenge that is not even considered cybercrime.)

<sup>198</sup> During a workshop at the (2010) Internet Governance Forum in Vilnius, Lithuania, on international cooperation on cybersecurity. (see for the background paper) Retrieved June 22, 2012 from. [http://www.afiliias.info/webfm\\_send/](http://www.afiliias.info/webfm_send/)

However, this complementary goes further than that. It is also obvious with regard to higher level objectives of cybercrime and concept of protection. For example, increased reliability, resilience, security and trust in ICT contribute to crime prevention and criminal justice and vice versa, but these also contribute to the rule of law and human rights (including privacy and the freedom of expression). Or increased protection contributes to crime prevention and criminal justice and vice versa. And the rule of law and human rights serve (or should serve) national interests and security.

## **2.8 Nature and Scope of Cyber Law**

Cyber specific laws fall into three categories; First, enabling, second, prohibition and third, investigation.<sup>199</sup>

Enabling typically gives legal effect to electronic documents and storage. For example, digital signatures can legally work as real signatures only when legislation provides such judicial capability. Evidence for tax or other purposes can be effective when a specific law defines electronic exchange and storage to be sufficient as evidence. The Digital Signature Act 1997 of Malaysia is a typical example.<sup>200</sup>

Prohibition typically prohibits and punishes computer related crimes. In several countries, electronic data destruction cannot be criminalized under the general law, because it does not destroy any physical matter. Similarly, intrusion itself does not constitute a crime as it does no physical harm. Thus, a specific law is required. The Unauthorized Access Prohibition Law of Japan is a typical example of this type of law. The Computer Crimes Act 1997 of Malaysia is another example. These are the most typical law enforcement against threats.<sup>201</sup>

---

<sup>199</sup>Buheita Fujiwara (2006. November 9)Cyber Security Threats and Countermeasures. A paper presented as Chairman, Information-technology Promotion Agency (IPA), Japan in a seminar organized by Global Business Dialogue on Electronic Commerce GBDe 2006 Issue Group. Pp.34-38

<sup>200</sup> Ibid

<sup>201</sup> Ibid

For investigation purposes Internet services providers are typically required to reserve communication logs for a certain period of time and submit such records to national investigative agencies. As communication services providers are prohibited from divulging communications secrets, specific legislation is required to give exemption. Eavesdropping and network monitoring for specific communication also should be allowed under a jury court's order judged in line with a law allowing special investigation. The Communications Protection and Surveillance Act of Taiwan is a typical example of this type of legislation. These types of laws are prepared to indirectly fight against threats.<sup>202</sup>

In the last 20 years, various countries and regional organizations have developed legislation and legal frameworks to address cybercrime. Despite certain common trends that have developed, the differences in national legislation remain significant. One reason for both national and regional differences in legislative frameworks is that the impact of cybercrime is not universally the same, as the fight against spam demonstrates.<sup>203</sup> Spam has emerged as a much more serious issue in developing countries than in Western countries as a result of the scarcity and expense of resources.<sup>204</sup> In terms of illegal content, some countries and regions may criminalize the dissemination of material that may be considered to be protected by the principle of freedom of speech<sup>205</sup> in other countries or regions.<sup>206</sup>

---

<sup>202</sup> Ibid

<sup>203</sup> International Telecommunication Union (2009) Understanding Cybercrime: A Guide for Developing Countries chapters 2,6& 7.

<sup>204</sup> See, Spam Issue in Developing Countries. Retrieved June 12, 2012 from [www.oecd.org/dataoecd/5/47/34935342.pdf](http://www.oecd.org/dataoecd/5/47/34935342.pdf).

<sup>205</sup> Woo/So, (2002)The case for Magic Lantern: September 11 highlights the need for increasing surveillance, Harvard Journal of Law and Technology. 15 ( 2):530, Volokh (2001) Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law. Loyola University Chicago Law Journal, 33:57. Retrived June 12, 2013 from [www.law.ucla.edu/volokh/harass/religion.pdf](http://www.law.ucla.edu/volokh/harass/religion.pdf); Cohen (2007) Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, Retrieved June 12, 2013 from [www.fas.org/sgp/crs/misc/95-815.pdf](http://www.fas.org/sgp/crs/misc/95-815.pdf).

<sup>206</sup> See, Explanatory Report to the First Additional Protocol, No. 4.Concerns over freedom of expression explain why certain acts of racism were not made illegal by the Convention on Cybercrime, but their criminalization was included in the First Additional Protocol.

## CHAPTER THREE

### THE DEVELOPMENT OF LEGAL AND INSTITUTIONAL REGIMES IN COMBATING CYBER CRIME AND CYBER INSECURITY

#### 3.1 Introduction

With a new decade beginning, the continent of Africa which was regarded as “backwards” has been able to get a leap into the world of Information Communication Technology (ICT). This leap has not come without a heavy price. The rapid rate of diffusion of cybercrime in Africa has been a call for concern. This concern even gets more sickening when literature indicate that, out of the top ten countries in the world with a high level of cybercrime prevalence, Sub Sahara Africa (SSA) is host to four of this countries, (Nigeria, Cameroon, Ghana and South Africa).<sup>1</sup>

This rate of cybercrime prevalence has triggered a renaissance in the fight against cybercrime in SSA. This fight involves not only law enforcement agencies, but all stakeholders. Stakeholders in the fight against cybercrime in Sub Sahara African countries range from the average man on the street that knows and fraternizes with cyber criminals to the president of the various countries who enact decrees and sign laws passed by the legislature. This fact highlights the wide scope of whom and what is involved in combating this malaise.<sup>2</sup> For the purpose of this study, this chapter will limit the discussion to the various organized structures and institutions that are at the fore front of combating cybercrime at the International, Regional and National levels while the strengths and weakness of the recent Nigeria cybercrime prohibition, prevention etc Act, 2015 will be reviewed.

---

<sup>1</sup> Akuta E, Ong’oa I, Chanika J. (2011, May) Combating Cybercrime in Sub-Sahara Africa: A Discuss on Law, Policy and Practice. *Journal of Research In Peace, Gender and Development*. 1(4):129-137

<sup>2</sup> Ibid

### 3.2 Role of Law in Combating Cybercrime

The definition of law is a persistent question in Jurisprudence and has always been a subject of much controversy among jurists. But law, however defined exists always to ensure legal order and the due administration of justice in an organized society. This is the general purpose of law. It is within this context that it has been said that “whatever else law may do or be, it contains the rules for the employment of the state machinery”<sup>3</sup>.

The Nigerian legal system follows the English Common Law System whose conception of man is that of a reasonable being, with the rights and duties of such a being. Law from this point of view has been taken as a system of rules which we are all presumed to know and against which we act at our own peril. Such rules of conduct must be authoritatively prescribed or knowable in a given society, whether or not the society is determined territorially. The object of such rules is to enable the settlement of disputes regarding the claims of individuals or groups to be made in accordance with reason and bearing in mind every man’s prima facie right to survive. It means that such rules must, at all times, be sufficiently clear and coherent so as to enable a person to predict with certainty the legal consequences of his acts.<sup>4</sup>

The 2001 Council of Europe Convention on Cybercrime is a historic milestone in the combat against cyber crime, and entered into force on July 1, 2004. The total number of signatures not followed by ratifications are 17, and 30 States have ratified the Convention.<sup>5</sup>In Europe, Turkey has signed on November 10, 2010, but Russia has not signed the Convention.<sup>6</sup>

By ratifying or acceding to the Convention, the States agree to ensure that their domestic laws criminalize the conducts described in the substantive criminal law section. Other States

---

<sup>3</sup> Ladan M.T (2008) Introduction to Jurisprudence: Classical and Islamic. Faith Printers and Publishers Ltd. Zaria. p.37

<sup>4</sup> Ibid

<sup>5</sup> Alexander S. (2010) The Budapest Convention on Cybercrime as a Global Framework: Introduction to Panel Discussions. A paper presented at the Conference Organized by Council of Europe. Held in Strasbourg France from 23-25 march. 2010.

<sup>6</sup> Stein Schjolberg and Solange Ghernaouti-Helie, (2011) A Global Treaty on Cyber security and Cybercrime, Second edition p.163. Retrieved February 16, 2014 from [www.cybercrimelaw.net](http://www.cybercrimelaw.net).

should evaluate the advisability of implementing the standards and principles of the Convention and use the Convention as a guideline, or as a reference for developing their internal legislation.<sup>7</sup>

Considering the Council of Europe's Convention on Cybercrime as an example of legal measures realized as a regional initiative, countries should complete its ratification, or consider the possibility of acceding to the Convention of Cybercrime. Other countries should, or may want to, use the Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal system and practice. It is very important to implement at least Articles 2-9 in the substantive criminal law section of the Council of Europe's Convention on Cyber crime.

But the Convention is based on criminal cyber conducts in the late 1990s. New methods of conducts in cyberspace with criminal intent must be covered by criminal law, such as phishing, botnets, spam, identity theft, crime in virtual worlds, terrorist use of Internet, and massive and coordinated cyber attacks against information infrastructures. Many countries have adopted or preparing for new laws covering some of those conducts. In addition, the terminology included in the Convention is a 1990s terminology, and is not necessarily suitable for the 2010s.<sup>8</sup>

Provisions on attempt, aiding or abetting should be enacted and implemented in accordance with the individual countries own legal system and practice and need not necessarily be included in a convention. Similar approach should be taken with regard to corporate liability, and punishable sanctions and measures for criminal offences.<sup>9</sup>

In order to establish criminal offences for the protection of information and communication in Cyberspace, provisions must be enacted with as much clarity and specificity as possible, and not rely on vague interpretations in the existing laws. When cybercrime laws are

---

<sup>7</sup> Ibid at p.41

<sup>8</sup> Ibid, at p.1

<sup>9</sup> Ibid

adopted, perpetrators will be convicted for their explicit acts and not by existing provisions stretched in the interpretations, or by provisions enacted for other purposes covering only incidental or peripheral acts.<sup>10</sup>

One of the most important purposes in criminal legislation is the prevention of criminal offenses. A potential perpetrator must also in cyberspace have a clear warning with adequate foresee-ability that certain offences are not tolerated. And when criminal offences occur, perpetrators must be convicted for the crime explicitly done, satisfactorily efficient in order to deter him or her, and others from such crime. These basic principles are also valid for cybercrimes.

### **3.3 Development of Legal and Institutional Regimes at Global Level**

The rapid growth of the Internet has dramatically changed the way entities interact. Cyberspace enables people to share ideas over great distances and engage in the creation of an entirely new, diverse and chaotic democracy, free from geographic and physical constraints.<sup>11</sup>The rapid progress of information technology has achieved significant advances in processing and transmitting data through use of computers and computer networks resulting in substantial benefits to society, including the ability to communicate with others real-time, access a library of information and transmit data instantly<sup>12</sup>.

The dark side of the above phenomenon is the fostering of new kinds of crimes, additional means to commit existing crimes and increased complexities of prosecuting crimes, since historical obstacles to international crime, such as distance, time and space, have now been eliminated. This international element in the commission of crime, whether it be traditional or

---

<sup>10</sup> Ibid

<sup>11</sup> Aldesco I.A. , (2002), The demise of anonymity: A constitutional challenge to the convention on cybercrime, Loyola of Los Angeles Entertainment Law Review. p.81

<sup>12</sup> Hopkins L.S. (2003), Cybercrime Convention: A positive beginning to a long road ahead, Journal of High Technology Law, p.101

new technological computer crime, creates new problems for both legal policy and law enforcement.

The above described challenge resulted in the Budapest's Convention, which with respect to human rights, aims at the adoption of appropriate and adequate international legal measures by the contracting countries.

The Convention on cybercrime provides a treaty-based framework that imposes on the participating nations the obligation to enact legislation criminalizing certain conduct related to computer systems, create investigative procedures and ensure their availability to domestic law enforcement authorities to investigate cybercrime offenses, including procedures to obtain electronic evidence in all of its forms and create a regime of broad international cooperation, including assistance in extradition of fugitives sought for crimes identified under the Convention.<sup>13</sup>

A treaty, according to Article 2 of Vienna Convention, is “an international agreement concluded between States in written form and governed by international law, whether embodied in a single instrument or in two or more related instruments and whatever its particular designation”<sup>14</sup>. Treaties are the only machinery that exist for adapting international law to new conditions and strengthening the force of a rule of law between states<sup>15</sup>. Thus, and taking into account the Council's of Europe declaration of the need to pursue a common criminal policy aimed at the protection of the society against cybercrime<sup>16</sup> it seemed very important for an

---

<sup>13</sup> Marshall J.J. (2005)The Convention on cybercrime: A harmonized implementation of international penal law: what prospects for procedural law process?, Computer & Information Law Journal,p.329

<sup>14</sup> Council of Europe, Treaty Office, online at <http://conventions.coe.int/Treaty/EN/v3Glossary.asp>/accessed 16/02/14

<sup>15</sup> Brierly J.L. (1978, Jan. 5 ) The law of Nations: An introduction to the international law of peace, Humphrey Waldock (ed).Oxford Univ. Press 6th ed, ,p.275

<sup>16</sup> Convention on Cybercrime, Preamble Retrieved February 16, 2014 from <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm/>

international regime to be set up to combat these types of crimes in a growing and integrated global society.

Before the Budapest's Convention adoption, a number of Committee of Ministers Recommendations, had been issued in an attempt to combat cybercrime. These Recommendations, also mentioned in the Convention's Preamble, are Committee of Ministers Recommendations No. R (85) 10, concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2, on piracy in the field of copyright and neighbouring rights, No. R (87) 15, regulating the use of personal data in the police sector, No. R (95) 4, on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9, on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13, concerning problems of criminal procedural law connected with information technology.

The Council of Europe's Convention on Cybercrime and its Explanatory Report have been adopted by the Committee of Ministers of the Council of Europe at its 109th Session on November 8, 2001 and the Convention was opened for signature on November 23, 2001.

Negotiations on the Convention began in 1997, following a determination by the Council that the transnational character of cybercrime could only be tackled at the global level. To date, the Convention has been signed by 43 Council of Europe members and four non-members i.e. Canada, Japan, South Africa and the United States<sup>17</sup> that also participated in the negotiations. It

---

<sup>17</sup> Council of Europe, Chart of signatures and ratifications, ETS no 185. Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other none member States. Retrieved February 16, 2014 from <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG/>

has also been supplemented by an Additional Protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence.

Greece signed the Convention on 23.11.2001, but has yet to ratify it. Although, some provisions of the Convention are already covered by existing Greek domestic legislation, there still is a long way ahead. The distance will be covered with the Convention's critical and careful incorporation into the Greek legal order.

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

As recognized in the Convention's Preamble, the profound changes brought about by the digitalization, convergence and continuing globalization of computer networks and the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks, require co-operation between States and private industry in combating cybercrime and increased, rapid and well-functioning international co-operation in criminal matters. Moreover, the Council of Europe is mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties and also mindful of the right to the protection of personal data. The Convention, as it is declared in its explanatory report, aims principally at (1) harmonising the domestic criminal substantive law elements of offences and connected

provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form. (3) Setting up a fast and effective regime of international co-operation<sup>18</sup>.

Thus, the Convention's main goal is to establish a "common criminal policy" to better combat computer-related crimes worldwide through harmonizing national legislation, enhancing law enforcement and judicial capabilities, and improving international cooperation. To these ends, the Convention is broken up into four main chapters: The first chapter defining the terms to be used, the second chapter referring to the measures to be taken at the national level, containing substantive law, procedural law and jurisdiction measures, the third chapter referring to the international cooperation and the fourth chapter, regarding the final provisions of the Convention.

Article 1 initially defines four terms vital to the treaty. The first term defined is "computer system", which is a device consisting of hardware and software developed for automatic processing of digital data<sup>19</sup> For the purposes of this Convention, the definition of "computer data" builds upon the ISO-definition of data and must be in a form suitable for processing in a computer system<sup>20</sup>. According to ISO, "ISO" is not an abbreviation. it is a word derived from the Greek isos, meaning "equal", which is the root for the prefix "iso-" that occurs in a host of terms, such as "isometric" (of equal measure or dimensions) and "isonomy" (equality of law or of people before the law).The name ISO is used around the world to denote the organization, thus avoiding the assortment of abbreviations that would result from the translation

---

<sup>18</sup> Convention on Cybercrime, Explanatory Report, paragraph 16. Retrieved February 16, 2014 from <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm/>.

<sup>19</sup> Ibid, page 9, explanatory report. paragraph, 23

<sup>20</sup> Ibid, explanatory report. Paragraph, 25

of “International Organization for Standardization” into the different national languages of members. Whatever the country, the short form of the organization’s name is ISO.

The term "service provider" encompasses a broad category of persons that play a particular role with regard to communication or processing of data on computer systems. This definition includes both public or private entities and “those entities that store or otherwise process data on behalf of public or private entities”<sup>21</sup>The fourth defined term is “traffic data” which means data that is generated by computers in the chain of communication in order to route a communication from its origin to its destination. It is therefore auxiliary to the communication itself. When a Convention Party investigates a criminal offence within this treaty, traffic data is used to trace the source of the communication. Traffic data lasts for only a short period of time and the Convention makes Internet Service Providers (ISPs) responsible for preservation of this data<sup>22</sup>.

It is noted that Convention Parties would not be obliged to copy *verbatim* into their domestic laws the four concepts defined in Article 1, provided that these laws cover such concepts in a manner consistent with the principles of the Convention and offer an equivalent framework for its implementation<sup>23</sup>.

Although there is an internationally continuing discussion “on just what constitutes a computer crime”, there is yet no generally accepted definition of the term. The Convention on cybercrime supports this effort to define computer crime by including an array of different computer related offences in its substantive criminal law provisions<sup>24</sup>.

---

<sup>21</sup> Ibid, explanatory report, paragraph.26,27.

<sup>22</sup> Ibid, explanatory report, paragraph.28-31

<sup>23</sup> Ibid, explanatory report, paragraph.22

<sup>24</sup> Viano C.E. (2004) Computer crimes and criminal law: international dilemmas and approaches, A paper presented at a Conference organized by Round Table II of the 17th International Congress of Penal Law. Held at Ant.N.Sakkoulas, on Monday, 4, October, (2004), pp. 51-52 & 67.

The purpose of Section 1, Articles 2-13 of the Convention is to establish a common minimum standard of relevant offences so as to improve the means to prevent and suppress computer- or computer-related crime.

Correspondence in domestic law may prevent abuses from being shifted to a Party with a previous lower standard. As a consequence, the exchange of useful common experiences in the practical handling of cases may be enhanced, too<sup>25</sup>.

As stated in the Explanatory Report, All the offences contained in the Convention must be committed "intentionally" for criminal liability to apply. In certain cases an additional specific intentional element forms part of the offence. The drafters of the Convention agreed that the exact meaning of "intentionally" should be left to national interpretation<sup>26</sup>.

The criminal offences in Articles 2-6 were intended by the drafters to protect the confidentiality, integrity and availability of computer systems or data and not to criminalise legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices<sup>27</sup>.

"Illegal access" covers the basic offence of dangerous threats to and attacks against the security, meaning the confidentiality, integrity and availability of computer systems and data. Examples of unauthorised acts of intrusion, which should be in principle illegal are "hacking", "cracking" or "computer trespass". Such intrusions may give access to confidential data, like passwords, information about the targeted system and secrets, to the use of the system without payment or even encourage hackers to commit more dangerous forms of computer-related offences, like computer-related fraud or forgery.

---

<sup>25</sup>Convention on Cybercrime, Explanatory Report, Explanatory report, Opcit.91,paragraph.33

<sup>26</sup> Ibid, Paragraph. 39.

<sup>27</sup> Ibid, paragraph. 43

The act must also be committed “without right”, meaning that there is no criminalization of the access authorized by the owner or other right holder of the system or part of it, such as for the purpose of authorized testing or protection of the computer system concerned <sup>28</sup>.

This provision of illegal interception aims to protect the right of privacy of data communication. The offence which is criminalized is the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons. The provision is based upon the right to privacy of correspondence of the Article 8 of the European Convention on Human Rights and the offence of “unauthorised interception” described in Recommendation (89) 9. The offence established at this point applies this principle to all forms of electronic data transfer, whether by telephone, fax, e-mail or file transfer and applies to “non-public” transmissions of computer data. The term “non-public” qualifies the nature of the transmission process and not the nature of the data transmitted, meaning that the data communicated may be publicly available information, but the parties wish to communicate confidentially or data may be kept secret for commercial purposes until the service is paid, as in Pay-TV. For criminal liability to attach, the illegal interception must be committed “intentionally”, and “without right”<sup>29</sup>.

The acts of damaging, deletion, deterioration, alteration or suppression of computer data is, under this provision, punishable, if committed without right in a way that computer data and computer programs are protected the same way to that enjoyed by corporeal objects against intentional infliction or damage. The offender, here, must have acted “intentionally”, too<sup>30</sup>.

The criminalization of the intentional hindering of the lawful use of computer systems including telecommunications facilities by using or influencing computer data is based upon the

---

<sup>28</sup>Ibid, paragraph. 44,47

<sup>29</sup> Ibid, paragraph. 51,52,54,58

<sup>30</sup> Ibid, paragraph. 60,63

“computer sabotage” of the Recommendation No. (89)9. The “hindering” must be “without right” and “serious” and the offence must be committed “intentionally” in order to give rise to criminal sanction<sup>31</sup>.

The article as it relate to misuse of devices establishes it as separate and independent offences, the intentional commission of illegal acts regarding certain devices that are used in the commission of the named offences of this Convention. The article intends to combat black markets which are established to facilitate the sale or trade of “hacker tools,” or tools used by hackers in the commission of cybercrimes by prohibiting the production, sale, or distribution of these devices. The drafters intended this Article to relate to devices that “are objectively designed, or adapted, primarily for the purpose of committing an offence”. Finally, in order to avoid over-criminalization, Article 6 requires both a general intent and also a “specific... intent that the device is used for the purpose of committing any of the offences established in Articles 2-5 of the Convention”<sup>32</sup>.

The purpose of Article 7, which outlaws computer-related forgery, is to create a parallel offence to the forgery of tangible documents. It is also noted that national concepts of forgery vary greatly, but, it was agreed that the deception as to authenticity refers at minimum to the issuer of the data, regardless of the correctness or veracity of the contents of the data. Parties may go further and include under the term "authentic" the genuineness of the data, if they choose so<sup>33</sup>.

Article 8 makes computer-related fraud illegal. The aim of this article is to criminalize any undue manipulation in the course of data processing with the intention to affect an illegal transfer of property and its objective is to protect assets represented or administered in computer

---

<sup>31</sup> Ibid, paragraph.65,67,68,70

<sup>32</sup>Ibid , paragraph.71,72,73,76

<sup>33</sup> Ibid, paragraph. 81,82

systems, such as electronic funds and money deposits. The computer fraud manipulations are criminalized if they are committed “intentionally”, “without right” and moreover, produce a direct economic or possessory loss of another person's property and the perpetrator acted with the intent of procuring an unlawful economic gain for himself or for another person<sup>34</sup>.

Article 9 centers on content-related offences and it tries to strengthen and modernize the existing criminal law provisions against sexual exploitation of children and expand them to electronic transmissions. The described illicit acts related to child pornography must be criminalized by the Parties if committed “intentionally”.

This provision responds to the preoccupation of Heads of State and Government of the Council of Europe, expressed at their 2nd summit (Strasbourg, 10 – 11 October 1997) in their Action Plan (item III.4) and corresponds to an international trend that seeks to ban child pornography, as evidenced by the recent adoption of the Optional Protocol to the UN Convention on the rights of the child, on the sale of children, child prostitution and child pornography and the recent European Commission initiative on combating sexual exploitation of children and child pornography. It is noted that child pornography has been criminalized in Nigeria<sup>35</sup>.

It criminalizes various aspects of the electronic production, possession and distribution of child pornography to combat the new form of sexual exploitation and endangerment of children via the internet. Paragraph 1(a) criminalizes the production of child pornography for the purpose of distribution through a computer system, when paragraph 1(b) criminalizes the “offering” of child pornography through a computer system and also intends to cover the creation or compilation of hyperlinks to child pornography sites in order to facilitate access to child pornography. Paragraph 1(c) criminalizes the distribution or transmission of child pornography

---

<sup>34</sup> Ibid, paragraph .86,89,90

<sup>35</sup> Section, 15, Child Rights Act. 2004

through a computer system, when in paragraph 1(d), actively obtaining child pornography, for example by downloading it, is criminalised. The possession of child pornography in a computer system or on a data carrier is criminalized in paragraph 1(e).<sup>36</sup>

The three types of pornographic material defined in paragraph 2 for the purposes of committing the offences contained in paragraph 1 cover depictions of sexual abuse of a real child (2a), pornographic images which depict a person appearing to be a minor engaged in sexually explicit conduct (2b), and finally images, which, although “realistic”, do not in fact involve a real child engaged in sexually explicit conduct (2c).

Paragraph 3 defines the term “minor” in relation to child pornography in general as all persons under 18 years, in accordance with the definition of a “child” in the UN Convention on the Rights of the Child (Article 1). Nevertheless, the provision allows Parties to require a different age-limit, provided it is not less than 16 years<sup>37</sup>.

Infringements of intellectual property rights, in particular of copyright, are among the most commonly committed offences on the Internet. Such protected works include literary, photographic, musical, audio-visual and other works. Each Party is obliged to criminalise willful infringements of copyright and related rights, sometimes referred to as neighbouring rights, arising from the agreements listed in the article, when such infringements have been committed by means of a computer system and on a commercial scale. Copyright and related rights offences must be committed "willfully" for criminal liability to apply. In contrast to all the other substantive law provisions of this Convention, the term "willfully" is used instead of "intentionally" in both paragraphs 1 and 2, as this is the term employed in the (Trade related

---

<sup>36</sup>Convention on Cybercrime, Explanatory Report, Explanatory report, Op.cit, p.91, paragraph.91,92, 94-98,105

<sup>37</sup> Ibid, paragraph. 94-102,104

Aspects of Intellectual Property Rights)TRIPS Agreement (Article 61), governing the obligation to criminalize copyright violations<sup>38</sup>.

Under the heading of attempt and aiding or abetting, this article relates to offences dealing with intentionally attempting or aiding and abetting “the commission of the offences defined in the Convention”. Liability under Article 11 arises when “the person who commits a crime established in the Convention is aided by another who also intends that the crime be committed”. With respect to paragraph 2 on attempt, some offences defined in the Convention, or elements of these offences, were considered to be conceptually difficult to attempt, like for example, the elements of offering or making available of child pornography.

According to the provision, it is only required that the attempt be criminalised with respect to offences established in accordance with Articles 3, 4, 5, 7, 8, 9(1)(a) and 9(1)(c)<sup>39</sup>.

Article 12 deals with the liability of legal persons. Here, liability is imposed on corporations, associations and similar legal persons for the criminal actions undertaken by a person in a leading position within such legal person, where undertaken for the benefit of that legal person. Article 12 also contemplates liability where such a leading person fails to supervise or control an employee or an agent of the legal person, where such failure facilitates the commission by that employee or agent of one of the offences established in the Convention. Under paragraph 1, four conditions need to be met for liability to attach, when under paragraph 2 Parties are obliged to have the ability to impose liability upon a legal person where the crime is committed not by the leading person described in paragraph 1, but by another person acting under the legal person’s authority. Liability under this Article may be criminal, civil or

---

<sup>38</sup> Ibid, paragraph, 107, 108, 113.

<sup>39</sup> Ibid, Paragraph. 118-122

administrative. Paragraph 4 clarifies that corporate liability does not exclude individual liability<sup>40</sup>.

The provision of sanctions and measures requires that the Convention Parties provide criminal sanctions that are “effective, proportionate and dissuasive” and “include the possibility of imposing prison sentences”<sup>41</sup>. With regard to Procedural law issues, the Convention defines powers to facilitate criminal investigations. The articles in the section for Scope of procedural provisions describe procedural measures that Convention parties must take “at the national level for the purpose of criminal investigation of the offences established in Section 1”.

Electronic data may very well be the only evidence in a criminal investigation. One way in which the Convention overcomes the problem of the speed and the easiness that this evidence can be altered, moved, or deleted, is by adapting traditional procedures, like search and seizure, to an ever-changing technological landscape. However, in order to make these traditional crime investigation methods effective, new measures have been created, such as the expedited preservation of data, the real-time collection of traffic data, and the interception of content data<sup>42</sup>.

In the provision for Conditions and safeguards, the establishment, implementation and application of the powers and procedures provided for in this Section of the Convention shall be subject to the conditions and safeguards provided for under the domestic law of each Party. Parties shall ensure that these conditions and safeguards provide for the adequate protection of human rights and liberties. The minimum safeguards to which Parties to the Convention must adhere include the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms and its additional Protocols No. 1, 4, 6, 7 and 12 (ETS N°s 005, 009, 046, 114, 117 and 177), in respect of European States that are Parties to them and also, other

---

<sup>40</sup> Ibid, Paragraph. 123-127

<sup>41</sup> Ibid, paragraph. 128

<sup>42</sup> Ibid, paragraph. 131, 134

applicable human rights instruments in respect of States in other regions of the world which are Parties to these instruments, as well as the more universally ratified 1966 International Covenant on Civil and Political Rights.

In addition, there are similar protections provided under the laws of most States. Another safeguard according to this article is that the powers and procedures shall "incorporate the principle of proportionality"<sup>43</sup>.

It is arguable that the Convention infringes upon basic human rights and liberties, with the most significant of them to be, the right to privacy.

Article 16 introduces a new measure in order to facilitate the investigation of cybercrimes. This measure, so as the other one referred in Article 17, apply to stored data that has already been collected and stored at data holders and not to real time data.<sup>44</sup>

Here, it has to be mentioned that while "data preservation" means keeping data, which already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate, "data retention" means keeping data, which is currently being generated, in one's possession into the future. On the one hand, data retention is the process of storing data. Data preservation, on the other hand, is the activity that keeps that stored data secure and safe. Articles 16 and 17 refer only to data preservation, and not data retention<sup>45</sup>.

Data preservation is for most countries an entirely new legal power or procedure in domestic law, as it is an important new investigative tool in addressing computer and computer-related crime, especially crimes committed through the Internet. The statute operates in either by the way in which the competent authorities in the Convention party country simply access, seize and secure the relevant data, or by the way in which, where a reputable business is involved,

---

<sup>43</sup> Ibid, paragraph. 145,146

<sup>44</sup> Ibid, paragraph. 149

<sup>45</sup> Ibid, Paragraph. 151,152

competent authorities can issue an order to preserve the relevant data. Convention parties are thus required to introduce a power that would enable law enforcement authorities to order the preservation of data for a particular period of time not exceeding 90 days. It is also noted that preservation measures exist at the national level in order to enable Parties to assist one another at the international level with expedited preservation of stored data located in their territory<sup>46</sup>.

The article under “Expedited preservation and partial disclosure of traffic data”, establishes specific obligations in relation to the preservation of traffic data as Article 16 and provides for expeditious disclosure of some traffic data so as to identify that other service. Obtaining stored traffic data that is associated with past communications may be critical in a criminal investigation. Article 17 ensures that where one or more service providers were involved in the transmission of a communication, expeditious preservation of traffic data can be effected among all of the service providers. Therefore, this article requires that the service provider, which receives a preservation order or similar measure, disclose expeditiously to the competent authorities, or other designated person, a sufficient amount of traffic data to enable the competent authorities to identify any other service providers and the path through which the communication was transmitted<sup>47</sup>.

The provision for production orders specifically allow “competent authorities to compel a person in its territory to provide specified stored computer data” or to compel an Internet Service Provider to provide subscriber information. Article 18 relates exclusively to production of stored or existing data. Production orders precede search and seizure as a means of obtaining specific data.

---

<sup>46</sup>Ibid, paragraph.155-157

<sup>47</sup> Ibid, paragraph. 165-169

As the powers and procedures in this Section are for the purpose of specific criminal investigations or proceedings (Article 14), production orders are to be used in individual cases concerning, usually, particular subscribers. For example, on the basis of the provision of a particular name mentioned in the production order, a particular associated telephone number or e-mail address may be requested. On the basis of a particular telephone number or e-mail address, the name and address of the subscriber concerned may be ordered. The provision does not authorize Parties to issue a legal order to disclose indiscriminate amounts of the service provider's subscriber information about groups of subscribers, like for example, for the purpose of data-mining.<sup>48</sup>

This article aims at modernizing and harmonizing domestic laws on search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Domestic legislations include powers for search and seizure of tangible objects. The aim of Article 19 of this Convention is to establish an equivalent power relating to stored data, even if it *per se* will not be considered as a tangible object.

With respect to the search for evidence, in particular computer data, in the new technological environment, many of the characteristics of a traditional search remain, with the preconditions for obtaining legal authority to undertake a search remaining the same. However, with respect to the search of computer data, additional procedural provisions are necessary in order to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of a tangible data carrier. In the case of electronic data either the physical medium on which the intangible data is stored must be seized or taken away, or a copy of the data must be made in either tangible form, such as a computer printout, or in intangible form,

---

<sup>48</sup> Ibid, Paragraph. 170,175 182

such as a diskette, before the tangible or intangible medium containing the copy can be seized and taken away<sup>49</sup>.

Article 20 addresses the subject of real-time collection and recording of traffic data for the purpose of specific criminal investigations or proceedings. Like real-time interception of content data, real-time collection of traffic data is only effective if undertaken without the knowledge of the persons being investigated. Thus, Internet Service Providers and their employees knowing about the interception must be under an obligation of secrecy in order for the procedure to be undertaken effectively. Paragraph 3 obligates Parties to adopt such legislative or other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any of the measures provided in this article concerning the real-time collection of traffic data. Paragraph 3 may be affected by the creation of explicit obligations in the law<sup>50</sup>. Traditionally, the collection of content data in respect of telecommunications, for example, telephone conversations, has been a useful investigative tool to determine that the communication is of an illegal nature.

Given that computer technology is capable of transmitting vast quantities of data, including written text, visual images and sound and that the communication through the Internet tends to be the most popular way of communication, it has greater potential for committing crimes involving distribution of illegal content. “Content data” refers to the communication  
Given that computer technology is capable of transmitting vast quantities of data, including written text, visual images and sound and that the communication through the Internet tends to be the most popular way of communication, it has greater potential for committing crimes involving distribution of illegal content. “Content data” refers to the communication content of

---

<sup>49</sup>Ibid, paragraph. 184,186,187.

<sup>50</sup> Ibid, paragraph. 216,225,226

the communication, which is the meaning of the communication, or the message or information being conveyed by the communication<sup>51</sup>. Under Jurisdiction and international cooperation, Article 21 establishes that Parties must enact laws so that they have jurisdiction of all the crimes described in the Convention if they occur in any of the four places the article mentions. In case more than one Party has jurisdiction over some or all of the participants in the crime, the affected Parties are to consult in order to determine the proper venue for prosecution where appropriate<sup>52</sup>. Countries, however, are not bound to accept these possible ways to attain jurisdiction and, thus, countries like the United States that seldom premises jurisdiction upon a nationality principle could easily ignore nationality as a base for acquiring jurisdiction<sup>53</sup>.

Chapter III (Articles 23- 35) contains a number of provisions relating to extradition and mutual legal assistance among the Parties. This was a significant point of the Treaty cybercrime legislation is plagued by a lack of geographically based jurisdictional boundaries. As Professor James Boyle noted, “If the king’s” writ reaches only as far as the king’s sword, then much of the content on the Internet might be presumed to be free from the regulation of any particular sovereign”, an observation which is particularly apt in the criminal enforcement context<sup>54</sup>.

Considering that it is impossible to regulate criminal behaviour without a means to ensure enforcement of sanctions, the objective of the drafters at this Chapter was to extend the ambit of the king’s sword through cooperation.

Article 23 sets forth three general principles with respect to international co-operation. First, it declares that international co-operation is to be provided among Parties “to the widest extent possible”. Second, it mentions that co-operation is to be extended to all criminal offences

---

<sup>51</sup> Ibid, paragraph. 228,229

<sup>52</sup> Ibid, paragraph. 239.

<sup>53</sup> Viano. C.E.Op.cit, p.92, at p,9

<sup>54</sup> Weber M.A. (2003), The Limit of Peer Production: Some Reminders for The Network Society, Yale Technology Law Journal, p.254

related to computer systems and data, as well as to the collection of evidence in electronic form of a criminal offence, meaning that either where the crime is committed by use of a computer system, or where an ordinary crime not committed by use of a computer system involves electronic evidence, the terms of Chapter III are applicable.

However, it should be noted that Article 24 (Extradition), according to which the obligation to extradite applies only to those crimes committed in Articles 2- 11, Article 33 (Mutual assistance regarding the real time collection of traffic data), according to which each Party is obliged to collect real time “traffic data” for another member country and Article 34 (Mutual assistance regarding the interception of content data), which discusses the cooperation and sharing of information obtained through means as eavesdropping and wiretapping, permit the Parties to provide for a different scope of application of these measures.

Third, it states that co-operation is to be carried out both "in accordance with the provisions of this Chapter" and "through application of relevant international agreements on international co-operation in criminal matters, arrangements agreed to on the basis of uniform or reciprocal legislation, and domestic laws".

Article 25 requires mutual assistance “to the widest extend possible”, when Article 26, referring to those cases when a Party obtains important information that may assist another member country in a criminal investigation, calls them “spontaneous information”. Article 27 discusses mutual assistance in the case of absence of applicable international agreements. Article 28, which is applicable only when no mutual assistance treaty exists, provides for confidentiality and limitations on use of information, so as to preserve sensitive materials of a host country.

Article 29 is the same as Article 16, except that it refers to international cooperation. Likewise, Article 30 is the mutual assistance version of Article 17. Article 31 requires that each

member country have the ability to search, access, or seize “data stored by means of a computer system located within its territory” for the benefit of another member country. Article 32 merely makes it permissible for a source of data that already is publicly available to be available to a Party unilaterally and without a mutual assistance request, while at the same time, not preparing a comprehensive, legally binding system. Parties become, through Article 35, members of an all “round the clock” network, in order to face effectively crimes which require a rapid response.

Improving a state’s legal ability to provide and receive international cooperation to face cybercrime effectively is not merely a question of improving its laws related to mutual assistance and extradition, but, there is a significant relationship between the legal ability to provide international cooperation and the quality of a state’s laws that define crime, establish legal investigative powers and provide safeguards. In order for the states to achieve the above goal, a number of measures<sup>55</sup> have been proposed.

The first Additional Protocol on Racism and Xenophobia on the internet (ETS 189) has been opened for signature in Strasbourg since January 26, 2003.

The Convention, as the most recent international instrument in its field, binds its ratifying Parties, shapes their domestic laws but also, functions as a model law for those Parties that consider acceding to it or serving as a model law for other states. In particular, the substantive part is meant as a framework, where new and other IT-related misuse will be added to the Convention in the form of additional protocols, like this first one, so that the Convention gives its full effect, when these protocols come into force<sup>56</sup>. The Additional Protocol after defining “racist and xenophobic material” as “any written material, any image or any other representation of

---

<sup>55</sup> Piragoff K.D.(2004) International cooperation in combating cyber-crime and cyber-terrorism, A paper presented at a Conference organized by Round Table II of the 17th International Congress of Penal Law. Held at Ant.N.Sakkoulas, on Monday, 4, October, (2004), Pp. 192-193.

<sup>56</sup> Kaspersen W.K.H.(2004) Gathering electronic evidence, A paper presented at a Conference organized by Round Table II of the 17th International Congress of Penal Law. Held at Ant.N.Sakkoulas, on Monday, 4, October,(2004)Pp.80-81

ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors”, proposes, with its Articles 3-6 certain measures to be taken at national level so as to criminalize acts of a racist and xenophobic nature committed through computer systems.

Article 7 criminalizes aiding and abetting the commission of any of the offences established in accordance with the Protocol, with intent that such offence be committed. Article 8, paragraph 1 states that Articles 1, 12, 13, 22, 41, 44, 45 and 46 of the Convention shall apply, *mutatis mutandi*, to this Protocol and paragraph 2 states that the Parties shall extend the scope of application of the measures defined in Articles 14 to 21 and Articles 23 to 35 of the Convention, to Articles 2 to 7 of this Protocol. Final provisions are included in articles 9-16. The Convention on cybercrime, as any pioneering legal tool, faced severe criticism and opposition. Among the arguments against the Convention is the claim that the Treaty restricts freedom of expression online.

Another argument against the Convention is that it overstrains the investigative powers of police forces and governmental organizations, meaning that the government is granted an excessive amount of investigatory power, which is best illustrated in the example of call data vs. “traffic data”. Before the Treaty, law enforcement agencies were allowed to seek call related data, such as the phone numbers that are dialed and the duration of the calls. However, under the Convention, law enforcement authorities would have the right to wide-ranging “traffic data,” which includes the source, destination, and duration of calls, as well as the type of traffic or the sort of services consulted. A point of discussion is whether it is a violation of privacy if an Internet Service Provider is forced to inform law enforcement agencies about the downloads, e-

mails and duration of visits to particular websites a client did<sup>57</sup>. The American Civil Liberties Union claims that United States authorities will use the Convention to conduct surveillance and searches that would not be permitted under current United States law. European critics worry that the Convention allows the transfer of personal data to countries outside Europe—such as the United States—that they believe have less protective laws regarding the use of such information. Council of Europe officials dismiss such fears, arguing that the Convention provides adequate civil liberty safeguards and limits information transfers to specific criminal investigations<sup>58</sup>.

Another point of criticism is that the Treaty obliges companies and individuals to provide law enforcement with far greater information than is considered the norm under most telecommunications laws. Internet Service Providers (ISPs) and other related businesses keep “subscriber data”, which is confidential client records and they are unwilling to offer them to an investigating governmental agency. Moreover, companies are concerned with the increased costs associated with retaining and preserving data should an order be served upon the company to do so and it is ultimately the consumer that will need to weigh the importance this cost<sup>59</sup>. Meanwhile, some business and consumer groups are concerned that the Convention’s provisions that increase costs to service providers impede the development of security technologies and sale of encryption programs, and negatively affect consumer confidence in e-commerce.

Another hot topic is that the Convention infringes upon citizen civil liberties. Article 15 requires member countries “to establish conditions and safeguards to be applied to the” governmental powers established in Articles 16 thru 21. Those conditions and safeguards are required “to protect human rights and liberties”. Article 15 in fact “lists some specific

---

<sup>57</sup> Keyser .M. (2003), Common Goods and Evil?: The Formation of Global Crime Governance, *Transnational Law and Policy Journal*, (12): 324-326

<sup>58</sup> Archick K. (2002) Europe Convention on Cybercrime of November 2001. A report of Congressional Research Service (CRS) on cybercrime presented to the Congress in USA on 26, April, (2002), The Council of Europe Convention, Retrieved February 16,2014 from <http://www.usembassy.it/pdf/other/RS21208.pdf/>

<sup>59</sup>Keyser .M,Op.cit. p.108 at p.33

safeguards, such as requiring judicial supervision that should be applied where appropriate in light of the power or procedure concerned”<sup>60</sup>.

The Global Internet Liberty Campaign (GILC), a non-profit, non-governmental organization, whose member organizations have joined together to protect and promote fundamental human rights such as freedom of speech and the right of privacy on the net for users all over the world, is strongly opposed to certain guidelines of the Treaty. GILC has drafted two letters against the Treaty’s provisions because it believes that they run contrary to internationally accepted human rights norms and infringe on the free speech and privacy rights of all internet users<sup>61</sup>. On the other hand, some analysts criticize the Convention as being too “indulgent” or “soft”, because of not permitting police authorities direct cross-border access to computer data, which they argue creates an extra, time-wasting step<sup>62</sup>.

Another point of consideration is that the states that participated in the Convention’s negotiations are not the “problem countries” in which cyber criminals operate relatively freely. Hackers frequently route cyber attacks through portals in Yemen or North Korea, neither of which are part of the Convention, so skeptics point out that for the Convention, in order to serve as a deterrent, more states will have to sign it and abide by its mandates.

As an example, it is noted that the Filipino author of the “I Love You” virus that caused millions of dollars in damage worldwide in 2000 was never prosecuted because no applicable laws existed<sup>63</sup>.

---

<sup>60</sup> Ibid

<sup>61</sup>Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber crime. Version 24.2, December 12, 2000.( GILC) (2000), Retrieved February 16, 2014 from <http://gilc.org/privacy/coe-letter-1000.html> and <http://gilc.org/privacy/coe-letter-1200.html/> .

<sup>62</sup>. Archick K. Op.cit,108, at p.33

<sup>63</sup> Ibid

Computer crime, and especially cybercrime, is not a specific new form of crime, but rather a wide variety of new phenomena, which encompasses both new types of crimes, as well as traditional crimes committed in connection with computer systems or computer networks<sup>64</sup>.

This represents a tremendous challenge for the criminal law.

The Convention on cybercrime is based on three pylons. First, it defines criminal offenses and sanctions under their domestic laws for four categories of computer-related crimes—fraud and forgery, child pornography, copyright infringements, and security breaches such as hacking, illegal data interception, and system interferences that compromise network integrity and availability. Second, it establishes domestic procedures for detecting, investigating, and prosecuting computer crimes, and collecting electronic evidence of any criminal offense. Such procedures include the expedited preservation of computer-stored data and electronic communications, search and seizure of system, and real-time interception of data. Third, it establishes a rapid and effective system for international cooperation. The Convention deems cybercrimes to be extraditable offenses, and permits law enforcement authorities in one country to collect computer-based evidence for those in another. It establishes an all “round the clock” contact network to provide immediate assistance with cross-border investigations.

Above all, parties to the Convention must guarantee the conditions and safeguards necessary to protect human rights and the principle of proportionality. There is no doubt that the Treaty represents a flexible and effective vehicle in combating cybercrime and a useful tool in harmonizing the law and improving cooperation between legal systems in the field of computer crime. The fast changing nature of cybercrime, nevertheless, necessitates both the monitoring of future developments in computer crime and further analysis of new threats which the criminal

---

<sup>64</sup> Sieber U. (2004) Computer crimes, cyber-terrorism, child pornography and financial crimes, A paper presented at a Conference organized by Round Table II of the 17th International Congress of Penal Law. Held at Ant.N.Sakkoulas, on Monday, 4, October, (2004) pp. 47-50

law will be required to address<sup>65</sup>. Moreover, the sensitive nature of the fundamental human rights, such as the privacy and freedom of speech, require borders at the guidelines and the procedures which restrict them.

### **3.4 Development of Legal and Institutional Mechanisms at Regional Level**

There are many regional international organizations, with a narrow or broad coverage of states, more or less making efforts to maintain cyber security and harmonize international measures to combat cybercrime. This section will introduce some of these organizations, which have taken typical actions in combating cybercrime and also review African Regional efforts.

#### **(i) The Organisation for Economic Co-operation and Development (OECD)**

The OECD was the first international organization that initiated guidelines for computer crime.<sup>66</sup> By its nature the OECD does not establish treaties, and it is devoted to the promotion of a global coordinated policy approach. The OECD established a Task Force on Spam in 2004 The OECD Working Party on Information and Privacy (WPISP) develops international guidelines on cyber security and in 2002 published a document titled “Security of Information Systems and Networks: Towards a Culture of Security.” In 2008 it released “Scoping paper on online Identity theft” a report with some recommendations on how to fight identity theft (this document also suggested to recognise identity theft as a separate offence in criminal laws.) It was followed up in 2009 by the “OECD Policy Guidance on Online Identity Theft” report.

---

<sup>65</sup> Ibid

<sup>66</sup> Schjolberg, S. (2013) Cybercrime Law. “Securing Cyberspace: A Comparative Review of Strategies Worldwide” A paper presented at the Conference on (Global organization) organized by Privacy and Cybercrime Institute of Ryerson University Canada. Held on Tuesday, March 19, 2013. Retrieved February 14, 2014 from <http://www.cybercrimelaw.net/OECD.html>

**(ii) The North Atlantic Treaty Organization (NATO)**

By virtue of its mandate NATO focuses more on cyber-attacks carried by countries or national elements against NATO members.<sup>67</sup> NATO's Senior Civil Emergency Planning Committee (SCEPC) assists NATO members in the protection of civilian populations from terrorist attacks against critical infrastructure and is also responsible for coordinating the civil critical infrastructure. NATO's Civil Communication Planning Committee (CCPC) is responsible for the electronic public and non-public communication infrastructures, and has published several papers on civil communications infrastructures. NATO's Civil Protection committee (CPC) has initiated work on critical infrastructure protection, and developed a Critical Infrastructure Protection Concept Paper in 2003. NATO's Industrial Planning Committee (IPC) has also contributed on preventive measures for the protection of critical infrastructure. NATO established a Centre of Excellence for Defense against Terrorism in 2008.

**(iii) The Shanghai Cooperation Organization (SCO)**

This is an organization of Russia, China and several former Soviet republics. These countries have entered into the Shanghai Convention on Combating Terrorism, Separatism and Extremism. SCO has also issued several related statements: The Yekaterinburg Declaration of 2009 mentioned information security as one of the main priorities in a common system of international security. In 2012 SCO's Heads of State Council meeting in Beijing stated: "The SCO will stand firm to fight against terrorism, separatism and extremism as well as international cybercrime"<sup>68</sup>.

---

<sup>67</sup> Avner, L. (2013) International Comparison of Cyber Crime, A paper presented at the Conference on (Global organization) organized by Privacy and Cybercrime Institute of Ryerson University Canada. Held on Tuesday, March 19, 2013.p.9

<sup>68</sup> Schjolberg, S.Opcit. p.111, at p.41

Sometimes international cooperation against cyber crime is established with a very particular goal and not just on a national level but between specific governmental agencies. An example of such organization is The Virtual Global Taskforce (VGT)<sup>69</sup>.

**(iv) The Virtual Global Taskforce (VGT)**

VGT is an alliance of international law enforcement agencies and private sector partners working together to combat online child sexual abuse. Specifically, the VGT comprises the Australian Federal Police as Chair, the Child Exploitation and Online Protection Centre in the United Kingdom, the Royal Canadian Mounted Police, the United States Department of Homeland Security, INTERPOL, the Italian Postal and Communication Police Service, the Ministry of Interior for the United Arab Emirates, the New Zealand Police and Europol.<sup>70</sup>

One more particularly notable international organization against cyber crime is Strategic Alliance Cyber Crime Working Group.

**(v) Strategic Alliance Cyber Crime Working Group (SACCWG)**

SACCWG was assembled in 2006. It is a special unit consisting of five law enforcement agencies. The Australian High Tech Crime Centre (AHTCC), FBI (USA), New Zealand Police, Royal Canadian Mounted Police, and Serious Organized Crime Agency (United Kingdom)<sup>71</sup>.

Over the last five years several countries repeatedly tried to initiate discussion about the need for common international Cyberspace Treaty, suggesting that bilateral and regional agreements are not enough to secure cyberspace and prevent cyber-war.

---

<sup>69</sup> Ibid, (Virtual Global Taskforce Official Website) Retrieved, February 14, 2014 from <http://www.virtualglobaltaskforce.com/>

<sup>70</sup> Ibrahim Baggil (2003) The Fight Against Transnational Cybercrime, Business & Economics platyplus Magazine: Journal of the Australian Federal Police. (80): 4-6.

<sup>71</sup> Ibid

**(vi) The Asia-Pacific Economic Cooperation (APEC)**

In the Asia-Pacific region, the APEC coordinates its 21 member economies to promote cybersecurity and to tackle the risks brought about by cybercrime<sup>72</sup>. The APEC has conducted a capacity-building project on cybercrime for member economies in relation to legal structures and investigative abilities, where the advanced APEC economies support other member-economies in training legislative and investigative personnel<sup>73</sup>.

After the 9/11 attacks on the United States of America, the APEC Leaders issued a Statement on Counter-Terrorism, condemning terrorist attacks and considering it urgent to reinforce collaboration at different layers to fight against terrorism. The Leaders called for reinforcing APEC activities to protect critical infrastructure<sup>74</sup>.

The Telecommunications and Information Ministers of the APEC economies issued the Statement on the Security of Information and Communications Infrastructures and a Programme of Action in 2002<sup>75</sup>, supporting measures taken by members to fight against misuse of information. The Senior Officials' Meeting has made a recommendation which designates six areas that can serve as the foundation for the APEC's endeavor for cybercrime prevention, comprising legal development, information sharing and cooperation, security and technical guidelines, public awareness, training and education, and wireless security<sup>76</sup>. The Ministers and Leaders of APEC have made a commitment to "endeavour to enact a comprehensive set of laws

---

<sup>72</sup> Skol Harnsuthivarin,(2003) Cyber Security and the Safety of Electronic Commerce. A paper presented at the Workshop organized by APEC, Cyber Security Electronic Commerce Steering Group. Held in Phuket, Thailand from 15-16 August 2003. Pp43-46

<sup>73</sup> Xingan Li, (2004) International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene. A paper presented at the Workshop organized by APEC Cybercrime Expert Group, on APEC Telecommunications and Information, 29th Meeting. Held in Hong Kong, China from 21-26 March 2004, p.28

<sup>74</sup> David L,(2001) International Relations of Asia.: In Report of APEC Leaders Statement on Counter-terrorism, in the APEC Economic Leaders' Meeting. Held in, Shanghai on 21 October 2001.p.63

<sup>75</sup>The Asia-Pacific Economic Cooperation(2002) Recommendation by the APEC Telecommunications and Information Working Group (TEL) to APEC Senior Officials (SOM) for an APEC Cybersecurity Strategy, 2002/CSOM/052, Concluding Senior Officials Meeting, held in Los Cabos, B.C.S., Mexico, from 21-22 October, 2002.

<sup>76</sup>Ibid

relating to cybersecurity and cybercrime that are consistent with the provisions of international legal instruments, including the UN General Assembly Resolution 55/63 and Convention on Cybercrime by October 2003"<sup>77</sup>.

In response to this call from the leaders, a survey of laws was carried out and a summary was made of the responses from member economies received in 2003<sup>78</sup>. The economies proposed corresponding projects in information-security task groups. For example, the U.S. proposed a project in the E-Security Task Group of the Telecommunications and Information Working Group.

The first phase of this project was a meeting of cybercrime experts from around the region. The meeting was held from 21-25 July, 2003 in Bangkok, Thailand, and was attended by over 120 delegates from 17 economies. The objectives of the meeting were to assist the economies to develop the necessary legal frameworks; to promote the development of law-enforcement capacity; and to strengthen cooperation between private and public sectors in addressing the threat of cybercrime<sup>79</sup>. In the conference, the experts present agreed that every economy needed a legal framework including one for substantive and procedural law, and for the law and policies of inter-economies cooperation. They confirmed the role of international instruments, particularly the Convention on Cybercrime. They also emphasized jurisdictional cooperation, law-enforcement construction, and the capacity building of the investigators<sup>80</sup>.

In 2005, The sixth APEC Ministerial Meeting on the Telecommunications and Information Industry passed the Lima Declaration, "encouraging all economies to study the 2001 Convention on Cybercrime and to endeavor to enact a comprehensive set of laws relating to

---

<sup>77</sup>Xingan Li, *Op.cit*, p.114, at p.45

<sup>78</sup>The Asia-Pacific Economic Cooperation, (2003) Media Release on Conference on the Strengthening International Law-enforcement Cooperation to Prosecute Cyber Criminals, Hackers, and Virus Authors. Held in Bangkok on, 25, July 2003.

<sup>79</sup> *Ibid*

<sup>80</sup> *Ibid* at, p.46

cyber security and cybercrime that are consistent with international legal instruments, including UN General Assembly Resolution 55/63 of 2000 and the Convention on Cybercrime of 2001<sup>81</sup>.

However, due to the great difference between member economies within the APEC, the development toward unified legal instruments has not been too satisfactory. Although some economies have claimed that their laws have been completely consistent with the Convention, and some other economies were taking actions to implement provisions similar to the Convention, many other countries have quite different legal systems or have no law criminalizing cybercrime.

Efforts are still to be made in the forum of the APEC to address cybercrime. The U.S. proposed the Judge and Prosecutor Cybercrime Capacity Building Project in 2006 in order to develop a curriculum devised by government and private sector experts; to translate the curriculum into domestic languages; and to train the trainer (judges and prosecutors)<sup>82</sup>.

**(vii) The Council of Europe (COE)**

The Council of Europe has been working to tackle rising international anxiety over the risks brought about by the automatic processing of personal data since the early 1980s. For example, on 13 September 1989, the Committee of Ministers of the Council of Europe adopted Recommendation R (89) 9 of the Council of Europe on Computer-Related Crime, which contained guidelines for national legislatures<sup>83</sup>. In 1981, the Council of Europe implemented the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108, 26 January 1981), which was revised according to the Amendment to Convention ETS No. 108 Allowing the European Community to Accede, 15 June 1999, and the

---

<sup>81</sup>Lima declaration, (Article 26)The 6th APEC Ministerial Meeting on the Telecommunications and Information Industry (TELMING). Held in Lima, Peru from 1-3 June, 2005.

<sup>82</sup>The Asia-Pacific Economic Cooperation, Report on 2006 Budget - Operational Account Project: TEL 04/2006 - Judge and Prosecutor Cybercrime Capacity Building Project, 2006/BMC1/012-6, Budget and Management Committee Meeting. Held at APEC Secretariat in Singapore from 29-30 March 2006

<sup>83</sup>Council of Europe, Convention on Cybercrime, CETS No.185, status as of 20 March, 2006.

Additional Protocol to Convention ETS No. 108 on Supervisory Authorities and Trans-border Data Flows, 8 June 2000. The Convention recognized the desirability "to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing, "and the necessity" to reconcile the fundamental values of the respect to privacy and the free flow of information between peoples" (Preamble). The Convention covers the protection of personal data in both the public and private sectors.

Chapter II of the Convention established basic principles for data protection, one of which is data security (Article 7), covering the prohibition of accidental or unauthorized access, alteration and dissemination.

The expert committee appointed in 1985 published Recommendations of 1989 and 1995, addressing the issues of substantive laws and procedural law in this area respectively as per the provision in Recommendation No. R. (95) 13).

Recommendation R. No. (89) 9 recognized the importance of an adequate and quick response to the new challenge of computer-related crime, which often has a trans-border character, and recommended the governments to consider the Report on Computer-Related Crime drawn up by the European Committee on Crime Problems.

Then there is Recommendation No. (95) 13 Concerning Problems of Criminal Procedure Law Connected with Information Technology. The Recommendation recognized that information systems may also be used for committing criminal offences, evidence of criminal offences may be stored and transferred by these systems, while the criminal procedure law of member states often do not provide for appropriate powers to search and collect evidence in these systems during a criminal investigation. The appendix to the Recommendation lays down

the principles for criminal procedure laws on search and seize, technical surveillance, obligations to co-operate with the investigating authorities, electronic evidence, use of encryption in research, statistics and training, and international cooperation.

In 1997, the Council of Europe began drafting the Convention on Cybercrime, which was open for signature in 2001 and took effect in 2004<sup>84</sup>. In 2003, the Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer System (ETS NO. 189) was implemented. The Convention addresses substantive law, procedural law, jurisdiction, and international law in the field of cybercrime. The Convention is a historic landmark in the combat against cybercrime. It is expected that the Convention will have a deep impact on the legal reform relating to cybercrime in its 46 member states and one candidate state.

In the 2004 Conference on Cybercrime, the Council of Europe called for "wide and rapid" access to and "effective implementation" of the Convention on Cybercrime, raising awareness in the highest political level, and encouraging cooperation between public and private sectors<sup>85</sup>.

In the 2005 Conference on Cybercrime, the Council of Europe expressed concern about the fast-increasing threats and serious social and economic results of cybercrime including terrorist activity on the Internet, noting that most cybercrime is international cybercrime, recognized the need for effective and compatible laws and tools to enable efficient cooperation to combat cybercrime, calling upon public and private cooperation, and encouraging access to the Convention on Cybercrime<sup>86</sup>.

---

<sup>84</sup>Council of Europe. In: Conference report on The Challenge of Cybercrime. Held in Palais del 'Europe, Strasbourg, France from 15-17 September 2004.

<sup>85</sup>Herman, Van R, (2005)Cybercrime: A Global Challenge, A Global Response. A paper presented at a conclusion meeting organized by Council of Europe. Held in Madrid, Spain, from 12-13 December,2005.

<sup>86</sup>Ibid

In 2006, the Council of Europe launched a Project against Cybercrime, intended to grant assistance to the development of national legislation in line with the provision of the Convention, training of judges, prosecutors and law-enforcement officers, and training of criminal justice officials and 24/5 contact points in international cooperation.

**(viii) The European Union (EU)**

The EU took a series of actions to tackle cybercrime through impelling a coordinated law enforcement and legal harmonization policy. Civil liberty has also been a focus in the anti-cybercrime field.

In 1995, the European Parliament and the Council endorsed Directive 95/46/EC of 24 October 1995 on the protection of Individuals with regard to the Processing of Personal Data and on the Movement of Such Data. Section VIII of the Directive specifically deals with confidentiality and security of processing of personal data. The Directive applied to protection of natural persons (Article 2(a)). The scope of the Directive was limited to the processing of personal data entirely or partially by automatic means (Article 3-1). The Directive required that appropriate technical and organizational measures have to be implemented to protect personal data against illegal destruction, alteration, access and other illegal forms of processing (Article 17-1).

The Directive required the Member States to provide administrative and judicial remedies for the victim (Article 22), and provided for the compensation liability of (Article 23) and sanctions on (Article 24) the transgressor.

In 1997, the European Parliament and the Council endorsed Directive 97/66/EC of 15 December 1997 concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. The Directive was aimed at furthering the protection implemented

in Directive 95/46/EC, and providing for the harmonization of the member states' provision to attain an equivalent level of protection (Article 1-1). The Directive extended the protection of legitimate interests to legal persons (Article 1-2).

The application scope of the Directive was limited to the processing of personal data relating to the provision of publicly available telecommunications services in the public telecommunications networks; particularly via the ISDN (Integrated Services Digital Network), and public digital mobile networks (Article 3-1). As the Directive 95/46/EC is concerned with automatic processing systems, Directive 97/66/EC has emphasized the linkage with the telecommunications network. The Directive provides requirements directly targeted at the service providers (but not member states) "to take appropriate technical and organizational measures to safeguard the security of its services." (Article 4-1). The Directive requires the Member States to implement the regulations ensuring the confidentiality of communications, prohibiting listening, tapping, storage or other kinds of interception or surveillance of communications by unauthorized natural and legal persons (Article 5). The Directive limited unsolicited communications (Article 12), which covers automatic calling systems or facsimile machines, but not e-mails.

On 27 November 2001, a plenary session took place in Brussels of the European Union Forum on Cybercrime, organized by the European Commission<sup>87</sup>, and where the primary discussion was about the retention of traffic data.

In April 2002, the Commission of the European Communities presented a proposal for a Council Framework Decision on Attacks against information systems, and this proposal

---

<sup>87</sup>European Commission, EU Forum on Cybercrime. In: Plenary session. Held in Brussels on November, 27, 2001.

constitutes the case of the Decision of 24 February 2005<sup>88</sup>. The Framework Decision criminalized the offences of illegal access to information systems (Article 2), illegal system interference (Article 3), illegal data interference (Article 4), and instigation, aiding and abetting of these offences or attempt at them (Article 5). The Framework Decision only dealt with attacks through unauthorized access to or interference with information systems or data. According to the Decision, illegal access can only be constituted when the illegal activities are targeted intentionally against an "information system with specific protection measures in place and [the attacks] must be for economic gain." (Article 2).

The Commission further considered the future possibility of "specific protection measures" (Proposal for a Council Framework Decision on Attacks against information systems) to broadband networks, saying that, "it is necessary that criminal law covers unauthorized access to their systems even though there may not be adequate technical protection for their systems." Thus, concerning the interference with information systems, it is constituted by serious "hindering" or "interrupting" of the functioning of information systems by "inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data" (Article 3).

This Framework Decision does not specify penalties for illegal access to information systems and instigation, aiding and abetting and attempting of these offences, but requires member states to take the necessary measures to ensure that they are punishable by effective, proportional and dissuasive criminal penalties (Framework Decision, Article 6.1). The Decision specifies the penalties for illegal system interference and illegal data interference as punishable by criminal penalties to a maximum of at least one to three years of imprisonment (Article 6.2).

---

<sup>88</sup>Council's Framework. In Report of 24 February 2005 on attacks against information systems, Official Journal L069, Decision 2005/222/JHA (2005) Pp. 0067-0071.

As for the "aggravating circumstances", the criminal draws a maximum of at least two to five years imprisonment (Article 7.1). These aggravating circumstances include an organized attack, and an attack that has "caused serious damages or has affected essential interests" (Article 7.2). Criminal organization is defined as a "structured association, established over a period of time, of two or more persons, acting in a concerted manner with a view to committing offences". Article 1, (Joint Action 98/733/JHA of 21 December, 1998) adopted by the Council on the Basis of Article K.3 of the Treaty on European Union, Official Journal<sup>89</sup>.

It is worth noting that the matters mentioned in the Framework Decision can also be found in the Convention on Cybercrime<sup>90</sup>. After revision of the legislation required by the Convention, the national law (of Finland) will also meet the demand of the Framework Decision<sup>91</sup>. Today, comprised of 27 member states and three candidate countries, the EU remains active in addressing cybercrime.

**(ix) The Organization of American States (OAS)**

As other regional organizations, the Organization of American States (OAS) with 35 member states is also highly concerned about the issue of cybercrime. Through its forum for the Ministers of Justice or of the Ministers or Attorneys General of the Americas (REMJA), the OAS has long recognized the central role that a sound legal framework plays in combating cybercrime and protecting the Internet.

Such recognition has prompted the REMJA to recommend the creation of the Group of Governmental Experts on Cybercrime (The Group of Experts) in March 1999<sup>92</sup>. The Group of

---

<sup>89</sup> European Union official Journal (OJ L 351, (1998, December 29) Retrieved February 16, 2014 from, [www.eur-europa.eu/legal-content](http://www.eur-europa.eu/legal-content).

<sup>90</sup>Xingan Li Op cit.p.114, at 45

<sup>91</sup> Ibid

<sup>92</sup>Report of Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA II). Held in Washington, DC 20006, USA. On 28, March 1999, Chapter V. Retrieved, February 16, 2014 from [www.oas.org/en/remja/background.asp](http://www.oas.org/en/remja/background.asp).

Experts has been devoted to analyzing cybercrimes, to inspecting the domestic cybercrime law, and to finding ways of cooperating in the Inter-American system of combating cybercrime. The Group of Experts has held four meetings. The First Meeting and Second Meeting were held in May and October 1999, separately, the Third Meeting in June 2003, the Fourth Meeting in February 2006, all in Washington D. C. United State of America<sup>93</sup>.

The Meeting of the Ministers of Justice or of the Ministers or Attorneys General of the Americas (REMJA. 'III')<sup>94</sup> has urged member states to take steps to endorse cybercrime law; harmonize cybercrime laws to make international cooperation possible. The Meeting of the Ministers of Justice or of the Ministers or Attorneys General of the Americas (REMJA. 'V')<sup>95</sup> has recommended that member states evaluate the advisability of implementing the principles of the Convention on Cybercrime, and consider the possibility of acceding to that Convention.

In 2004, the Fourth Plenary Session of the Organization of American States General Assembly passed the resolution on "Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity," proposing that "An effective cybersecurity strategy must recognize that the security of the network of information systems that comprise the Internet requires a partnership between government and industry".<sup>96</sup>

#### **(xi) Africa Regional Efforts**

---

<sup>93</sup> Xingan Li. *Op cit.* P.114, at, 45 see also OAS web site, Retrieved, February 14, 2014 from [http://www.oas.org/juridico/english/cyber\\_experts.htm](http://www.oas.org/juridico/english/cyber_experts.htm).

<sup>94</sup> The Organization of American States, Report. In: Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA III). Held in Washington D.C, USA, (1999) Chapter IV.

<sup>95</sup> The Organization of American States, Report In: Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA V) Held in Washington D.C. USA (2000) Appendix I.

<sup>96</sup> The Organization of American States, Resolution, AG/RES. 2040 (XXXIV-O/04), Adopted at the fourth plenary session of the Organization of American States General Assembly. Held on 8 June 2004 in Quito, Ecuador.

In all of this, the African Region is not left out as the regional heads seems to understand the menace of cybercrime and it seems even clearer that there is need for adequate legislation in order to secure the cyber space.

The African Region have so far made tremendous efforts while being guided with a mindset that an appropriate legal and regulatory environment for the knowledge economy ensures that there are set rules and regulations which allow the ICT sector to be more competitive allowing the economy to grow. It has been noted that there is a core relationship between the level of attainment of knowledge economy and the inflow of financial investments. Countries that have advanced economies such as Japan, Germany, Australia, United Kingdom and United States of America have all embraced e-commerce activities, as a way of life and enacted cyber legislation to regulate e-commerce activities.

African countries aspire to attract financial investment to boost economic growth and should therefore embrace this trend for the creation of a knowledge economy. However, Africa is lagging behind and there is fear that Africa will be excluded from the digital revolution. Africa faces a number of challenges such as lack of technologically advanced telecommunications infrastructure, lack of legal and regulatory frameworks supportive of ICT developments and the high rate of illiteracy.<sup>97</sup> The report further recommended that an enabling environment which allows/ encourages creation of a knowledge economy is of paramount importance.

It is noted that between this report of May 2009 and year 2014, African region has made tremendous advancement in the development of legal regime to combat cyber security and crime. For instance, ICT policies and regulation have continued to develop in Africa with increased pressure from the convergence of technologies and awareness of the importance of ICT as a tool

---

<sup>97</sup>United Nations Economic and Social Council, Economic Commission for Africa. In: Report of a Workshop on Legal and Regulatory Framework for the Knowledge Economy. Held in Ethiopia from 28, April -1, May 2009 at p.12

for social and economic growth.<sup>98</sup> There has been a continued effort by regional bodies in promoting regional consensus around policies and regulation that promote the ICT sector since the Connect Africa Summit. The major players are the African Union Commission, the Economic Commission for Africa (UNECA) and regional economic communities such as the East African Community (EAC), the Central African Economic Community (ECCAS), the Common Market for Eastern and Southern Africa (COMESA), the Economic Community for West African States (ECOWAS) and the Southern African Development Community (SADC).<sup>99</sup> Notwithstanding this development, it is educative to trace the various steps that may be regarded as the road map to the appreciable level that Africa as a region has achieved today in the fight against cyber crime.

**(a) Economic Commission of Africa (ECA)**

In recognition of the challenges as earlier enumerated in the Ethiopia conference report of 2009, Economic Commission of Africa (ECA) upon the request of its Member States launched the Africa Information Society Initiative (AISI). This was the first framework of its kind to concretely prioritize the issue of ICTs within the socio-economic development agenda. This initiative was approved by the ECA Conference of Finance Ministers in 1996 and adopted the same year by the Summit of Heads of State and Governments of the Organization of African Unity (OAU) and ultimately supported by the then G7+1 as Africa's major ICT initiative in its 1997 Denver Summit. The AISI recommendations fed into the World Summit on the Information Society (WSIS) Action Plans and are the cornerstone of the New Partnership for Africa's Development (NEPAD) ICTs Short Term Action Plan where ICT projects and initiatives have

---

<sup>98</sup> Ladan M.T. (2015) *Cyberlaw and Policy on Information and Communications Technology in Nigeria and Ecowas*. Ahmadu Bello University Press Limited Zaria. pp.431-432

<sup>99</sup> Ibid

been initiated to speed up sub regional/regional connectivity.<sup>100</sup> Africa Information Society Initiative (AISI) provides the road map to guide African countries in addressing the challenges of emerging globalization and the information age by developing and implementing National Information and Communication Infrastructure (NICI) policies and plans.<sup>101</sup>

**(b) Africa Information Society Initiative (AISI)**

AISI is the action framework that has been the basis for information and communication activities in Africa for over ten years. It is therefore in this context that a workshop on “Legal and regulatory frameworks for the knowledge economy” was organized on 28 April 2009 at the UN Conference Center in Addis Ababa, Ethiopia. The workshop, which was organized with the support of the Organisation Internationale de la Francophonie (OIF), United Nations Conference on Trade and Development (UNCTAD) and Internet Society (ISOC), analyzed the formulation and modalities for adoption of legal and regulatory frameworks which is one essential element towards the creation of an enabling environment for the knowledge economy.<sup>102</sup>

A general overview of the status of cyber legislation in Africa as at 2009 was presented in the report of the Ethiopia conference.<sup>103</sup> The status as per the 2009 report shows that although an increasing number of African countries have embarked on designing and formulating ICT policies, the majority of them are still in the early stage of cyber legislation development and enactment. This position is true of most countries including Nigeria who has just enacted a Cybercrime Act<sup>104</sup> only on 15<sup>th</sup> of May, 2015.

---

<sup>100</sup>United Nations Economic and Social Council , Economic Commission for Africa (WSIS) Academia Research Network Brainstorming. In: Report of Workshop held in Ethiopia from, 9 – 11, June 2004. p. 20

<sup>101</sup> Ibid

<sup>102</sup>United Nations Economic and Social Council, Economic Commission for Africa. In: Report of Workshop on Legal and Regulatory Framework for the Knowledge Economy. Held in Ethiopia from 28 April -1 May 2009 at p.2.

<sup>103</sup> Ibid at p.4

<sup>104</sup> Cybercrime (Prohibition Prevention Etc) Act, 2015

**(c) The Economic Community for West African States (ECOWAS)**

The Economic Community of the West African States (ECOWAS) in September 2004 conducted a situational assessment survey which involved meetings with ICT policy makers within ECOWAS. The findings were that there was no appreciable legislation on e-Commerce in member states. As a result a workshop was organized by Economic Commission of Africa (ECA) in Ouagadougou in December 2006. The workshop proposed that a legal framework for e-Commerce and related activities had to be formulated and draft guidelines were to be drafted and circulated to member states before adoption by ECOWAS. Following a workshop on 11 December 2007 in Lome, Togo the participants from the ECOWAS states adopted new guidelines on combating cyber crime in the sub-region. As a result of this process, Ministers in charge of Information and Communication Technologies adopted a harmonized ICT legal framework, a bill on e-commerce in ECOWAS states and a model ICT framework. The Acts aimed at modernizing the instruments for promoting e-commerce, preserving personal data and curbing cyber crime through the necessary sub-regional and national legislation. The Regional workshop on Legal and political frameworks for Information Society in West Africa took place in Senegal on 11-13 March 2009. The workshop recommended inter alia, the extending of harmonization of text to cover important issues not yet examined such as regulating convergence of telecoms and media, harmonizing models of intellectual property rights, cyber security etc by creating regional norms.<sup>105</sup> Since this workshop there are indications that “ECOWAS regards ICT as a key tool for development and a sector that can bring growth and competitiveness to the

---

<sup>105</sup> United Nations Economic and Social Council, Economic Commission for Africa. In: Report of Workshop on Legal and Regulatory Framework for the Knowledge Economy. Held in Ethiopia from 28, April – May, 2009 at p.5

region. The revised ECOWAS Treaty puts a strong commitment on the establishment of a common market for ICTs and for harmonization of legislation”.<sup>106</sup>

The council of Ministers of ECOWAS has made telecommunications policy a particular priority in fostering competition and granting operating licences on a priority basis to private investors that are interested in entering market in the region. ECOWAS has also achieved a considerable expansion of international bandwidth as a result of the landing of Glo 1 and Main One between 2009 and 2011.<sup>107</sup>

ECOWAS has also been active in promoting regulatory harmonization and regional mobile roaming. ECOWAS’ regulatory harmonization efforts are being carried out through the West African Communications Regulators Assembly (WATRA). WATRA is the latest regulators’ association that has adopted guidelines in licensing, universal access, frequency management, numbering, interconnection, data management, digital migration and cybersecurity.<sup>108</sup>

In 2009, ECOWAS adopted a legislative framework in cybersecurity, a key area that has been a challenge to the region. The proposed legal document on cybersecurity that has been adopted by ministers in charge of ICT serves as a tool for a harmonized sub-regional penal framework for cybercrime. ECOWAS has also supported the establishment of computer emergency response teams (CERT) at the national level with the assistance of the ITU and is considering setting up a harmonized framework for a certification authority and the creation of public key infrastructure for the region.<sup>109</sup>

---

<sup>106</sup>Ladan M.T.Opcit,p.125 at,439

<sup>107</sup> Ibid. Pp. 439-440, see , p.440 for other projects for promoting infrastructure development

<sup>108</sup> Ibid

<sup>109</sup> Ibid

**(d) East African Community (ECA)**

The five member states of the East African Community (EAC) are also coordinating efforts to harmonize and pass cyber crime laws that would be effective throughout Burundi, Kenya, Rwanda, Tanzania and Uganda. A common information security policy on cyber crime formulated by East African countries will serve as a foundation for new laws. In 2006, with the support of United Nations Conference on Trade and Development (UNCTAD) several East African Community (EAC) workshops were organized which focused on the area of e-commerce, these include the two workshops held in April in Kampala which were on the Cyber laws and E-justice and Information security. In the same year another workshop on legal aspects of e-commerce was held in December in Nairobi. The workshops agreed on the need to formulate a Regional task force to spear head and develop model cyber laws covering e-signatures, electronic transactions, authentications, cyber crimes and data and consumer protection. The task force also had to review existing laws and thereafter develop a regional legal framework for harmonization of cyber laws. In June 2008, a framework for the adoption of laws to deal with electronic transactions, e-signatures and authentication, data protection and privacy, consumer protection and computer crime was reviewed by EAC member states.<sup>110</sup> All these efforts paid off as the current position has revealed a tremendous progress from the 2009 Ethiopian conference report.

The East African Community's initiative in the area of ICT policy and strategy derives from its treaty, which states that "member states shall facilitate an enabling environment to promote private sector investors in the info-telecommunication equipment within the

---

<sup>110</sup> Ibid at p.7

community”. The ECA Development Strategy 2006-2010 captures “Information and Communication Technology Integrated into regional development objective.”<sup>111</sup>

In 2010, the ECA Secretariat adopted a policy to ensure that a new, independent regional network linking the capitals of the partner states be established. The goal of the EAC-BIN network is to address missing links and ensure that landlocked countries in the region have access to the submarine landing stations at the same cost as coastal countries.<sup>112</sup>

**(e) Arab Maghreb Union**

Unlike the other RECs, the Arab Maghreb Union (AMU) does not have a specific policy to promote ICT within the region nor is there an association of telecommunications regulators. However, the region’s regulators do meet within other fora such as the African Telecommunications Union (ATU), the Arab Information and Communication Technologies Organization (AICTO) OF THE League of Arab States, and the Arab Regulators Network (AREGNET) (AFDB). Some of the regulators are also members of the Francophone Telecommunications Regulatory Network (FRATEL) or the Euro-Mediterranean Regulators Group (EMERG).<sup>113</sup>

**(f) South African Development Community (SADC)**

The South African Development Community has been very active in the development of ICT policies and strategies in support of the development of the ICT sector. The SADC Regional Indicative Strategic Development plan (RISDP) document states that: “ it is imperative for the SADC Region to review and refocus development strategies and approaches by aggressively using ICT as a catalyst for socio-economic development and prosperity”.<sup>114</sup>

---

<sup>111</sup>Ladan M.T. Op.cit, p.125, at,436

<sup>112</sup> Ibid

<sup>113</sup> Ibid at,441

<sup>114</sup> Ibid at,444

SADC's approach to achieving this is contained in its Declaration on Information and Communications Technology (ICT), which sets out commitments amongst other things, to create favourable regulatory environments for the deployment of ICTs and promote the use of ICT in/for business development. The RISDP specifies Areas of Focus with respect to ICTs.<sup>115</sup>

SADC's ministers of communications have committed themselves to a variety of priority areas of action in policy and regulatory support for the development of the telecommunication sector. The latest commitment came from the meeting of Heads of States of Governments in 2007 that discussed ICT issues and recognized the need to promote investment in infrastructure and the development of the SADC Regional Infrastructure Development Master Plan (RIDMP) as a basis for benchmarking infrastructure development. At the 2010 Luanda Ministerial meeting, the SADC ICT Regional Priorities for 2011/2012 were adopted and grouped along the three key priority areas of Infrastructure Development, Policy and Regulatory Framework, and Postal Operations and Regulation.<sup>116</sup>

**(g) Comparative Legal Initiatives in West African Economic and Monetary Union (UEMOA)<sup>117</sup>**

Pursuant to Article 42 of the UEMOA Treaty, the Assembly adopt additional Acts where necessary, the Council of Ministers (of Foreign Affairs) enacts regulations, directives and decisions and the Commission adopts regulations for the implementation of the Council's act and decisions.

Pursuant to Article 43, regulations have a direct and binding effect, directives have to be transposed into national Law with an obligation to achieve the defined result and the decisions have a direct effect for the addressee.

---

<sup>115</sup> Ibid

<sup>116</sup> Ibid at,445

<sup>117</sup> Ibid at,456

Acts of primary law- that have been signed by Member States and not by one of the organization's institutions- are subject to signatories' ratification process.<sup>118</sup>

**(h) Comparative Legal Initiatives in Inter-Governmental Authority on Development (IGAD)<sup>119</sup>**

Pursuant to the Agreement establishing IGAD the Assembly of Heads of State and Government (Article 9), the Council of Ministers (Article 10) and the Committee of Ambassadors (Article 11) are vested with a decision making power. No precisions are provided about the effect of those decisions.<sup>120</sup>

### **3.5 Development of Legal and Institutional Frameworks at National Level**

Problem of cyber crime induced many states to reconsider their own legislation. Nowadays more than 100 countries (including 60% Interpol members) have no laws or regulations to fight cyber crimes<sup>121</sup>. The problem in regulating cyber crime is that there are no uniform laws. Some countries, such as the United Kingdom, have cyber crime laws like the Computer Misuse Act (1990) that are well implemented, other territories have laws that have yet to be fully implemented, while some countries are yet to make provisions for cyber crimes within their judicial system at all.<sup>122</sup>

Detailing the position of legislation in countries of the world is beyond the scope of this work. Therefore, the discourse here shall be limited to one main concern, that is: the position in Nigeria.

---

<sup>118</sup> Ibid ( see p. 457 For tabular analysis )

<sup>119</sup> Ibid at,p.469

<sup>120</sup> Ibid ( see p. 470 For tabular analysis)

<sup>121</sup> Victor Sabadash. (2004) Law Improvement: The legal base in fighting cyber crime. A paper presented at the conference organized by Computer Crime Research Center (CCRC). Held at Computer Crime Research Center, Eth- Zurich, on October, 27, 2004.

<sup>122</sup> Handbook of Information Security Management: Law Investigation, and Ethics. Retrieved February 16,2014from,[www.cccire/prg/Documents/hism/522525.html](http://www.cccire/prg/Documents/hism/522525.html).

## **Position in Nigeria**

### **(a) The General Statutes for Fighting Criminal Activities**

Nigeria as a nation has several statutes that prohibit and punish criminal activities.<sup>123</sup> The traditional statutes in Nigeria fighting general crimes are the Criminal Code Act<sup>124</sup> and the Penal Code Law.<sup>125</sup> There are however other statutes that are enacted to fight certain specific and special crimes, some of which are discussed below.

Before now, the Nigerian government had adopted various regulatory measures to fight economic and financial crimes in the country. Some of such measures include, among others is first, the promulgation of the National Drug Law Enforcement Agency (NDLEA) Act No. 48 of 1989 – which was meant to confront the menace of money laundering, and to comply with the Vienna Convention; second, the Failed Bank (Recovery of Debt and Financial Malpractice in Banks) Act No. 18 of 1994 – which was promulgated to check the cases of money laundering and insider abuses by bank officials in the country; third, the Money Laundry Act of 1995; fourth, the Advanced Fee fraud (419) Act of 1995; and fifth, the comprehensive amendments of the Banks and Other Financial Institutions Act (BOFIA) and the Central Bank of Nigeria Act in 2002. Also worthy of mention is the Anti-Corruption Act of 1999 as amended in 2000, which established the Independent and Corrupt Practices and Other Related Offenses Commission.

These laws today look very out-of-place in the present era of cybercrime. However, the new cybercrime Act, 2015<sup>126</sup> has cured all foreseeable defects in all the various criminal statutes before its enactment on 15<sup>th</sup> of May 2015. The general overview of the cybercrime Act, 2015 with arguably, the merit and demerit of the Act is fully discussed in this chapter ahead.

---

<sup>123</sup> Chukkol K, (2010) The Law Of Crimes in Nigeria Ahmadu Bello University Press Nigeria, Revised Edition p.495

<sup>124</sup> Criminal Code Act Cap. C38 Laws of the Federation (LFN) 2004 applicable with few modification in all southern States of Nigeria.

<sup>125</sup> Penal Code Law Cap.89 Laws of Northern Nigeria 1963 applicable in all northern states and F.C.T subject to few modifications

<sup>126</sup> Cybercrime (Prohibition prevention Etc) Act, 2015

In order for the understanding of how Nigeria had fared before the enactment of this cybercrime Act, it is instructive to assess and trace the development of the earlier efforts to tackle cybercrime in Nigeria in order to obtain a better idea of how the law is developing in this area. To this extent, this chapter will examine some of the statutes that were the saving grace prior to the enactment of the cybercrime Act.

Before the enactment of the cybercrime Act, 2015, the government, interestingly, in recognition of the lapses in the earlier mentioned laws on electronic financial transactions and commerce has long been occupied with efforts to close such gaps. In 2001, for instance, there was a proposition for the establishment of a National Electronic Commerce Council (NECC) under the Federal Ministry of Science and Technology. The body, which was later dumped in 2003, was expected to serve as the regulatory body for e-commerce and would have been made up of professionals from the public and private sector.

**(b) The Genesis of the Cybercrime Act, 2015**

The Nigerian legislative arm (the National Assembly) has since 2001 been deliberating two bills relating to the Internet and electronic usages – the Internet Freedom bill and the Electronic Data bill. While the Internet Freedom bill was aimed at empowering the government to implement an integrated internet policy that will ensure a vibrant internet culture in the country; the Electronic Data bill was targeted at according electronic data legal effect, validity, admissibility or enforceability. On its own side, the former also proposes an Internet curriculum for the educational institutions to align with global trends by equipping Nigerian students with relevant Internet skills for the global age, while the latter was focused partly on addressing all issues concerning electronic commerce in the country using consistent and environmental friendly regulatory frameworks.

**(c) The Economic and Financial Crimes Commission (Establishment) Act, 2002 (EFCC)**

In 2001, the Nigerian government also inaugurated the National Committee on Advance Fee Fraud (NCAFF), and charged the body with the task of formulating the more effective strategy for fighting fraud perpetrators and their agents in the country. This was against the backdrop of the plan by the United States, Britain and France, among others, in November 2001, to sanction Nigeria unless some serious steps were taken to solve the menace of Nigerian financial crimes<sup>127</sup>. A deadline to this effect was given as December 15, 2002. The report of this committee culminated into the passage into law of the Economic and Financial Crimes Bill 2002, which among others established the Economic and Financial Crimes Commission (EFCC). The 19-member Commission was set up specifically to deal with cases of obtaining under false pretence (419) and enforce the various laws relating to banking in Nigeria. Its relevance in the general fight against Internet banking frauds lies in the fact that the regulation establishing it gives it unrestricted access to investigate the accounts of bank customers suspected of 419 frauds.

This is one of the statutes that came into existence during the regime of former President Olusegun Obasanjo in 2002 and amended in 2004 and it was called Economic and Financial Crimes Commission Act.<sup>128</sup> The EFCC was primarily established to fight the notorious then ‘new’ crimes promoted by Nigerians both within and outside the country called Advanced Fee Fraud.<sup>129</sup> This ‘new’ crimes are committed by Nigerians in various ways including the use of modern information technology systems or services such as computers, internet and e-mails. Advance Fee Fraud became known as 419, the name given to such offence under the conventional Criminal Code Act. The EFCC however is not only vested with powers to fight the

---

<sup>127</sup> Ezeoha A (2006 April) Regulating Internet Banking in Nigeria, *Journal of Internet Banking and Commerce*.(11):4

<sup>128</sup> Economic and Financial Crimes Commission Act, Cap. E1 L.F.N. 2004

<sup>129</sup> Advance Fee Fraud and Other Related Offences Act, Cap. A6 L.F.N 2004

crime of 419 but other crimes that have direct or indirect negative results in the nation's economy and finances such as money laundering, corruption, financial fraud, embezzlement and mismanagement leading to collapse or failure of Banks and other financial institutions. The EFCC no doubt by the nature of the offence of 419 gets itself fighting Cybercrimes and computer related offences.

On its own, the EFCC has since 2003 championed some legislative moves for the amendment of the country's Criminal Procedure Law to allow for the easiness of prosecution, "the legal regime as it is currently couched is prone to manipulation"<sup>130</sup>. It is noted that with the new cybercrime Act, 2015 the fear of manipulation may have been conquered. The EFCC Chairman's areas of concern for amendment include "bail, adjournment, spurious motions, unduly long trials and underhand tactics for which lawyers are notorious in employing to delay the legal process and he advocated that they ought to have been addressed in the light of the experience of the ICPC, which could not secure a considerable number of convictions for four years after it was established".<sup>131</sup>

Unfortunately, this latter concerns of the EFCC Chairman is an issue of Constitutional provisions and Court procedural laws so even the new cybercrime Act, 2015 is not able to address it.

**(d) The Nigeria Cybercrime Working Group (NCWG)**

In 2003, a new national body - the Nigerian Cybercrime Working Group (NCWG), was inaugurated under the Chairmanship of the Attorney General of the Federation and Minister of Justice. This body since 2004 has worked on a project titled "National Cybersecurity Initiative", which is aimed at developing cyber crime and cyber security regulations in the country. These

---

<sup>130</sup> Ribadu N, (2003, December 4) Vanguard Newspaper, p.7 . (During an interview with Disu J, as then Chairman of EFCC.)

<sup>131</sup> Ibid

efforts culminated into a draft proposal, the “Computer Security and Critical Infrastructure Protection Act”, which was sent to the National Assembly, to be passed to law. Some of the intents of the proposed law are to create a central institution (the National Cybercrime Working Group) that will be responsible for the enforcement of its provisions; and to seek to regulate the security of computer systems and networks and protect sensitive ICT infrastructures.<sup>132</sup> The law when promulgated seeks to prohibit three main classes of conduct, namely: (1) Conduct against computer systems, with “Offence in this category made up of activities like unauthorized access to computer systems, access exceeding authorization, computer systems and networks interference, systems intrusion, data interception, denial of service, computer trespass, email bombing, etc.; (2) Conducts utilizing ICT systems to commit unlawful acts or crimes, covering such offences as computer contamination, illegal communications, computer vandalism, cyber-squatting, cyber-terrorism, cyber-pornography, online intellectual property theft, etc.; and (3) Unlawful conduct against critical ICT infrastructures in Nigeria.<sup>133</sup>

The Nigerian Cyber crime Working Group (NCWG), is an intergovernmental body. The body has its membership made up of the all key law enforcement, security, intelligence and ICT agencies of government, plus major private organizations in the ICT sector; including Economic and Financial Crimes Commission (EFCC), Nigeria Police Force (NPF); the National Security Adviser (NSA), the Nigerian Communications Commission (NCC); Department of State Services (DSS); National Intelligence Agency (NIA); Nigeria Computer Society (NCS); Nigeria Internet Group (NIG); Internet Services Providers' Association of Nigeria (ISPAN); National Information Technology Development Agency (NITDA), and Individual citizen representing public interest; with its leadership made up of two Chairmen and one Coordinator. The Group is

---

<sup>132</sup>Ikeocha D, (2004 August 2,) Nigeria Move to Protect ICT Infrastructures, Daily Sun Newspaper, p.11

<sup>133</sup>Ibid

expected to handle cyber crime and cyber security matters and coordinates enforcement, investigation, as well as prosecution, with other law enforcement agencies in the country.

**(e) Central Bank of Nigeria Guidelines on Electronic Banking**

In 2003, the Central Bank of Nigeria released the Guidelines on Electronic Banking in Nigeria. The main intent of the guidelines was to define technical requirements and permissible scope of electronic banking, as well as the modalities for adherence by Nigerian banks.

**(f) The Advance Fee Fraud and Other Related Offences Act, 2006**

A Bill, tagged Advance Fee Fraud and other Fraud –related Offences Bill 2005 was proposed in 2005. The Bill after due deliberation by the National Assembly became the Advance Fee Fraud and Other Related Offences Act, 2006 as amended.<sup>134</sup>

The Act in part II, under Electronics Telecommunication Offences, etc provides that any person or entity providing the electronic communication service of remote computing service either by e-mail of any other form, who fails to comply with the provision of the Act, commits an offence and is liable on conviction to a fine of ₦100,000.00 and forfeiture of the equipment or facility used in providing the service.<sup>135</sup> It also specifies that any person or entity convicted more than once under this Act shall have his operational licence revoked or cancelled.<sup>136</sup>

**(g) National Identity Management Commission Act, 2007 (NIMC)**

In 2007, the National Assembly had foreseen the emergent confusion and had enacted the National Identity Management Commission Act to take care of this emergent confusion and to enact into existence a body that would be charged with building a central database for the country from where other agencies would share. The May 2007 NIMC Act,<sup>137</sup> which empowered

---

<sup>134</sup> Advance Fee Fraud and Other Related Offences Act, CAP. A6 LFN 2004 as amended in 2006.

<sup>135</sup> Section, 12 ( 3), Advance Fee Fraud and Other Related Offences Act 2006

<sup>136</sup> Section, 13 (6) , Advance Fee Fraud and Other Related Offences Act 2006

<sup>137</sup> National Identity Management Commission Act, No. 23, 2007

NIMC to set up, manage and operate the National Identity Database (NID), automatically made the Commission the sole operator and manager of an all-embracing database.

The ramifications of the tasks of the Commission and the direct relationship it would have with the activities of the other end-user organizations, had compelled the NASS to make those bodies to sit on the NIMC governing board. Specifically, agencies like the National Population Commission (NPC), Economic and Financial Crimes Commission (EFCC), Federal Road Safety Corps (FRSC), Federal Inland Revenue Service (FIRS), Independent National Electoral Commission (INEC) with obvious linkages was also included, not as competitors, but rather as enhancers and facilitators as end-user organizations of the central identity database that would be generated by NIMC. That made clear and obvious sense, so as to erase the confusion that would be created when every Tom, Dick and Harry started building a central database. The NIMC Act, 2007 which repealed the law that had set-up the Department for National CivicRegistration (DNCR) enabled NIMC to inherit the assets and operation of the DNCR and to more holistically embark on the implementation of the National identity Management System, which it developed to embrace all aspects of central data management modalities and platforms.

Under its mandate, it started with the task of establishing its offices across the 36 states of the country from where it would carry out its mandated tasks on a permanent basis as opposed to the once in a while method of other agencies which periodically embark on data collection activities.

A very innovative feature of the NIMC mandate is the plan to provide every adult Nigerian or legal resident in Nigeria, with a unique National Identity Number (NIN) which would, apart from providing a secure means of accessing the National Identity Database so that

an individual can irrefutably assert his or her identity, it would become an omnibus reference number which would open a secure window.

The National Identity Management Commission (NIMC) is charged with the responsibility of creating, managing, and operating the National Identity Database<sup>138</sup> established pursuant to NIMC Act.<sup>139</sup> NIMC also has the duty to carry out the registration of citizens of Nigeria and non-citizens lawfully resident in Nigeria into the National Identity Database<sup>140</sup>. To this end, the NIMC has been given the responsibility of maintaining, operating and managing all identity registration centers in Nigeria.

After laying some foundation for eventual enrolment of Nigerians into the database, NIMC has commenced the creation of a database by using 10 fingers and head-to shoulder photograph. “Once you are enrolled in that database, you will be given a unique national identification number (NIN).

With these two in place, you can be issued the National ID Card, a multi-purpose smart card. You can confirm your identity, with or without your card, because the number is there and that number is related to a database”.<sup>141</sup> Every citizen from the age of 16 years and above and legal residents are eligible to enroll for the NIN.

Besides, the entire existing ID database System in the country will be harmonized and integrated into the National ID Database. Data from existing government agencies including INEC (voters’ registration) and NCC (SIM registration), Immigration (international passport registration), FRSC (driver’s license) and FIRS (tax registration) will be integrated. Once the

---

<sup>138</sup> Section 5(a) of the National Identity Management Commission Act No. 23, 2007,

<sup>139</sup>Section 14 NIMC Act 2007.

<sup>140</sup> section 5 (b) and (c) NIMC Act, 2007,

<sup>141</sup>Chris Onyemenam, (then NIMC’s Director General and Chief Executive Officer) (Public Awareness Campaign) Retrieved February 22, 2014 from <http://3.blogspot.com>.

integration is achieved, no government agency would have any valid excuse to embark on any ID scheme.

**(h) Terrorism (Prevention) Act, 2012**

Considering a report on “a Bill for an Act to amend the Terrorism (prevention) Act, 2012,” brought forward by its Conference Committee during plenary, the Senate in a unanimous resolution, held that there was no alternative to punishing terrorism offenders than death.

All the senators who contributed to the issue, did not spare persons or corporate bodies linked to any terrorist acts in the country as they said people knowingly in or outside Nigeria directly or indirectly and who “willingly assist, facilitate, organize or direct the activities of persons or organizations engaged in acts of terrorism are liable on conviction to maximum of life imprisonment.”<sup>142</sup>

The Terrorism (prevention) Act, 2011 (amendment) Bill, 2012 was passed by the Senate on October 17, 2012 and in the House of Representatives on October 11, 2012 but after the development, some differences were noticed in the two versions of the Bill, prompting it to be re-submitted where the Conference Committee was constituted comprising both chambers on October, 2012 to reconcile the areas of differences, which appeared in six clauses of the Bill. New amendments to Section 17 of the Terrorism Act, gave a clear distinction between “an act of terrorism” and “an act of conspiracy.” For the latter, an imprisonment for a term of not less than twenty years is prescribed.

A new provision (section 1A) dealing with national coordinating bodies in counter terrorism designates specific institutions and vest specific powers and functions.

---

<sup>142</sup> Joseph Erunke. (2014, July 20) Senate Okays Death Penalty for Terrorists. Vanguard Newspaper, p.3

In line with the new amendments, the Office of the National Security Adviser, (ONSA), shall be the coordinating body for all security and enforcement agencies including the Attorney General of the Federation, (AGF), under the Terrorism Act.

The new version of the bill stipulates that the AGF is to ensure conformity of Nigeria's counter-terrorism laws and policies with international standards and United Nations conventions on Terrorism as well as maintain international co-operation required for preventing and combating international acts of terrorism.

The Conference Committee added a new section (30) under clause 14 dealing with detention of conveyance. Accordingly, any person who without reasonable excuse, fails to comply with the requirement of a detention order or intentionally obstructs or hinders any person acting in accordance to detention order shall on conviction be liable to a fine of N5,000,000 or imprisonment for not less than five years.

Amendments of Sections 26-29 of the prior Terrorist Act produced a new Section 28 which allows relevant law enforcement or security officials to detain suspected terrorist for a period not exceeding forty-eight hours after arrest without having access to any person, or a medical officer.

Anti-terrorism Act, gives law enforcers greater powers to detain and prosecute suspects and gave judges more guidance on handing down punishments. The Act also gives the police and security forces powers to seal off a property or vehicle without a search warrant.

**(i) The National Information Technology Development Agency Act, 2007 (NITDA)**

The National Information Technology Development Agency Act 2007 was meant to give a legal bite to the establishment of the National Information Technology Development Agency to plan, develop and promote the use of information technology in Nigeria.

NITDA is empowered to advise the government on ways of promoting the development of information technology in Nigeria including introducing appropriate information technology legislation, to enhance national security and vibrancy of the industry.<sup>143</sup>

The Act also provided that “Information Technology” encompasses all forms of technology used to create, store, exchange and use information in its various forms ( business data, voice, conversation, still images, motion pictures multimedia presentations and other forms including those not yet conceived).<sup>144</sup>

**(j) The Criminal Code Act**

The Nigeria Criminal Code Act<sup>145</sup> may be an old legislation in Nigeria but it is noted that it is not a completely useless legislation in fighting cybercrime which is a modern day method of stealing per se. The Criminal Code Act criminalizes any type of stealing and it does not matter in whatever form, it is an offence punishable under the Act. Although cyber crime is not mentioned in the Act, it is a type of stealing and it is punishable under the criminal code. The most renowned provision of the Act is Chapter 38, which deals with obtaining Property by false pretences i.e. cheating.

The specific provisions relating to cyber crime is section 419, while section 418 gave a definition of what constitutes an offence under the Act. Section 418 states that any representation made by words, writing, or conduct, of a matter of fact, either past or present, which representation is false in fact, and which the person making it knows to be false or does not believe to be true, is a false pretence.

Also, section 419 states that 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

---

<sup>143</sup> Section 6(i), NITDA Act, 2007

<sup>144</sup> Section 34 (interpretation) NITDA Act 2007

<sup>145</sup> Criminal Code Act, Cap.C38 LFN 2004

person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years.

**(k) Nigerian National Policy for Information Technology Act, 2001(NPFIT)**

The government of the Federation in 2001 commissioned a body of experts to design a National Policy on Information Technology. The policy was expected to deal with all emerging issues in the information and communication technology fields. The perception of the Policy is correct that Information Technology (IT) is the bedrock for national survival and development in a rapidly changing global environment, and challenges us to devise bold and courageous initiatives to address a host of vital socio-economic issues such as reliable infrastructure, skilled human resources, open government and other essential issues of capacity building.<sup>146</sup>

The General Objectives as provided in section “(vii) is To improve judicial procedures and enhance the dispensation of justice...” (xv) to empower the youths with IT skills and prepare them for global competitiveness...” and “(xvii) To create IT awareness and ensure universal access in order to promote IT diffusion in all sectors of our national life...”

The Policy’s objective in (xxiii) provides for promoting “legislation (Bills and Acts) for the protection of on–line business transactions, privacy and security.” This appears to be the most pertinently framed objective of the policy.

In further clarifying its objectives, the policy defines ‘Information Technology’ to mean “computers, ancillary equipment, software and firmware (Hardware) and similar procedures, services (including support services) and related resources.” The term ‘IT’ is also defined to include “any equipment or interconnected system or sub-system of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information.” This comprehensive

---

<sup>146</sup>*Nigerian National Policy for Information Technology*, (NPFIT 2001) Federal Ministry of Science and Technology, Abuja. p.ii

definition captures well all imaginable uses, and abuses, of the cyberspace. Further relevant to cyber-criminality and explanatory of the policy are its chapters 9, 12, 13, 14, 16 and Appendix B. Chapter 9 section 9 (3) 'Strategies' states: "(i) Provide a sound responsible and efficient regulatory environment." At (4), it states: "providing legal safeguards for the privacy of individuals and the confidentiality of transactions against misuse." In Chapter 12 ("National Security and Law Enforcement"), the pertinent issues are in Section 12(3) which reveal's the "strategies" of the NPFIT. These are: (i) to use IT "to combat contemporary and emerging security threats and challenges that are being re-defined by Information Technology"; and (ii) to promote "the awareness and education of all those engaged in National Security and law enforcement duties on the use, benefit and risks of new IT environment."

The policy also proposed (iii) to inform and protect Nigerians, the government, infrastructure and assets "from illegal and destructive activities found in the global environment" in order to boost the confidence of Nigerians and the international community in the country. In (iv) the policy says: "Government ... will frame appropriate legislation." Chapter 13 of the IT policy, on legislation, reiterates the proposition (iv) in Chapter 12(3). It states: "The nation shall promote and guarantee freedom and rights to information and its use, protect individual privacy and secure justice for all by passing relevant Bills and Acts."

The objectives of legislation, as stated in the policy, are to facilitate e-governance, e-commerce, secure e-fund transfer and electronic payment system, and protection of government's digitalized records and information. Other objectives include establishing and enforcing 'cyber laws' to deal with 'computer crime'. Cyber legislation, according to the Policy, shall also encourage public confidence in IT and its proper usage, "enhance freedom and access to digital information at all levels while protecting personal privacy, promote intellectual

property rights and copyrights, and address other issues arising from the digital culture and protect the rights of the vulnerable groups.”

To realize the foregoing legislative objectives, the strategies of the IT policy are stated as follows:

The National Information Technology Development Agency (NITDA) and the Federal Ministry of Justice are to work out Bills and Acts that would bring about free access and rights to information, and other on-line transactions, with due protection, security and property rights, for individuals as well as for groups. The policy would also seek to introduce the necessary machinery for verifying and admitting in evidence electronically generated records and digital evidence in the event of administrative and legal proceedings, which will be digitalized as much as possible. Also very important in the policy is the plan to review relevant existing laws to make the implementation of the IT policy unhindered. The policy will, in addition, see to the passage of ‘Computer Crime and Cyber Laws (CCCL)’. In chapter 16, (“policy implementation”), the policy at 16(2) (xxi) restates that it will see to the enactment of “Bills and Acts to stimulate and protect the right of users and developers including intellectual property rights.”

Towards realizing the above objectives, the policy, in Appendix B (Details on the Legal Areas that must be addressed”), states inter alia:

Government through the Federal Ministry of Justice, after due deliberation with IT and sectoral experts, will frame appropriate legislation, using technology-neutral statutory definitions. The legal mechanisms so framed are to apply in the following areas: computer crimes, information technology law, and amendment of non-specific provisions in existing laws. Other areas of application are personal privacy and digital signature.<sup>147</sup>

---

<sup>147</sup> Ibid (NPFIT, 2001) Appendix B, 40

The Federal Government constituted a cyber crime working group, the Nigeria Cybercrime Working Group (NCWG), to examine all associated problems of cyber-criminality as related to Nigeria and make appropriate submissions to government on how to nip them in the bud. This body was formally launched on 31st March 2004, sequel to the recommendations of the Presidential Committee on Illegal On-line activities led by the National Security Adviser to Ex-President Olusegun Obasanjo (1999-2007).<sup>148</sup> The constituent member of this group is as already discussed supra.

The effort of the working group resulted in a draft Cybercrime Bill that was before the National Assembly since 2004. This Bill was fine-tuned and re-presented to the National Assembly severally with the latest being: The Cyber Crime Bill 2013 which is discussed infra. It is noted that this Bill has eventually culminated to the enactment of the cybercrime Act, 2015.

The commissioning of the policy could be seen as a manifestation of the Nigerian government's awareness of the pivotal role of information and communication technologies in the contemporary world.<sup>149</sup> This awareness of government was well captured in the Policy thus: "Information Technology (IT) is the bedrock for national survival and development in a rapidly changing global environment."<sup>150</sup> Cognate to this governmental awareness, the IT policy focused on some areas that should be covered by appropriate laws. Of particular relevance here is the section of the IT policy on Information Technology Law. This section proposes to:

Criminalize the use of computers and related technologies for the commission of crimes or to facilitate criminal behaviour, wrongful access, and deceitful usage; and criminalize the targeting of

---

<sup>148</sup>Ezeoha A, (, 2006 )"Regulating Internet Banking In Nigeria: Some Success Prescriptions – Part 2", *Journal of Internet Banking and Commerce*. (11) :5,

<sup>149</sup>Obada R, Oke M ( 2012, May 30).Cyber Capacity without Cyber Security: A Case Study of Nigeria's National Policy for Information Technology (NPFIT). *The Journal of Philosophy, Science and Law*. (12): 7

<sup>150</sup> "Executive Summary", *Nigerian National Policy on Information Technology (IT)*, Federal Ministry of Science and Technology, Abuja March 2001:p. ii.

computers and the data contained within them through an authorized access, unlawful copying of information, damage or tampering with such information, and /or depriving the legitimate owner of data of the benefit of such data.<sup>151</sup>

Wide-ranging in its coverage of cybercrimes as this aim of government was, nothing was done towards enacting either an Information Technology Law or a Computer Crime Law until 2004 when the NCWG was created.<sup>152</sup> The NCWG, a unit of the National Information Technology Development Agency (NITDA), worked out a foundation for a cybercrime law for Nigeria.<sup>153</sup> As proposed, the envisaged law would include a substantive law that would criminalize the following kinds of conduct: (i) Conducts against information and communication technology (ICT) system, (ii) Conducts using ICT systems as tools for committing crime, and (iii) Legally prohibited conducts that have essential ICT infrastructures as targets.<sup>154</sup> It will also contain some procedural provisions that deal with investigation of crime, collection of evidence relating to cybercrime as well as procedures for searches, seizures and interception of digital communication.<sup>155</sup> The third component of the proposed law is an array of options on infrastructure and institutional arrangement. The details of this component are: (i) promote and develop specialized units to deal specifically with ICT offences, as units of existing law enforcement formations, (ii) facilitate cooperation between industry and law enforcement agencies, (iii) create an advanced ICT centre to collect, collate, analyze, and circulate relevant technical information to and for other relevant Agencies, and (iv) if need be, create an entirely new cybercrime and cyber security agency at par with other specialized agencies like Economic and Financial Crime Commission (EFCC), Independent Corrupt Practices and Other Related

---

<sup>151</sup>Ibid, Appendix B; 47.

<sup>152</sup>Obada R, Oke M. Op.cit. p.158 at. 6

<sup>153</sup>Udotai B, (2004) Challenges of Cybercrime Enforcement in the ECOWAS Sub-Region-Case Study-Nigeria, a Paper presented at a seminar organized by NCWG. Held at NITDA Building Abuja.

<sup>154</sup>, (Sections,2, 9, and 13.) *National Policy on Information Technology Act*, 2001

<sup>155</sup> Ibid. at Section 9

Offences Commission (ICPC), National Drug Law Enforcement Agency (NDLEA), National Agency for the Prohibition of Traffic in Persons (NAPTIP), National Agency for the Control of AIDS (NACA) and National Agency for Food and Drug Administration and Control(NAFDAC).<sup>156</sup>

The NCWG had a correct perception and apprehension of the enormity of the problem of cybercriminal as reflected in the conclusion of its report as follows:

Enforcing cybercrime in Nigeria is a necessary compliment to the great strides the Nigerian Government has made towards transforming Nigeria into an ICT–driven economy. To leave our systems and networks unprotected is to deliberately endanger the same infrastructures we worked so hard and invested so much to build.<sup>157</sup>

The lofty ideal encapsulated in this statement is in the right direction and in accordance with what obtains in the highly more technologically and economically advanced countries.<sup>158</sup>

#### **(I) Cybercrime Draft Bill 2004**

The Nigerian state has demonstrated her willingness to enact an Act on Cybercrime and security since 2004 when the presidency had repeatedly presented draft bills on Cyber security and crime to the National Assembly for passage into law.

One provision by the Nigerian Cybercrime Working Group (NCWG) in the proposed Nigeria Cybercrime draft Bill, 2004, is a Data Retention Law that required Nigerian Information Technology and Telecommunications Service Providers, to implement prolonged archival procedures for all transactional records generated for a period of five years. The Draft Data Retention Law also compels these Service Providers, to make transactional records available to Nigerian Law Enforcement agencies, for investigation or prosecution proceedings. The proposed

---

<sup>156</sup>Ibid, at sections,10& 16.

<sup>157</sup>Ibid, at section,18.

<sup>158</sup>Obada R, Oke M, Opcit.P.158, at.6

draft law, however, did not require Nigerian Law-Enforcement officials to obtain due process court order before obtaining Data Retention records from Nigerian Service providers.

The five year requirement was however dropped in the final draft of the law while new parameters was set to ensure that ISPs keep records of traffic and transactions on their networks which will be made available to security agencies on request.<sup>159</sup>

**(m) The Cybercrime Draft Bill 2005**

In 2005, the Nigerian government adopted the Computer Security and Critical Information Infrastructure Protection Bill (known as the Cybercrime Bill). The Bill aims to *‘secure computer systems and networks and protect critical information infrastructure in Nigeria by prohibiting certain computer based activities’* and to impose liability for global crimes committed over the Internet. The Bill requires all service providers to record all traffic and subscriber information and to release this information to any law enforcement agency on the production of a warrant. Such information may only be used for legitimate purposes as determined by a court of competent jurisdiction, or other lawful authority. The Bill does not provide independent monitoring of the law enforcement agencies carrying out the provisions, nor does the Bill define ‘law enforcement agency’ or ‘lawful authority.’

Finally the Bill does not distinguish between serious offenses and emergencies or minor misdemeanors. As a result it may conflict with Section 37 of The 1999 Constitution of Federal Republic of Nigeria(as amended), which guarantees the privacy of citizens including their homes and telephone conversations, absent a threat on national security, public health, morality, or the safety of others.

On a cursory look, the bill aims at putting in place a coordinated legal regime that will secure computer systems and networks in Nigeria. It was expected to also protect critical

---

<sup>159</sup>Shina B. (2005, January, 14) “Nigeria and IT laws: progress made” Techtimes news. p.1

information infrastructure by providing criminal liabilities and penalties for harmful computer – based activities.

The bill cures the defect in our justice system, to wit, reception and the evidentiary weight attached to electronic documents. It makes provisions for activities like unlawful access to computers, unauthorized disclosure of access code, fraudulent electronic mail messages, cyber terrorism, pornography and other general offenses against critical information infrastructure.

The bill seeks severe penalties for cyber crimes and was before the National Assembly. It recommends as punishment, fines varying from ₦15million to ₦20million and a maximum term of thirty years imprisonment for anyone who commits cyber related crimes. The bill also aims at securing computer systems and networks in the country. It seeks to protect critical information infrastructure by providing criminal liabilities and penalties for undesirable activities carried out through the use of computers and other information and communication technology devices.

Sponsored by Presidency, the proposed law is titled, “Computer Security and Critical Information Infrastructure Protection Bill 2005”.

The twenty-eight page document has appeared in the National Assembly Journal 18, Volume 3 of 13<sup>th</sup> July 2006. It has already passed the first reading in the House of Representatives but couldn’t push through as an Act before the end of that assembly.

Listed in the bill are eighteen computer - related offences. Such as: fraud; fraudulent electronic mail messages, computer forgery; cyber – squatting; system interferences; denial of service (by providers); unlawful access code; identity theft; cyber – terrorism; violation of intellectual property rights with the use of computers, using computers for unlawful sexual purposes.

Part IV, section 20 of the bill provides that the President may on the recommendation of the National Security Advisor, by order published in the Federal Gazette, designate certain

computer systems, networks and information infrastructure vital to national security or the economic and social well being of the citizens as constituting critical information infrastructure.

A Presidential order in section 20 might require audit and inspection on any crucial information infrastructure to evaluate compliance with the provisions of the Act. Under this section, any person who infringes on the bill “commits an offense and shall be liable, on conviction to a fine of not less than ₦15million or imprisonment of a term not less than 25years or to both such fine and imprisonment.”<sup>160</sup>

Section 30(1) provides for a fine not less than (₦10, 000,000) ten million or term of imprisonment of not less than 10 years or to both such fine and imprisonment for an offence of cyber – terrorism.

Unfortunately, “cyber or information terrorism” is an elusive term because it is not legally defined anywhere and does not fit clearly even within the definition of acts of terrorism as defined under international law. Some writers have argued that under international law there is no definition of terrorism.<sup>161</sup> It is submitted that acts of “terrorism” is defined under international law, the problem is with lack of general acceptability by most Nation-States and the facts that acts, as it relate to cyber terrorism does not fit within the definition. Ironically this is in spite of the fact that General Assembly of the United Nations as well as the Security Council has repeatedly condemned “all acts, methods and practices of terrorism wherever and by whoever committed”.<sup>162</sup> Even the new International Criminal Court will not have jurisdiction over terrorism because no consensus could be reached as to its definition. “Although there was considerable interest in also including terrorism and drugcrimes in the courts mandate, countries

---

<sup>160</sup> Section 20, Nigerian Computer Security and Protection Bill, 2005

<sup>161</sup> Jordan J. Paust, M. Cherif Bassioun, et al. (1996), *International Criminal Law. (Cases and Materials)*, Oxford University press, p.72

<sup>162</sup> U.N.G.A. Res. 51/210, Jan. 16, 1997, U.N.Doc. A/RES/51/210; Accord, U.N.G.A. Res. 49/60; 9, Dec. 1994, U.N. DOC. A/RES/49/60; U.N.G.A. Res. 50/53, 11, Dec. 1995, U.N. DOC. A/RES/50/53; U.N.G.A. Res. 46/51; 9, Dec. 1991, U.N. Doc A/46/ 654; U.N. Sec. Council Res. 1189, 13, Aug. 1998; U.N. DOC. S/RES/1189 Press Release GA/L/3103 (1998).

could not agree in Rome on a definition of terrorism”,<sup>163</sup> and so it was not included. No international efforts have yet been undertaken with the specific goal of controlling information terrorism.

Nevertheless, those proposals made in the bill to control computer crime generally would appear to provide an adequate starting point for addressing this closely related concern. For instance the attempt made in section 30(2)(a),(i)(ii)(iii) and (b) of the bill, to define what constitute terrorism is helpful to determine the act of terrorism at our domestic level.

In all cases, as provided for in section 38 of the bill, only the Federal High Court shall have jurisdiction to try offenders under this Act.

#### **(n) Cybercrime Draft Bill 2011**

There was another draft Cyber Security Bill 2011. The proposed bill Sponsored by Hon. Bassey Etim and had passed through the second reading stage at the lower parliamentary House of Representatives. It was expected that when it is passed to law it will eventually provide an effective, unified and comprehensive legal framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria and address international Cooperation. This however was not to be as the bill did not progress beyond this stage.

#### **(o) Cybercrime Draft Bill 2013**

The latest effort seems a significant improvement over the earlier efforts. The Bill titled, Cybercrime Bill 2013 proposed an Act to provide for the prohibition, prevention, detection response and prosecution of cybercrimes and for other related matters.

The objectives among others include providing an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and

---

<sup>163</sup> U.N. fact sheet, setting the Record straight: The International Criminal Court, Retrieved February 16, 2014 from [http://www.un.org/plweb/cgi/idoc.pl?45+unixt\\_free\\_user\\_+www.un.org.80+un+un+webnews+webnews++terrorism](http://www.un.org/plweb/cgi/idoc.pl?45+unixt_free_user_+www.un.org.80+un+un+webnews+webnews++terrorism).

punishment of cybercrimes in Nigeria. Part ii provides for protection of critical National Information Infrastructure and designate certain computer systems or networks as critical national information infrastructure. Section 6 criminalizes unlawful access to computer and propose a punishment ranging from two to three years in prison and a fine within the range of ₦5,000,000.00 to ₦7,000,000.00 or both.

Misuse of devices under the Act will attract a punishment of five years in prison or a fine not less than ₦10,000,000.00 or to both. Section 14 deals with child pornography and related offences and it provides for a relatively high punishment for offenders. The offence here is ten years in prison while the fine is ₦20,000,000.00 or both. Offence of Cyberterrorism under the Act attracts a life imprisonment.

In all, the Federal High Court located in any part of Nigeria regardless of the location where the offence is committed or High Court of Federal Capital Territory Shall have jurisdiction to try offences under this Act where such is committed in areas as provided for in Section 33 (1)(a)(b)(c)(d).

On the whole, this Bill seems to have taken into consideration all issues raised and the recommendations by the Council of Europe Convention on Cybercrime, commonly called “The Budapest Convention”.

**(p) National Cybersecurity Policy<sup>164</sup>**

This is one of the several efforts of the Federal Government of Nigeria to fight the menace of cybersecurity in the country. The mood of the country at this point is vividly captured by the forward to this document, written by the National Security Adviser<sup>165</sup> thus:

The emergence of cyberspace, a virtual global domain, is increasingly impacting almost every aspect of our lives. The

---

<sup>164</sup> This document came into being on 23<sup>rd</sup> December 2014 and is one of Federal Government’s efforts to tackle cyber crime.

<sup>165</sup> Dasuki M.S. (2014 December, 23) Forward to National Cybersecurity Policy. p.iii

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. It is transforming many countries' growth, dismantling barriers to commerce, and allowing people across the globe to communicate, collaborate and exchange ideas.<sup>166</sup>

He went further to say that: "However, behind this increasing dependence on cyberspace lies new risks that threaten the national economy and security. 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". This posture reveals that the Federal Government is not unmindful of the diversity of the implications of the nation's risk exposure in cyberspace, hence the decision to put in place cohesive measures towards addressing national risks effectively now and in the immediate future.

By this document, the government has shown that it recognized that for Nigeria and its citizens to continue to benefit from the full potential of information and communication technology revolution, we must take the cyber-risks seriously. This document is therefore a determination to confront the threats, uphold and support the openness of the cyberspace as well as balance security with respect to privacy and fundamental rights. "If we fail to prepare now and act appropriately, we may be faced with future challenges that will be more complex to manage"<sup>167</sup>

With this document, government has developed a common framework that aggregates our collective responses towards addressing the challenges. These are encapsulated in this National Cybersecurity Policy. It outlines the actions government and other players alike will take to lessen the risks and secure the gains of our continuous dependence on cyberspace. The

---

<sup>166</sup> Ibid

<sup>167</sup> Ibid

policy recognizes three key approaches to a successful national cybersecurity program, public private sector partnership, multi-stakeholders engagement, and international cooperation.

This policy is divided into eleven parts with three appendixes. Appendix one is the interpretation of the abbreviations while appendix two explains the definition of terms and appendix three list the members of interagency committee on national cybersecurity policy development. It is noteworthy that this document shall be due for a comprehensive review in another five years.

This policy in a nutshell, set out the strategic intent of the government in mitigating the country cybercrime risk exposure by prioritizing our needs while focusing on key areas, curtailing escalation of cyber threats that are inimical to the national security posture and the Nigeria economic wellbeing. This policy is a vital response element for safeguarding the nation. It helps to enlighten the citizens on the components that are to be used to empower the nation to understand, respond, and collectively deter cyber threat activities. The policy outlines the doctrinal framework and guiding principles for achieving our roadmaps through a coordinated effort of all stakeholders in the country.

**(q) General Overview of Cybercrime Act, 2015<sup>168</sup>**

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

---

<sup>168</sup> Cybercrime ( Prohibition Prevention Etc) Act, 2015

It is structured into 8 parts, 59 sections and a schedule as follows: Part 1 provides for the objective and application of the Act. Section 1(a) states that the objective is to provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. The provision in Section 1(b) shows that the intention of the Act is to ensure the protection of critical national information infrastructure while section 1(c) clearly declare that the Act will promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights. The application of the Act is provided for in section 2, and it states that the provision of the Act shall apply throughout the Federal Republic of Nigeria. Part 2, provides for protection of critical national information infrastructure and designate certain computer systems or networks as critical national information infrastructure and also provide for audit and inspection of critical national information infrastructure.

Offences and penalties are provided for in part 3. This part covers a wide range of offences which include unlawful access to computer, registration of cyber café, unlawful interception, computer related forgery, cyber terrorism, identity theft and impersonation, child pornography and related offences, breach of confidence by service providers and many more. This part also provides for the punishment for all the offences.

The duty of financial institutions is covered in part 4. In this part, section 37(1)(a) states thus:

(1) A financial institution shall :

- (a) Verify the identity of its customers carrying out electronic financial transactions by requiring the customers to present documents bearing their names, addresses and other relevant information - - -

(b) Apply the principle of know your customer in documentation of customers - - -

Except for the electronic specific, this section of the Act is impari-material with section 5(1)(2)(a)(b)(3)(4)(5)(6) and (7) of the money laundering Act, 2011.<sup>169</sup>

Part 5 which provides for administration and enforcement of the Act covers: coordination and enforcement, establishment of cybercrime advisory council, functions and powers of the council and establishment of national cyber security fund.

Arrest, search, seizure and prosecution is provided for in part 6 and it specifically mentioned, power of arrest, search and seizure, obstruction and refusal to release information, prosecution of offences, order of forfeiture of assets and order for payment of compensation or restitution.

In part 6, jurisdiction and international co-operation is provided for. Section 50(1) provides thus:

- (1) 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 - - -.

Under this part, the provision for international cooperation include: extradition, request for mutual assistance, evidence pursuant to a request, form of request from a foreign state, expedited preservation of computer data and designation of contact point.

Part 8 provides for regulations which highlighted the powers of the Attorney General of the Federation to make orders, guidelines or regulations as are necessary for the efficient implementation of the provisions of this Act.

**(r) Challenges of the Cybercrime Act, 2015**

---

<sup>169</sup> Section 5 (Identification of customers) Money Laundering Act, 2011. As amended. (Cap. M118, LFN.2004 )

It was a long process to the enactment of the cybercrime Act, 2015 and until the Act is reviewed, it will remain the legal instrument with which the Government at all levels will fight the menace of cybercrime and the only tool for the prosecutors to bring cybercriminals to justice. It is therefore important to review the strengths and weaknesses of the provisions. It is noted that a detailed analysis of this Act is beyond the scope of this work; however, efforts will briefly be made to address some sections of major concern below:

- 1) Section 5(1) A person who, with intent, commits any offence punishable under this Act against any critical national information infrastructure, designated under section 3 of this Act, is liable on conviction to imprisonment for a term of not more than 10 years without option of fine.
  - 2) Section 6(1) A person, who, without authorization, intentionally accesses, in the whole or in part, a computer system or network for fraudulent purposes and obtains data that are vital to national security, commits an offence and is liable on conviction to imprisonment for a term of not more than 5 years or to a fine of not more than ₦ 5,000,000.00 or both.
- 6(4), A person or organization who knowing it and intentionally traffics in any password or similar information through which a computer may be accessed without lawful authority, if such trafficking affects public, private or individual interest within or outside the Federation of Nigeria, commits an offence and is liable on conviction to a fine of not more than ₦ 7,000,000.00 or imprisonment for a term not more than three years or both.

- 3) Section 7(2) A person who perpetrates electronic or online fraud using a cybercafé, commits an offence and is liable on conviction to imprisonment for a term of 3 years or a fine of ₦1,000,000.00 or both.
- 4) Section 14(1) A person who, knowingly and without authority or in excess of authority, causes any loss of property to another by altering, erasing, inputting or suppressing any data held in any computer, whether or not for the purpose of conferring any economic benefits on himself or another person, commits an offence and is liable on conviction to imprisonment for a term of not less than 3 years or to a fine of not less than ₦ 7,000,000.00 or both.
- 5) Section 16(1) A person who, with intent and without lawful authority, directly or indirectly modifies or causes modification of any data held in any computer system or network, commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦7,000,000.00 or both.
- 6) Section 19 (3) Financial institutions shall, as a duty to their customers, put in place effective counter-fraud measures to safeguard their sensitive information, where a security breach occurs the proof of negligence lies on the customer to prove the financial institution in question could have done more to safeguard its information integrity.<sup>170</sup>

Looking first at the deficiencies of the Act, it should be pointed out that nearly all the provisions for offences requires proof of a specific intent, specifically the intent to commit an illegal transfer of funds or data, the intent to commit a forgery, the intent to hinder the function of computer and /or telecommunication system, and the intent to exploit commercially the

---

<sup>170</sup> Cybercrime ( Prohibition Prevention Etc) Act, 2015

program and put it on the market. The requirement to prove these specific intents significantly narrows the scope of each offence and also makes proving each offence more difficult. Suppose for instance an individual access a bank's computer and manipulates the records to make it appear that one account has been debited with ₦10,000.00 while another has been credited with ₦10,000.00. it may be argued, rightly, that such should be criminal in and of itself, under section 16(1) of the cybercrime Act, 2015 however, the prosecutor would have the additional burden of proving that manipulation of data was done for the specific intent of illegally transferring funds. If the defendant could successfully claim that he was a hacker who just wanted to see if he could actually manipulate bank data, such intent would be a defense to the charge.

Section 14(1) makes criminal mere access to a computer, if knowing and without authorization or in excess of authority. Thus, it appears that if the hacker capitalized on this provision, he could overcome the charge here. For instance, if he could raise a reasonable doubt that the hacking was not dishonest or harmful intention, then he is acquitted of the offence under this section as well.

It is noted that the rational used by many hackers who are caught is "I was just trying to highlight the deficiencies of the computer system". Arguably however, if such is enough to escape any criminal liability, it would seem to provide a fairly large loophole for computer criminals.

It is submitted that mere cyber trespass itself should be criminal. If a criminal was able to gain access to a store after hours of trying to break the locks and then fix the locks so that the night security guard would not suspect anything, only a few would disagree that the trespass itself was criminal and should be so characterized. This analogy should carry over into the cyber world.

Another significant shortfall of the cybercrime Act, 2015 is that it fails to address exceptions for law enforcement, military or intelligence activities. Section 14(1) criminalizes access to “any computer without authority”. This could mean the authority of the owner or person in charge of such computer. This makes it appear that law enforcement authorities accessing a computer under a valid authorized search warrant, but without the authorization of “the person responsible for the system” would be guilty of offence in section 14(1) if the criminal’s computer had any security measures which the police had to alter in order to overcome it.

The Act in providing for the punishments for the offences, section 5(1) for example provides thus: “- - - is liable on conviction to imprisonment for a term of not more than 10 years- - -”, the phrase “a term of not more than” used in this section as in many more sections of the Act means that the “term” can be less. That leaves the final decision to the discretion of the court. A corrupted judge could take the advantage of this loophole and mischievously hand down a one day sentence to a culprit and such pronouncement will still be within the ambient of the provision in this section.

It is submitted that the provisions in section 7(2)(3) of the cybercrime Act are “term certain” and that approach should extend to all sections of the cybercrime Act, 2015.

In the unreported case of *FRN v Dr. Bello Muhammad Shallah and another*,<sup>171</sup> section 19 of the ICPC Act under which the accused persons were charged provides thus “- - - and shall on conviction be liable to imprisonment for five (5) years without option of fine.”<sup>172</sup> The first accused person was found guilty under this Section and Honourable Justice N.U. Gummi of The High Court of Zamfara State in Gussau sentenced the first accused person to five years in prison

---

<sup>171</sup> Suit no. ZMS/GS/ZC/10

<sup>172</sup> Section 19, The Corrupt Practice and Other Related Offences (ICPC) Act, 2000.

under the provision of the ICPC Act, 2000.<sup>173</sup> It is noted that it was the wish of all the parties in this case, including the prosecution team which, with all modesty, was led by this research, that justice be tempered with mercy but the “term certain” of the provision in this Act prevailed over all sentiments.

Of a particular concern is the provision of section 19(3) as already reproduced above. This section does not seem to protect a customer of a financial institution enough. To the extent that where there is a case of fraud against a financial institution, this section provides an escape route for such financial institution to claim that they did everything possible to the best of their knowledge, and that will be sufficient to escape liability, even when they may not have done enough. The idea of passing the burden of proving what more the financial institution could have done to the customer is not fair. It is submitted that since the financial institution is in custody of the investments of the customer, and the customer is not privy to the security arrangements of the financial institution couple with the fact that it is the customer who has lost his investment in the fraud, the financial institution should be liable to adequately compensate the customer.

Interestingly, the cybercrime Act, 2015 is already facing what may be a litmus test with the first known case to be tried under the Act. In the recent case of *State v Oloketuyi*<sup>174</sup> A Federal High Court in Lagos ordered the remand of a blogger, Seun Oloketuyi, in prison over alleged malicious publication against the Managing Director and Chief Executive Officer of Fidelity Bank Plc, Nnamdi Okonkwo.

Oloketuyi, was ordered to be remanded in Ikoyi prison by Justice Mohammed Yunusa after he was arraigned on a two-count charge by the Special Fraud Unit (SFU) of the Nigerian

---

<sup>173</sup> Ibid

<sup>174</sup> FHC/L/346C/15

Police. The accused had published a news report on his blog where he alleged that Okonkwo had a love relationship with a married lady in the marketing department of the bank.

In the report, Oloketuyi had further alleged that the extra-marital affair between Okonkwo and the said lady simply identified as Justina, resulted in the birth of a baby, and that the affair also destroyed the marriage of the said Justina. He further alleged that Okonkwo had since sent the affected lady abroad to further her studies. Okonkwo had petitioned the police, and after investigation, Oloketuyi was charged to court.

According to the charge with reference number FHC/L/346C/15, Oloketuyi in count one was accused of intentionally sending message and other matters by means of computer system or network against Okonkwo, which he knew to be false, for the purpose of causing him annoyance, insult and ill-will.

The offence was said to be contrary to and punishable under Section 24 (1) (b) of the Cybercrime (Prohibition Prevention Etc) Act, 2015.

In count two, Oloketuyi was accused of knowingly publishing defamatory matters on Okonkwo, which he knew to be false, contrary to and punishable under Section 375 of the Criminal Code Act.<sup>175</sup>

The report was published sometime in June 2015 via Oloketuyi's blog, [www.naijahottestgist.com](http://www.naijahottestgist.com).

It is instructive to note that a team of nine lawyers lead by Muize Banire<sup>176</sup> has taken this matter up "pro bono" in defence of the accused person. They argued that there was no element of crime in the charge filed by the police against the blogger, saying what anyone who felt maligned with his publication should have done, was to sue for libel.

---

<sup>175</sup> Criminal Code Act, Cap C38, LFN 2004

<sup>176</sup> Muize Banire, is a former Attorney General and commissioner for Justice in Lagos State.

This research aligns itself with this position to the extent that libel is a civil matter and it is the person who felt offended that is expected to sue, therefore, the State has no business with civil matters. The opinion of the Court is still being awaited in this case but this is obviously one of the many challenges that this Act will have to contend with, and no doubt, an early test case to prove the efficacy of the cybercrime Act, 2015.

Cumulatively, the national efforts and those of the international organizations have reinforced each other, achieving a nearly global attention to the problem of cybercrime and terrorism and promoting international harmonization of legal approaches.<sup>177</sup> National efforts to fight cybercrime tend to be a different levels sophistication and priority, but such efforts are present in at least 40 major countries. Many of them are developing specialized police capabilities through equipment training and laws. International and supranational organizations have significantly contributed to the harmonization of criminal laws as well as of underlying civil law in all of the areas of computer related criminal law reform.

The European Community's power to adopt binding directives opened a new age of legal harmonization in Europe.<sup>178</sup>

However, a major problem in writing, enforcing, prosecuting, and interpreting cybercrime laws, is the lack of technical knowledge on the part of legislators and experts charged with these duties. Legislators, in most cases, don't have a real understanding of the technical issues and what is or not desirable or even possible to legislate. Police investigators are becoming more technically savvy, but in many small jurisdictions, no one in the department knows how to recover critical digital evidence.<sup>179</sup>

---

<sup>177</sup> Goodman M. D. and S. Brenner, (2000) The Engineering Consensus on Criminal Conduct in Cyber Space. Oxford International Journal of Law and Information Technology.(10):173.

<sup>178</sup> Ibid

<sup>179</sup> Shinder, D. (2008) Scene of The Cybercrime. Elsevier Ltd; 2<sup>nd</sup> Edition.p. 35.

Judges, too, often have a lack of technical expertise. That makes it difficult for them to do what courts do, that is, interpret the laws. The fact that many computer crime laws use vague language aggravates the problem. The answer to all these dilemmas is the same, and they are; education and awareness programs. These programs must be aimed at everyone involved in the fight against cybercrime, including:<sup>180</sup> Legislators and other politicians, Criminal Justice professionals, IT professionals, the community at large and especially the cyberspace community in particular.

---

<sup>180</sup>*Ibid.* Pp. 35,36

## CHAPTER FOUR

### THE ROLE OF LAW ENFORCEMENT AGENCIES IN COMBATING CYBER INSECURITY AND CRIME

#### 4.1 Introduction

The term ‘law enforcement officials’ includes all officers of the law, whether appointed or elected, who exercise police powers, especially the powers of arrest and detention. “This should be given the widest possible interpretation, and includes military and other security personnel as well as immigration officials where they exercise such powers.”<sup>1</sup> The cross-national nature of most computer related crimes have rendered many time-honoured methods of policing both domestically and in cross-border situations ineffective even in advanced nations, while the ‘digital divide’ provides ‘safe havens’ for cyber-criminals.<sup>2</sup>

Law enforcement agencies in many jurisdictions have been unable to respond effectively to cybercrime and even in the most advanced nations, ‘play catch-up’ with cyber savvy criminals.<sup>3</sup> Law enforcement broadly refers to any system by which some members of society act in an organized manner to promote adherence to the law by discovering and punishing persons who violate the rules and norms governing that society. Although the term may encompass entities such as courts and prisons, it is most frequently applied to those who directly engage in patrols or surveillance to dissuade and discover criminal activity, and those who investigate crimes and apprehend offenders.<sup>4</sup> Although law enforcement may be most concerned with the prevention and punishment of crimes, organizations exist to discourage a wide variety of non-

---

<sup>1</sup> Amnesty International, (2009) “International Police Standards” Geneva Centre for the Democratic Control of Armed Forces (DCAF) Amnesty International publication United Kingdom, p.9

<sup>2</sup> Roderic B, Developments in the Global Law Enforcement of Cyber-Crime, Policing: An International Journal of Police Strategies and Management, Queensland University of Technology [Revision 7.1.06 – 13256 words] 29(2) : Pp. 408-433.

<sup>3</sup> Sussmann, M.A. 1999, ‘The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium’, (1999) *Duke J. of Comp. & Int'l L.*, 9: at p.451

<sup>4</sup> Kären M., Christine O, *Introduction to Law Enforcement and Criminal Justice* (2008), p.1. Retrieved July 7, 2012 from : ([http://biosecuritycommons.org/index.php?title=Law\\_enforcement](http://biosecuritycommons.org/index.php?title=Law_enforcement)) .

criminal violations of rules and norms, affected through the imposition of less severe consequences.

Most law enforcement is conducted by some type of law enforcement agency, with the most typical agency fulfilling this role being the police. Societal investment in law enforcement through such organizations can be massive, both in terms of the resources invested in the activity, and in the number of people professionally engaged to perform those functions.<sup>5</sup>

The Nigeria cybercrime Act is very recent having being promulgated only in May, 2015 and there is no sufficient history of the Nigerian police performance in this area. Except for the case of *State v Oleketuyi*<sup>6</sup> which is still at trial stage. This is not to say that law enforcement agency did not have a performance record in area of cybersecurity and crime before the promulgation of the cybercrime Act,2015, in fact, the Economic and Financial Crime Commission (EFCC) was able to secure a number of sentences although from an overstretch of the existing Acts that are not cybercrime specifics. In the light of the above, this topic is treated from two angles, first, from the practice of law enforcement as obtainable in United Kingdom and second, in accordance with the provisions of the United Nation's code of conduct for Law Enforcement Officials as well as other basic international human rights standards applicable to law enforcement officials.

#### **4.2 Nature of Traditional Law Enforcement Functions**

Every society needs a police force as part of its institutional mechanisms to ensure the maintenance of law and order and for the good of the public. "The systems of policing worldwide are not stereotyped neither do all countries have an identical police practice. Rather,

---

<sup>5</sup>Ibid

<sup>6</sup> FHC/L/346C/15

the police institution in one country presents a pattern peculiar to its circumstances depending on its size, population, economic and political development.”<sup>7</sup>

For the fact of the variety nature of crime, police operation must be diverse and flexible. Police must be able to react to situations that range from threat of explosives to fleeing suspect. During these operations officers need tools and training to be as effective and as safe as possible.

The Federal government has the responsibility to provide the law enforcement response to cyber crime, through the provision of adequate police and other units to tackle the problem and ensure that the perpetrators of these crimes are brought to justice. The government has created a number of specialist units to help tackle cyber crime and protect the public. It is believed that the creation of specialist units, such as Economic and Financial Crimes Commission (E.F.C.C.) is the right approach, as it allows for the development of expertise in highly complex areas. This approach allows a flexibility of response, and an ability to understand the key drivers and criminal behaviours as well as the characteristics of victims who may be vulnerable to the crimes. As there are many types of crime committed on the Internet, so across Government a number of specialist responses have grown up to meet them.

In another hand, law enforcement is strongly linked to local culture, ethic, politic, law, as to say to specific national environments, which means that in an interconnected global information society, law enforcement should answer the challenge to be locally significant and efficient for a particular national context and interoperable and compatible at the international level.

To this end, this work shall discuss this topic with reference to the nature of law enforcement in United Kingdom, not because the law in U.K. is applicable in Nigeria, but

---

<sup>7</sup>Jenibewon D.M. (2001) *The Nigeria Police in Transition: Issues: Problems and Prospects*, Spectrum Books Limited, Abuja, p.150.

because the U.K. is a more technologically advanced country than Nigeria, and her experience can serve as a point of lesson for Nigeria.

In order to achieve a reasonable level of law enforcement, the United Kingdom's Home Office supports the safety of the citizen through the provision of law enforcement units to tackle online crime. The National Fraud Authority, an executive agency of the Attorney General's office, has launched Action Fraud, while the Department of Health supports the work to tackle the sale of counterfeit drugs online, through the Medicines and Healthcare products Regulatory Agency.<sup>8</sup>

The Department for Business, Innovation & Skills is responsible for intellectual property policy and the Department for Culture, Media and Sport lead an online copyright protection in relation to the 2012 Olympics.

Her Majesty's Revenue and Customs (HMRC) has a bespoke investigation capability to address fiscal fraud, including online attacks made against their tax regimes. HMRC are members of the Association of Chief Police Officers (ACPO) e-crime group and support the work of the Police Central e-crime Unit of Metropolitan Police Service (PCeU).

The 2009 Consumer White Paper also announced the creation of an internet enforcement team to tackle e-crimes against consumers. This is being set up across the U.K. through Trading Standards and Regional Scam buster teams. They will also work closely with the PeCU and their Scottish equivalent. Developing this, the Office of Fair Trading (OFT) planned to put together a national e-consumer protection strategy by the end of 2010, to enable all relevant agencies in the consumer protection landscape to work together even more effectively, ensuring lack of

---

<sup>8</sup> National Security Strategy. Retrieved June 22, 2012 from [http://www.cabinetoffice.gov.uk/reports/national\\_security.aspx](http://www.cabinetoffice.gov.uk/reports/national_security.aspx).

duplication and better coordination of e-protection activities, including intelligence gathering, e-enforcement and other consumer protection tools.<sup>9</sup>

The UK needs to have a law enforcement response that is capable of dealing with these issues, and has access to the right level of tools and support. The Home Office has recognised this, and has created the Police Central e-crime Unit (PCeU) to lead the police response within the UK, and the e-crime unit of the Serious Organised Crime Agency (SOCA) to work internationally. The ACPO e-crime strategy, published in 2009 and set out the work of the PCeU in delivering an operational response to the most serious of e-crime incidents, the engagement with industry through the virtual task force and the establishment of the ACPO committee which consists of 9 strands of activity focused on improving law enforcements response to cyber crime.<sup>10</sup>

Law enforcement resources in this highly technical area are limited, and to address this, the PCeU are progressing opportunities to brigade resources, intelligence and expertise by promoting the need for forces to establish regional capability. The Home Office fully supports this work, and recognises the efforts made by the Police Service and SOCA to tackle cyber crime. Other Departments, such as HMRC, also have specialist units dealing with fraud in their particular areas.<sup>11</sup>

One important nature of law enforcement is technical development for law enforcement. Cyber crime is committed using communications between networked devices, with those communications conveyed in various applications such as e-mail or malware. The ability to trace offenders and victims, and to investigate and gather evidence of cyber crimes can depend on the

---

<sup>9</sup> Cyber Security Strategy. Retrieved June 22, 2012 from [http://www.cabinetoffice.gov.uk/reports/cyber\\_security.aspx](http://www.cabinetoffice.gov.uk/reports/cyber_security.aspx).

<sup>10</sup> Digital Britain Report. Retrieved June 22, 2012 from <http://www.culture.gov.uk/images/publications/digitalbritain-finalreport-jun09.pdf>.

<sup>11</sup> Extending our Reach. Retrieved June 22, 2012 from <http://www.homeoffice.gov.uk/documents/extending-our-reach/index.html>.

ability to recover and analyse network data and, once an offence has been detected and reported, the ability to research and analyse historic data.

In a changing and increasingly complex communications environment investigators need to be able to continue to investigate communications data, and to be able to acquire and analyse complex network traffic data.<sup>12</sup> The Home Office Communications Capabilities Directorate is leading a cross-government programme of work to ensure that investigators can continue to be able to investigate communications data to protect the public, investigate online crimes and prosecute offenders.<sup>13</sup>

The Directorate is working closely with the UK's law enforcement and security and intelligence agencies and with communications service providers to put in place and maintain arrangements permitted by law for the retention, retrieval and disclosure of communications data. Within the Directorate, the Interception Modernisation Programme is considering the implications for cyber crime detection of the increasing distinction between traditional networked services and newer application layer services.<sup>14</sup>

Next in line of importance in the nature of law enforcement is Prosecution.

Following the detection and investigation of cyber crimes it is important that offences are effectively prosecuted, that those involved in dealing with these cases receive appropriate training, and that the criminal justice system has knowledge of the complexities which hi-tech crime cases can present and sufficient expertise to deal with them. It is also important that, as "Extending the Reach" of law enforcement is made clearer, the prosecuting authorities use all

---

<sup>12</sup> Association of Chief Police Officers (ACPO) e-crime strategy. Retrieved June 22, 2012 from <http://www.acpo.police.uk/asp/policies/data/Ecrime%20Strategy%20Website%20Version.pdf>.

<sup>13</sup> UK Council for Child Internet Safety (UKCCIS) Strategy. Retrieved June 22, 2012 from <http://www.dcsf.gov.uk/ukccis/>.

<sup>14</sup> House of Lords Science & Technology Committee Report into Personal Internet Security. Retrieved June 22, 2012 from <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf>.

available tools to recover any assets and to limit the future activities of those responsible for the crimes.<sup>15</sup>

In cases where there is a significant involvement of computers in the facilitation of an offence, it will usually be dealt with by a prosecutor who has undergone specialist training in this area and has experience of handling such cases. The Crown Prosecution Service (CPS) has now trained 120 high-tech crime specialist prosecutors across the regions, and over 45 cyber crime specialist caseworkers. Within the CPS further forms of continuous on the job training and development exist through a cyber crime bulletin board whereby prosecutors are informed of developments in cases with a hi-tech element by dissemination of case summaries.<sup>16</sup>

Furthermore, it is the objective of law enforcement to protect consumer.

The Government has therefore asked the Office of Fair Trading (OFT) to develop a longer term national strategy for consumer protection on the Internet. The e-Consumer Protection Strategy will consider how relevant agencies can work together even more effectively, ensuring lack of duplication and better coordination of e-protection activities. The OFT is expected to publish a public consultation document in spring 2010, where it will lay out the key challenges and options to address them. A completed e-Consumer Protection Strategy is expected to be published by the end of 2010.<sup>17</sup>

The key aim of cyber crime prevention is to ensure that information and education is made available to the public and businesses to help them keep themselves safe. As with the work to directly tackle crimes through law enforcement activity, there is a need to be able to provide safety information that is specific to a particular area or group, but also general messages that

---

<sup>15</sup> Council of Europe Cybercrime Convention. Retrieved June 22, 2012 from <http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm>.

<sup>16</sup> Contest Strategy. Retrieved June 22, 2012 from <http://security.homeoffice.gov.uk/news-publications/publication-search/contest/contest-strategy/contest-strategy2009.html>.

<sup>17</sup> Findings from consumer surveys on Internet Shopping. Retrieved June 22, 2012 from [http://www.oft.gov.uk/shared\\_ofi/reports/Evaluate](http://www.oft.gov.uk/shared_ofi/reports/Evaluate).

apply to safety as a whole. This includes working with Internet service providers to develop an internet culture that stamps out unacceptable behaviour online, such as abuse, stalking and harassment.

The United Kingdom's Home Office has taken the lead in bringing together different groups to provide education and develop a preventative response, which can include the relevant industry for a particular area, charities and the third sector, as well as civil society.

Law enforcement also provides for financial and technical safety information, thereby revealing that the best way to stop cyber crime is to prevent it happening in the first place, and as part of that the public and business needs to be provided with accurate, relevant information on how to keep themselves safe online and to secure their devices and data. The Government is strongly supportive of growing the use of the internet, and recognises the need to provide adequate and accurate information on the risks to consumers should they decide to use Internet services. The primary purpose of any of the safety information is to ensure that the public and business has accurate information to help them protect themselves.

This applies whether the issues are relating to fraud, to protecting children, or to using standard services on the Internet.<sup>18</sup> Individuals can protect themselves by controlling the amount of personal data they make available on the internet. However, the use of privacy enhancing technology in systems can also enhance an individual's privacy, help reduce the risks of privacy breaches and the significant costs associated with them and build trust between customers and clients. A number of Government departments provide safety information relating to the Internet, as part of the provision of their services, and many of these are particular to the problems faced by those departments.<sup>19</sup>

---

<sup>18</sup>Contest Strategy.Op.cit,p.193

<sup>19</sup> Ibid at p.27

Finally the position of the Global Prosecutors E-crime Network (GPEN) in law enforcement is also noteworthy. The United Kingdom's Crown Prosecution Service (CPS) and the International Association of Prosecutors (IAP) have established a global network of specialists called the Global Prosecutors E-Crime Network (GPEN). GPEN not only encourages and enhanced international cooperation in the e-crime arena; but it enables all jurisdictions to develop a co-ordinated approach for dealing with e-crime that supports effective prosecutions and promotes the principles of the Council of Europe Cybercrime Convention.<sup>20</sup>

### **4.3 Prevention and Detection of Crime**

All over the world one of the challenges hampering effective administration of criminal justice is the detection and investigation of crime and criminals. This problem is more pronounced in the developing counties like Nigeria where technological advancement is still at the lowest ebb. Criminals are becoming sophisticated leaving almost no trace or clue after the commission of crime.

The sanctions imposed by the criminal law are carried out by the law enforcement agencies. In Nigeria, the main body that does this is the police apart from other government agencies. The police department is the first body that any offender comes into contact with. The primary role of the police is to keep peace and enforce criminal rules in the state on the basis of the specific jurisdiction and mission. Thus, the power to detects and investigates crime is statutorily vested in the Nigeria police.<sup>21</sup> Although, there are other governmental agencies saddled with the responsibility of crime detection and investigation in specific cases such as the Economics and Financial Crimes Commission<sup>22</sup>, State Security Services, Independent Corrupt

---

<sup>20</sup> Ibid at, 32.

<sup>21</sup>Section 4 of the Police Act, Cap. P19, Laws of the Federation of Nigeria, 2004

<sup>22</sup> Economics and Financial Crime Commission Act, 2004

Practices Commission<sup>23</sup> and the likes, none of them is confer with such enormous and wide power as the Nigeria police. Therefore, the emphasis here is the police.

The Nigeria police Force is established by Section 214(1) of the 1999 Constitution of the Federal Republic of Nigeria (as amended) and under section 3 of the Police Act.<sup>24</sup> Section 4 of the police Act defines the duties of the Police to include the prevention and detection of crime. It provides:

The police shall be employed for the prevention and detection of crime, the apprehension of offenders, the preservation of law and order, the protection of life and property and due enforcement of all laws and regulations with which they are directly charged and shall perform such military duties within or outside Nigeria as may be required of them by, or under the authority of this or any other Act.

The first role of the Police is to prevent the commission of crime. Prevention they say is better than cure. It is the first responsibility of the Police to detect that a crime is about to be committed and quickly nipped it on the bud before the act is actually carried out. This power is derived from Section 4 of the Police Act. Also, Section 52 of the Administration of Criminal Justice Law of Lagos State and Section 53 of Criminal Procedure Law of Ogun State provides:

- (1) Every Police Officer may intervene for the purpose of preventing, and shall to the best of his ability prevent, the commission of any offence.
- (2) A Police Officer may of his own authority intervene to prevent any damage attempted to be committed in his view to any property, movable, or the removal of or damage to any landmark or buoy or other mark used for navigation.

Under section 54 of the Administration of Criminal Justice Law of Lagos State and section 55 of same Law in Ogun State, a Police Officer Knowing of a design to commit any offence may arrest, without an Order from a magistrate and without a warrant, the person so

---

<sup>23</sup>Independent Corrupt Practices Commission Act, 2000

<sup>24</sup> Cap.P19, Laws of The Federation of Nigeria, 2004

designing, if it appears to such officer that the commission of the offence cannot otherwise be prevented.

Prevention of crime if holistically pursued is the most effective method of administering criminal justice all over the world. This is because since it makes it possible for a suspect to be arrested before he carries out his criminal acts, injury to members of the society is avoided. It also reduces the cost and time spent on investigation, detention, prosecution and imprisonment of criminals.

However, prevention of crime before they are committed involves a lot of information gathering which has to do with intelligent work. The security havocs and the security embarrassment which terrorist groups and militants have inflicted on Nigeria in recent time would have been avoided or reduced if our intelligent networks are effective in Nigeria. These same lapses are carried over to the prevalent of cybercrime in Nigeria. There is therefore an urgent need to overhaul the intelligent units of our security agencies for effective information gathering.

The role of the members of the public in providing information to the security agents cannot be overemphasized. The security agents are not angels. They need information from members of the public. One of the identified reasons why most Nigerian are always reluctant in supplying information about criminals to the security agents in Nigeria is lack of trust. It is generally believed that security agents in Nigeria cannot be trusted with information as you may either become the criminal or the information is leaked to the criminals and the informant subsequently becomes the target of the criminal and exposed to great danger of vulnerability.

Prevention and detection of crime are among the area of immediate interest to law enforcement agencies around the world. The responsibility for the prevention and detection of

crime is assigned primarily to law enforcement agencies. The full discharge of that responsibility however, requires more than law enforcement impute alone. The effective prevention and detection of crime are critically dependent upon the existing level and quality of cooperation between a law enforcement agency and the community it serves, and are as much a private responsibility as a public one. “Politicians, members of the judiciary, community groups, public and private business corporations and individual need to join forces if the result of efforts towards prevention and detection of crime are to be better than the inevitably unsatisfactory results of merely attempting to enforce criminal laws.”<sup>25</sup>

This subject matter is lucidly expressed in the Law Enforcement Training Manual of The International Committee of the Red Cross. “However, it cautions that its information should not be interpreted as providing practical guidance on how to conduct investigations or how to gather evidence, it should rather be regarded as a mere attempt to put law enforcement practice in the correct legal framework of international standards.”<sup>26</sup>

This work borrowed a leave from the ICRC and shall follow its approach at this juncture: First is Evidence gathering. Gathering of evidence is an integral and an important aspect of detection. The effective detection of crime hinges completely on the successful gathering of evidence in relation to a particular crime committed. Two kinds of evidence are important in this aspect:

- a) Material evidence ( silent witnesses) and
- b) Statements by witnesses.

Material evidence can in principle be found where a crime has been committed, or where it has left traces. It is therefore important that the scene of a crime be located, as well as all sites

---

<sup>25</sup> International Committee of Red Cross (ICRC) Geneva,(1998) To Serve and To Protect: Human Rights and Humanitarian Law for Police and Security Forces, law enforcement training manual. Pp.171-172

<sup>26</sup> Ibid at p.178

where material related to the crime have subsequently been left behind. In the case of a murder this would mean finding the actual site of the killing (if it did not occur at the place where the victim's body was found), working out the route taken by the killer to get to and away from that particular site or (those site) and trying to identify the places where the killer might have disposed of materials related to the crime.

The International Covenant on Civil and Political Rights (ICCPR) states “no one shall be subjected to arbitrary interference with privacy, family, home or correspondence”<sup>27</sup>. Where a crime has left traces in public places, this provision does not constitute a problem to law enforcement practice. However, if such traces have been left behind in a private home, or if indeed the crime occurred inside it, then the mere fact of the crime having been committed is not usually considered a sufficient basis for law enforcement officials to enter a private dwelling. In such a situation law enforcement will generally require a court order allowing the access to that home, if need be against the will of the inhabitants, for the purpose of gathering evidence. This procedure, established in most countries, seeks to protect individuals against unlawful and or arbitrary invasions of their most private sphere. The actual securing, collection and treatment of material evidence is work for police specialists. Subsequent analysis, in certain cases, is even left to forensic laboratories. The requirements for material evidence to be accepted as irrefutable proof in a court of law are extremely high and rigid. Such standards represent recognition of the importance of a fair trial, to which all accused persons are entitled.

The second type of evidence is information obtained from the statements of witnesses. Witnesses are important to the investigation process because they can be compelled to testify, and when testifying they are obliged to tell the truth. “The situation of witnesses is in direct

---

<sup>27</sup>The International Covenant on Civil and Political Rights (ICCPR) Article 17,

contrast to suspected and accused persons, who cannot be compelled to testify against themselves or to confess guilt”.<sup>28</sup>

However, in order to obtain a useful statement from a witness, the law enforcement official(s) conducting the interview must focus on “the reason for knowing” of each witness. What did the witness see, hear or smell of the actual events, what is direct observation, what is hearsay? The statements of witnesses will help establish factual evidence against known or unknown perpetrators of crime. Although the rules for the interrogation of suspect or accused persons do not apply to witnesses. Certain countries advise their law enforcement agencies nevertheless to observe those same rules as regards the recording of time, duration, intervals, etc. This is done to avoid subsequent criticism in a court of law that, for instance, the testimony of a witness should be deemed unreliable owing to extreme fatigue induced by the frequency and duration of interviews.

Under this heading a few words need to be said about the common practice in law enforcement of using confidential informants for the prevention and detection of crime, and the practice of infiltration for the same purpose. For both practices, the basic premise is that they may be used only when to do so is legal and necessary for lawful law enforcement purposes.

As the use of confidential informants often entails the payment of moneys for information given, the attention of law enforcement officials must be drawn to the potential risks of such practices, including the risk that:

- a) The informant, attracted by the prospect of payment, may incite others to commit crimes, of which he/she subsequently informs his law enforcement contact:

---

<sup>28</sup> Ibid at, Article 14.3(g).

- b) The informant may be induced, by his/her law enforcement contact, to instigate crimes committed by others that subsequently enable the law enforcement agency to make an arrest:
- c) The money involved in the dealings with informants has a corrupting influence on law enforcement officials involved.<sup>29</sup>

The term “infiltration” refers to the practice whereby either a law enforcement official or a confidential informant is brought into a criminal organization for the purpose of gathering information that cannot be obtained otherwise. This practice must be lawful and absolutely necessary for lawful law enforcement purposes. Even if those conditions are met, a number of risks will still remain. First of all, infiltration can be highly dangerous for the person carrying it out. Secondly, as protection of the identity of this person will be an objective throughout all stages of the criminal proceedings, there is the risk of conflict with the principle of fair trial, and particularly the provision stating that the suspect or accused has the right to cross-examination of witnesses brought against him or her.<sup>30</sup> In situations where for security reasons the identity of the infiltrator(s) is not revealed, this right can be in serious jeopardy.

It is clear that both practices must be closely supervised by a competent member of judiciary and, in order to safeguard the right to a fair trial that their application must be made dependent on permission obtained prior to their implementation.

Second is interrogation. Statements by suspects or accused person with regard to a crime that has been committed are a third important source of evidence. It should be emphasized, however, that in investigation process law enforcement officials should not overly rely on such statements as a basis for a certain case to be presented in court. The reasons for this are simple. A

---

<sup>29</sup> International Committee of Red Cross (ICRC) Op.cit, p.198, at p.180

<sup>30</sup>The International Covenant on Civil and Political Rights (ICCPR) Article 14.3 (e)

suspect has the right to remain silent, and cannot be compelled to testify against himself (or herself) or to confess guilt. Furthermore, a suspect is entitled to withdraw or alter statements made during any stage of the proceedings. It is evident that in many situations, material evidence and witness statements will be more valuable than information obtained through interrogation of a suspect.

In relation to the interrogation of suspects and accused person the absolute prohibition of torture forbidden by law, the results (confessions or information) obtained through torture will always be unreliable, because at no stage can it be determined beyond doubt whether a tortured person speaks the truth or merely confesses in order to stop the torture. Torture is degrading both for the victim and the perpetrator. It undermines the basic principle of liberty, security and democracy upon which our societies are supposed to be built. “Torture can never be justified under any circumstances.”<sup>31</sup> Suspected and accused persons have a right to be presumed innocent until proven guilty in a court of law. Therefore interrogating law enforcement officials do not establish innocence or guilt through their questioning, their task is to establish facts.

Their fact finding mission starts with an investigation of the scene of the crime, as well as the sites where that crime has left traces, for the purpose of gathering material evidence in relation to the crime committed. Their subsequent attention is focused on those persons who may have witnessed the crime as it was being committed or who may have other relevant information. Only this dual investigative approach and an analysis of the information obtained thereby might enable them, by assembling sufficient facts, to establish a reasonable suspicion against an individual as having committed this crime (if a suspect or suspects was or were not arrested in the act).

---

<sup>31</sup>International Committee of Red Cross (ICRC)Op.cit, p, 198, at p.181

The arrest of a suspect is again surrounded by procedural safeguards as is their subsequent detention and interrogation. The subject “arrest and detention” is discussed in details under sub head “4.4” below.

The questioning of suspect requires preparation on the part of the law enforcement officials involved. These officials must have a clear picture of the facts that have been established so far, which help to determine the order of events as they happened. The purpose of an interrogation is clarification of facts already established as well as the establishment of new facts in relation to the crime committed.

Every interview must be clearly recorded. Statements by the suspect that contain a confession of guilt should be taken down as far as possible in his or her words. The duration of the interview and the people present at it, as well as the length of time between two interviews, must also be clearly recorded. It has already been established that torture or pressure on the suspect to compel him or her to testify can result in a false confession, given by the suspect in order to prevent further torture or pressure. It should be noted however, that the phenomenon of false confess is not limited to situations where people have been subjected to torture or ill treatment.

Law enforcement agencies around the world are familiar with individuals confessing to crimes they did not commit, often for complex personal and psychological reasons. “Most agencies have chosen a tactic of not disclosing certain facts (only known to the “true perpetrator”) of a crime committed, in order to enable such false confessions to be swiftly dismissed”.<sup>32</sup>

The third is disappearances and extrajudicial killings. There are two types of violations which, because of their gravity and their rejection of fundamental principles of democracy and

---

<sup>32</sup> Ibid at p.182

the rule of law, merit particular mention in this discourse on the prevention and detection of crime. The seriousness of these human rights violations is made more acute by the fact that they are committed by State officials.

For clarity of purpose it is instructive to distinguish what a “disappearance” is and what an “Extrajudicial execution” is. “The “disappeared” are people who have been taken into custody by agents of the state, yet whose whereabouts and fate are concealed, and whose custody is denied.”<sup>33</sup>

“Extrajudicial executions are unlawful and deliberate killings, carried out by order of a government or with its complicity or acquiescence”.<sup>34</sup>

In the first definition the quotation marks have been used to make it clear that the persons concerned have not really vanished. The victims’ whereabouts and fate, concealed from the outside world, are known by those responsible for their disappearance.

Unlawful and arbitrary deprivation of liberty and the deliberate and unlawful taking of life are the most serious crimes that can be committed by those who are in fact called upon to protect and promote the human rights of all persons. The very foundation of a democratic society is swept away whenever and wherever the State is responsible for the denial of such fundamental rights to its citizens.

Every effort must therefore be made towards the effective prevention of such great violation of human rights. “The recruitment, training and supervision of law enforcement officials must offer operational guarantee for an adequate lawful and non arbitrary task performance.”<sup>35</sup>

---

<sup>33</sup> Amnesty International 14-point Programme for the Prevention of “Disappearances”

<sup>34</sup> Amnesty International 14-point programme for prevention of Extrajudicial Executions

<sup>35</sup> International Committee of Red Cross (ICRC) Op.cit, p.198, at, 183

Only the complete transparency of law enforcement agencies and their further evolution to open system type organizations will help to establish the levels of true accountability which are necessary for the effective prevention of such acts.

At the same time the seriousness of such crimes must be understood by law enforcement agencies as well as by state governments, resulting in the prompt, thorough and impartial investigation of any allegation of such a crime having been or being committed. “Any such investigation must ensure that due attention is given to any victims and that the results of the investigation are made public. The official responsible must be brought to justice”.<sup>36</sup>

#### **4.4 Powers of Law Enforcement in the Prevention and Control of Crime**

The mechanisms established by States to protect people’s rights, establish and maintain order and guarantee stability and security are usually referred to collectively as the security sector.

It is generally agreed that the security sector includes “core security actors (e.g. armed forces, police, gendarmerie, border guards, customs and immigration, and intelligence and security services); security management and oversight bodies (e.g. ministries of defence and internal affairs, financial management bodies and public complaints commissions); justice and law enforcement institutions (e.g. the judiciary, prisons, prosecution services, traditional justice systems), and non statutory security forces (e.g. private security companies, guerrilla armies and private militia).<sup>37</sup>

“An important actor in the security sector is the police, whose functions, as a minimum, are:”<sup>38</sup>

---

<sup>36</sup> Ibid

<sup>37</sup>(Organisation for Economic Co-operation and Development, *OECD DAC Handbook on Security System Reform: Supporting Security and Justice* (Paris, 2007), p. 5). Retrieved December 12, 2014 from [www.oecd.org/dataoecd/43/25/38406485.pdf](http://www.oecd.org/dataoecd/43/25/38406485.pdf). A similar definition is given in the report of the Secretary-General on securing peace and development: the role of the United Nations in supporting security sector reform (A/62/659-S/2008/39).

<sup>38</sup>Council of Europe, Recommendation Rec (2001)10 of the Committee of Ministers to member States on the European Code of Police Ethics, adopted by the Committee of Ministers on 19 September 2001, see also: Cees de Rover, *To Serve and to Protect: Human Rights and Humanitarian Law for Police and Security Forces* (Geneva, International Committee of the Red Cross, 1998),p.146, Ralph C, Barry D and Tom W (1998) *Human Rights and Policing: Standards for Good Behaviour and a Strategy*

- a) Prevention and detection of crime
- b) Maintenance of public order
- c) Provision of assistance to the public

“In order to carry out these functions, the police have certain powers, namely the power to arrest and detain and the power to use force. It is precisely this monopoly on the use of force”<sup>39</sup> and the power to arrest and detain that place the police in a unique and sensitive position within the democratic State, so that adequate control mechanisms are required to ensure that these powers are consistently used in the public interest. Like any other public service, the police must operate with impartiality.

The notion that the State and all its institutions are to serve the public interest is reflected in the International Code of Conduct for Public Officials which states: “A public office, as defined by national law, is a position of trust, implying a duty to act in the public interest. Therefore, the ultimate loyalty of public officials shall be to the public interests of their country as expressed through the democratic institutions of government.”<sup>40</sup> The International code of conduct for public officials is recommended to member states “as a tool to guide their efforts against corruption”.<sup>41</sup>

The description of the police as the strong arm of the State reflects their authorization to enforce laws and policies defined by State institutions. In some countries, this leads to State representatives trying to influence the police to serve their interests rather than the public interest

---

*for Change* (The Hague, Kluwer Law International), The European Code of Police Ethics is available on <https://wcd.coe.int/wcd/ViewDoc.jsp?id=223251&Site=CM.rE> Retrieved, December 9, 2014.

<sup>39</sup> Ibid, (In most countries, the police are the only State body that may legally use force to maintain order (in times of peace). Others are allowed to use force only in self defence. This is referred to as a police monopoly on the use of force in times of peace.)

<sup>40</sup> UN. General Assembly resolution 51/59, annex, Article 1

<sup>41</sup> Ibid at annex ii

(known as political interference).<sup>42</sup> Others therefore prefer to regard the police as a service to the public, with the emphasis on the requirement for the police to be responsive to the people's needs, given that they are carrying out their functions on the people's behalf. However, it may be difficult to define the people and their needs because in many countries, different social groups may have different expectations about how the police should respond to certain situations.

The operational independence of the police leadership filters down to rank and file officers, where it takes the form of discretion (or discretionary powers). While on duty, a police officer typically has discretionary power in deciding which deviant behaviour to act on (obviously, acting within the bounds established in national law and policy). "Exercising some discretion is at the very heart of policing, not every offence is worthy of police action nor is police action always the best solution to a problem".<sup>43</sup> Additionally, police officers typically have some room for manoeuvre when using police powers, with the authority to make decisions on such matters as how much force to use and on whether to carry out arrests or searches.

"In other words, good policing is policing that is both effective and fair."<sup>44</sup> "Police who are ineffective, or illegitimate or unfair, in protecting the public against crime will lose the public's confidence."<sup>45</sup> "Good policing is policing with legitimacy on the basis of public consent, rather than repression."<sup>46</sup>

The investigation of crime is the first essential step in the administration of justice. It is the means by which those accused of a crime may be brought before the courts and their guilt or innocence determined. It is also essential to the well being of society, for crime distresses people

---

<sup>42</sup> United Nations Office on Drugs and Crime (UNODC) Handbook on police accountability, oversight and integrity (Criminal Justice Handbook Series) UN New York, July 2011.p.6

<sup>43</sup> Anneke Osse,(2006) *Understanding Policing: A Resource for Human Rights Activists* Amsterdam, Amnesty International Nederland, chapter 4.

<sup>44</sup> United Nations Office on Drugs and Crime (UNODC), at footnote 4. The Secretary-General refers to the importance of an effective, professional and accountable security sector.

<sup>45</sup> Kristina M, Lyn H and Jenny F, (2008 June), "Encouraging public cooperation and support for police", *Policing and Society*, vol. 18, No. 2 Pp. 136-155.

<sup>46</sup> *Ibid* at p.137

and undermines social and economic development. For these reasons, “effective, ethical and lawfully conducted criminal investigation is an extremely important aspect of policing.”<sup>47</sup>

During the course of an investigation, police may well exercise powers of arrest. These powers should be exercised only when necessary and when legal authority to do so exists. People suspected of the crime under investigation may be detained. When that is the case, such detainees must be treated humanely. “It may be necessary to use force to arrest or detain a suspect. Force may be applied only when strictly necessary, and then only to the extent required to achieve the lawful purpose being pursued.”<sup>48</sup>

For the investigation of crime to comply with ethical principles, there must be respect for human dignity and human rights, and compliance with the law by investigators. Investigation of crime in a democratic society entails accountability and responsiveness of the investigators to the community. Furthermore, investigations must be conducted with due regard to the principle of non discrimination.

The purpose of investigating a crime is to gather evidence, to identify the presumed author of the crime, and to present evidence before a court so that guilt or innocence may be decided. The fundamental principles derived from international human rights standards are therefore:

- a) Presumption of innocence of all accused persons,
- b) Entitlement to a fair trial of all accused persons,
- c) Respect for dignity, honour and privacy of all persons

The above principles which are briefly discussed below are embodied in provisions of human rights instruments guaranteeing the right to be presumed innocent until proved guilty,

---

<sup>47</sup> United Nations, New York and Geneva (1997) Human Rights and Law Enforcement ( A manual on Human Rights Training for the police) professional training series No. 5 at p.60

<sup>48</sup> Ibid

protecting the right to a fair trial, and prohibiting arbitrary and unlawful interference with privacy. The right for presumption of innocence is expressed in the Universal Declaration of Human Rights, which reads: “Everyone charged with the penal offence has the right to be presumed innocent until proved guilty according to the law in a public trial at which he has had all the guarantees necessary for his defense.”<sup>49</sup> It is also guaranteed in the international Covenant on civil and political rights<sup>50</sup>, the African Charter on Human and Peoples’ Rights<sup>51</sup>, the American Convention on Human Rights<sup>52</sup> and European convention on human rights.<sup>53</sup> There are two important points that are noted from these provisions and these are:

- (a) Guilt or innocence can be determined only by a properly constituted court, following a properly conducted trial at which the accused person has had all the guarantees necessary for his defense.
- (b) The rights to be presumed innocent until guilty is proved is fundamental to securing a fair trial.

“The presumption of innocence has one important implication for the investigative process which is the fact that all persons under investigation are to be treated as innocent people, whether they have been arrested or detained, or whether they remain at liberty during the investigation.”<sup>54</sup>

The law enforcement agencies have the powers to arrest where it becomes necessary to do so. To arrest someone is to deprive him of his liberty. In law enforcement, the usual purposes of arrest are:

- a) To prevent a person from committing, or continuing to commit, an unlawful act,

---

<sup>49</sup> United Nations, New York and Geneva (1997) Human Rights and Law Enforcement at, Article 11, paragraph 1,

<sup>50</sup> Ibid at Article. 14, para. 2

<sup>51</sup> Ibid at, Article. 7, para. 1 (b)

<sup>52</sup> Ibid at article, 8 para.2

<sup>53</sup> Ibid, at, Article, 6, para. 2

<sup>54</sup> Kristina M, Lyn H and Jenny F, Op.cit, p.207 at 60

b) To enable an investigation to be carried out in relation to an alleged unlawful act committed by the person arrested, or

c) To prevent a person before a court for consideration of any charges against him or her.

Whatever the purpose or purposes of a person's arrest, there must be legal grounds for the arrest, and the arrest must be effected in a professionally competent and adept manner. This means that police must exercise both knowledge and skills when carrying out an arrest.

The term "arrest" is not defined in the human rights instruments' prohibiting arbitrary arrest, but it is defined in the Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment, under "Use of terms", as ...the act of apprehending a person for the alleged commission of an offence or by the action of an authority.

It is of paramount importance for law enforcement officials to be fully aware of how the term "arrest" is defined in their domestic legislation, and of the powers of arrest accorded them under that legislation.

Three Fundamental principles under the general aspects of human rights and arrest deserve mention. First, the principle of individual liberty is one of the essential core principles from which all human rights flow. Deprivation of individual liberty is an extremely serious matter and can be justified only when it is both lawful and necessary. Second is the principle of legality and third being necessity, all underlie the specific provisions on arrest.

There are various provisions in international human rights law designed to protect individual liberty. Provisions which relate specifically to arrest are the prohibition of arbitrary arrest, those which set out procedures to be followed on arrest, those on the arrest of juveniles, and those which require compensation for victims of unlawful arrest.

The European Convention<sup>55</sup> actually states that no one shall be deprived of his liberty except in specified cases, which, in summary, are arrest or detention and it listed the exceptions as follows:

- a. Following conviction by a competent court,
- b. For non-compliance with a lawful order of a court or to secure the fulfillment of an obligation prescribed by law,
- c. For the purpose of bringing a person before the competent legal authority on reasonable suspicion of having committed an offence,
- d. Of a minor by lawful order for the purposes of educational supervision or bringing him or her before a competent legal authority,
- e. Of persons for the purpose of preventing the spread of infectious disease, or of persons of unsound mind, alcoholics or drug addicts, or vagrants,
- f. To prevent a person's unauthorized entry into, or residence in, the country.

Notably, these cases fall into three broad categories, although there is some overlap, for instance, whereas those in (a) and (c) are clearly connected with criminal law and procedure, those in (b),(d) and (e) are more concerned with social protection or control, and those in (f) fall into the category of “administrative detention”.

The International Covenant on Civil and Political Rights<sup>56</sup> also laid down procedures to be followed on arrest thus:

- a) Anyone who is arrested shall be informed, at the time of arrest, of the reasons for his arrest and shall be promptly informed of any charges against him.

---

<sup>55</sup>United Nations, New York and Geneva (1997) Human Rights and Law Enforcement at, Article, 5

<sup>56</sup>Ibid at Article 9, paragraphs 2 and 3

- b) Anyone arrested or detained on a criminal charge shall be brought promptly before a judge or other officer authorized by law to exercise judicial power and shall be entitled to trial within a reasonable time or to release. It shall not be the general rule that persons awaiting trial shall be detained in custody, but release may be subject to guarantees to appear for trial, at any other stage of the judicial proceedings, and, should occasion arise, for execution of the judgment.

These provisions are repeated in the American Convention on Human Rights<sup>57</sup> and the European Convention on Human Rights.<sup>58</sup> No similar provisions are contained in the African Charter on Human and People's Rights.

However, four of the principles in the Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment refer to procedures to be followed on arrest, as follows:

- i) Arrests are to be carried out in accordance with the law and by competent officials or authorized persons.<sup>59</sup>
- ii) At the time of arrest, persons are to be informed of the reason for their arrest. They are to be informed promptly of charges against them.<sup>60</sup>
- iii) A record is to be made of the reason for arrest, the time of arrest, arrival at place of custody and first appearance before a judicial or other authority, the identity of law enforcement officials' concerned and precise information concerning place of custody.<sup>61</sup>

---

<sup>57</sup>Ibid at Article 7, paras. 4-5

<sup>58</sup>Ibid at, Article. 5, paras 2-3

<sup>59</sup>The International Covenant on Civil and Political Rights (ICCPR) at Principle 2

<sup>60</sup>Ibid at, Principle 10

<sup>61</sup>Ibid at, Principle 12

- iv) Persons arrested are to be provided with information on and an explanation of, their rights and how to avail themselves of them<sup>62</sup>.

Various instruments include additional safeguards designed to secure supervision of the arrest process are provided in the International Covenant on Civil and Political Rights. A detail analysis of these safeguards is beyond the scope of this work. It is however instructive to note the aspect that clarify arrest where a juvenile is concerned.

The United Nations Standard Minimum Rules for the Administration of Juvenile Justice (Beijing Rules)<sup>63</sup> requires:

- a) The parents or guardians of arrested juveniles to be immediately notified of the fact of such arrest,
- b) A judge or other competent official or body to consider, without delay, the issue of release,
- c) Contacts between law enforcement officials and juvenile offenders to be managed in such a way as to respect the legal status of the juvenile and avoid harm to him or her, with due regard to the circumstances of the case.

The Convention on the Rights of the Child also refers to the arrest of juveniles where it states that:

No child shall be deprived of his or her liberty unlawfully or arbitrarily. The arrest, detention or imprisonment of a child shall be in conformity with the law and shall be used only as a measure of last resort and for the shortest appropriate period of time.<sup>64</sup>

Detention is one of the powers of law enforcement and the International human rights standards and most national legal systems make a distinction between “detainees” and

---

<sup>62</sup>The United Nations Standard Minimum Rules for the Administration of Juvenile Justice (Beijing Rules) at, Principle 13

<sup>63</sup>Ibid at, Rules 10

<sup>64</sup>The United Nations Convention on the Rights of the Child, Articles, 37 (b)

“prisoners”. A detainee is a person who is deprived of personal liberty, but who has not been convicted for an offence. A prisoner is a person deprived of liberty as a result of having been convicted. As police in most legal systems deal principally with pre conviction detainees, the discourse here shall be centered on that category of detainee.

All persons deprived of their liberty are vulnerable to mistreatment. Some categories of detainee, such as women and children, are particularly vulnerable. Furthermore, as noted above, it is usually the case that detainees in police custody have not been convicted of any crimes. They are innocent people in respect of whom the presumption of innocence applies.

For these reasons, police conduct towards detainees should be humane, and in strict compliance with the law and guidelines governing treatment of people in custody. “This is particularly important when police are interviewing or interrogating persons suspected or accused of committing a crime.”<sup>65</sup>

International standards on the treatment of detainees set out fundamental principles and detailed provisions which, if complied with, will secure humane and legal conditions of detention for persons in police custody. People are kept in police detention following the exercise of a judge or other legal authority exercising judicial power that they may be detained by police.

Detainees are subject to a legally sanctioned process, and they are a category of persons who benefit from specific forms of protection based on the following principles:

- i) No one shall be subjected to torture or other ill treatment.
- ii) All detainees are entitled to humane treatment and to respect for their inherent human dignity,

---

<sup>65</sup> United Nations, New York and Geneva (1997) Human Rights and Law Enforcement ( A manual on Human Rights Training for the police) professional training series No. 5 Op.cit, p.208 at p.75

iii) All persons are presumed innocent until proved guilty according to law.

International human rights instruments contain very detailed provisions on detention. They cover the prohibition of torture, general requirements on humane treatment and specific requirements concerning juveniles and women. Torture been comprehensively outlawed by the international community is prohibited by the Universal Declaration of Human Rights, which reads: “*No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment.*”<sup>66</sup>

It is prohibited in virtually the same terms in the international covenant on civil and political rights,<sup>67</sup> the African Charter on Human and peoples’ rights,<sup>68</sup> the American Convention on Human Rights,<sup>69</sup> and the European Convention on Human Rights.<sup>70</sup>

A United Nations Declaration, and a convention, against torture set our detailed measure to counter the practice of torture.

“Declaration on the protection of all persons from being subjected to torture and other cruel, inhuman or degrading treatment or punishment.”<sup>71</sup>

The declaration defines torture in article I. and that definition is relevant to police officials because part of it states that torture is severe pain or suffering whether physical or mental Inflicted by or at the instigation of a public official on a person for such purposes as obtaining from him or a third person information or confession, punishing him for an act he has committed or is suspected of having committed, or intimidating him or other person”...<sup>72</sup>

---

<sup>66</sup>United Nations Declaration, and a convention, against torture Article 5

<sup>67</sup>Ibid at Art. 7

<sup>68</sup>Ibid at, Art. 5

<sup>69</sup>Ibid at, Art. 5 para. 2

<sup>70</sup>Ibid at, Art.3

<sup>71</sup>Ibid at, Art.1

<sup>72</sup> United Nations, NewYork and Geneva (1997) Human Rights and Law Enforcement ,Op.cit, p.208 at p.82

The care and custody of detainees is an extremely important aspect of policing. “Despite the fact that the treatment of persons in detention is very closely regulated, under both international law and domestic law, abuses continue to occur.”<sup>73</sup>

Law enforcement agents are empowered to use force and firearms when it is inevitable. Police in every society are entrusted with a variety of powers for the purposes of enforcing law and maintaining order. Inevitably, the exercise by a police official of any of the powers which are vested in him or her has an immediate and direct effect on the rights and freedoms of fellow citizens.

Along with the authority of police to use force under certain conditions and restraints comes a great responsibility to ensure that this authority is exercised lawfully and effectively. The task of police in society is a difficult and delicate one, and it is recognized that the use of force by police under clearly defined and controlled circumstances is entirely legitimate. However, abuse of the power to use force strikes at the very principle on which human rights are based i.e. that of respect for the inherent dignity of the human person. It is, therefore essential that steps be taken to prevent such abuse, and to provide for effective remedies, investigations and sanctions when there has been excessive or abusive use of force.

The concept of “force” is not defined in international texts relevant to the use of force by police. Dictionary definitions of force usually invoke such terms as strength, power, violence and exertion. “Law enforcement officials should be familiar with the ways in which “force” has been defined under their own domestic laws and codes”.<sup>74</sup>

There are some Fundamental principles of the general aspects of the use of force as discussed below:

---

<sup>73</sup> Ibid, p.80

<sup>74</sup> Ibid, p.86

(a) The principles of necessity and proportionality lie behind all the detailed provisions regulating the use of force by police. These principles require, respectively, that force should be used by police only when strictly necessary for law enforcement and maintaining public order, and that the application of force should be proportional, i.e. force should be applied only to the extent required for the legitimate end of law enforcement and maintaining public order.

(b) There is also specific provisions on the use of force and all these principles are embodied in the codes of conduct for law enforcement officials, which states that:

“Law enforcement officials may use force only when strictly necessary and to the extent required for the performance of their duty.”<sup>75</sup>

The commentary to article 3 repeats the requirement of proportionality in the use of force and states that the use of firearms is considered an extreme measure.

The basic principles on the use of force and firearms by law enforcement officials provide specific and detailed guidelines on how the requirements of necessity and proportionality can be met.

In the preamble to the principles, it is acknowledged that: “the work of law enforcement officials is a social service of great importance”.

A threat to the life and safety of law enforcement officials must be seen as a threat to stability of society as a whole.

Law enforcement officials have a vital role in the protection of the right to life, liberty and security of the person, as guaranteed in the universal declaration of human rights and reaffirmed in the international covenant on civil and political rights.

---

<sup>75</sup> United Nations, New York and Geneva (1997) Human Rights and Law Enforcement, Article 3

The exercise of the power to use force can affect the most fundamental of right which is the right to life. Police use of force which amounts to a violation of the right to life represents a clear defeat of one of the prime purposes of policing, that of maintaining the safety and security of fellow citizens. Depending on the circumstances, it may also be a very serious breach of both domestic criminal law and international law.

The right to life is protected under customary international law, and going by of the provision of the Universal Declaration of Human Rights, which states; “Everyone has the right to life, liberty and security of person.”<sup>76</sup>

It is also protected under the international covenant on civil and political rights,<sup>77</sup> and under regional instruments such as the African Charter on Human and Peoples’ Rights,<sup>78</sup> the American Convention on Human Rights<sup>79</sup> and the European Convention on Human Rights<sup>80</sup>.

The international covenant requires the right to life to be protected by law, and forbids arbitrary deprivation of life, the American Convention and the European Convention require the right to life to be protected by law, and the African Charter and the American Convention state explicitly that no one shall be arbitrarily deprived of life.

An arbitrary action can be taken to mean one which is not in conformity with the law, or one which is unjust notwithstanding conformity with the law. “Arbitrary deprivations of life include such atrocities as genocide, war crimes, death arising from executions not preceded by proper legal proceedings, deaths arising from torture or ill treatment, and deaths arising from excessive use of force by law enforcement officials.”<sup>81</sup>

---

<sup>76</sup> Ibid

<sup>77</sup>Ibid at. Article. 6

<sup>78</sup>Ibid at Article.4

<sup>79</sup>Ibid at Article.4

<sup>80</sup>Ibid at Article. 2

<sup>81</sup>International Committee of Red Cross (ICRC) Geneva,(1998)Op.cit, p.198, at,p.88

#### **4.5 Ethical and Legal Standards in Law Enforcement on the Prevention and Control of Crime and Insecurity**

Police ethics or a lack thereof is a serious topic that has been the pinnacle of law enforcement concern for several years. Ethics can best be defined as an individual's moral principles or values and police officers are held to higher standards in both their work and personal life. If officers feel they are being victimized by their agency or the system it can cause a breakdown in ethics. "The higher our ethical values the lower the chance of corruption, but the lower our values the higher the chance of corruption."<sup>82</sup>

Officers cannot bend the law if they want the occupation to be considered professional, therefore, it is each individual member's responsibility to act in a professional manner.

The United Nations Office on Drugs and Crime (UNODC) also define ethical code as a system of internal and external checks and balances aimed at ensuring that police carry out their duties properly and are held responsible if they fail to do so. Such a system is meant to uphold police integrity and deter misconduct and to restore or enhance public confidence in policing. "Police integrity refers to normative and other safeguards that keep police from misusing their powers and abusing their rights and privileges"<sup>83</sup>.

The International Covenant on Civil and Political Rights<sup>84</sup> and the International Covenant on Economic, Social and Cultural Rights<sup>85</sup> set out principles on the fundamental rights of individuals to be observed by States. Several treaties and principles also contain provisions that are applicable to policing, both in terms of prohibited police behaviours such as torture and desirable priorities for police to set in their activities.

---

<sup>82</sup> James, R. (2003, October). For the Veteran Officers: Leadership, Ethics, and Wellness Training. [Electronic Version]. *The Police Chief*, vol. 79, no. 10.p.5

<sup>83</sup> UN. (New York 2011), Handbook on police accountability, oversight and integrity, Criminal Justice Handbook Series in summary.

<sup>84</sup> UN. General Assembly resolution 2200 A (XXI),16 December, 1966, UN Treaty series. Vol.999.p.171, Retrieved May 30, 2015 from <http://www.refworld.org/docid/3ae6b3aa.html>.

<sup>85</sup>Ibid

Some examples are the Convention on the Elimination of All Forms of Discrimination against Women,<sup>86</sup> the Convention on the Rights of the Child,<sup>87</sup> and the International Convention on the Elimination of All Forms of Racial Discrimination.<sup>88</sup> An overview of the international standards that are relevant to policing can be found in annex I.<sup>89</sup> Treaties such as the International Covenant on Civil and Political Rights, which has been ratified by an absolute majority of States, establish legally binding obligations. “As at 9 August 2010, 166 countries worldwide are party to this treaty”.<sup>90</sup>

A basic notion underlying the international legal framework is the right to remedy, which means that States need to establish a mechanism whereby people can seek redress if their rights have been violated. The Covenant states:

“Each State Party to the present Covenant undertakes:

(a) To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity;

(b) To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy;

(c) To ensure that the competent authorities shall enforce such remedies when granted.”<sup>91</sup>

---

<sup>86</sup>United Nations, *Treaty Series*, vol. 1249, No. 20378.

<sup>87</sup>Ibid, vol. 1577, No. 27531.

<sup>88</sup>Ibid, vol. 660, No. 9464.

<sup>89</sup>*United Nations Criminal Justice Standards for United Nations Police*, ( A compilation of international human rights and criminal justice principles that United Nations police Personnel must know, abide by and promote when deployed in peacekeeping operations has recently been updated and released), Retrieved December 11,2014 from [www.unodc.org/documents/justice-and-prison-reform/08-58900\\_Ebook.pdf](http://www.unodc.org/documents/justice-and-prison-reform/08-58900_Ebook.pdf)).

<sup>90</sup> Ibid

<sup>91</sup>Ibid at, Article 2, paragraph 3

More specifically, the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment<sup>92</sup> states in article 12: “Each State Party shall ensure that its competent authorities proceed to a prompt and impartial investigation, wherever there is reasonable ground to believe that an act of torture has been committed in any territory under its jurisdiction.” Articles 13 and 14 establish that any individual who alleges that he or she has been subjected to torture in any territory under the jurisdiction of the State Party has the right to complain to, and to have his case promptly and impartially examined by, its competent authorities and has the right to fair and adequate compensation. Moreover, also in accordance with article 13, the complainant must be protected against all ill treatment or intimidation as a consequence of his complaint. Pursuant to article 15, any statement which is established to have been made as a result of torture shall not be invoked as evidence in any proceedings, except against a person accused of torture as evidence that the statement was made. Pursuant to part II of the Convention, States parties have to report periodically to the Committee against Torture on the measures they have taken to give effect to their undertakings under the Convention. Documents such as principles and declarations give guidance to Member States on the implementation of binding treaties. An important document for the police is the Code of Conduct for Law Enforcement Officials adopted by the General Assembly in its resolution 34/169.

The Code of Conduct for Law Enforcement Officials, which refers to the various functions of law enforcement as well as the different aspects of accountability as discussed earlier sub. Heads of this chapter states that the Code needs to be supported by additional important principles and prerequisites for the humane performance of law enforcement functions, namely:

---

<sup>92</sup>United Nations, *Treaty Series*, vol. 1465, No. 24841

- (a) That, like all agencies of the criminal justice system, every law enforcement agency should be representative of and responsive and accountable to the community as a whole;
- (b) That the effective maintenance of ethical standards among law enforcement officials depends on the existence of a well-conceived, popularly accepted and humane system of laws;
- (c) That every law enforcement official is part of the criminal justice system, the aim of which is to prevent and control crime, and that the conduct of every functionary within the system has an impact on the entire system;
- (d) That every law enforcement agency, in fulfillment of the first premise of every profession, should be held to the duty of disciplining itself in complete conformity with the principles and standards herein provided and that the actions of law enforcement officials should be responsive to public scrutiny, whether exercised by a review board, a ministry, a prosecutor, the judiciary, an ombudsman, a citizens' committee or any combination thereof, or any other reviewing agency;
- (e) That standards as such lack practical value unless their content and meaning, through education and training and through monitoring, become part of the creed of every law enforcement official.

In addition, articles 7 and 8 of the Code of Conduct require police to oppose and combat corruption and to oppose and report any violation of the Code of Conduct internally or to other appropriate authorities or organs vested with reviewing or remedial power. The commentary on article 8 refers to the need to report violations within the chain of command but, only when no other remedies are available or effective, to take other lawful action outside the chain of command, and, as a last resort, to the media. This is known as whistle blowing.

In order to clarify the discursion so far, it is helpful to reproduce the Code of Conduct in full as in below:

Code of Conduct for Law Enforcement Officials,

***Article 1***

Law enforcement officials shall at all times fulfill the duty imposed upon them by law, by serving the community and by protecting all persons against illegal acts, consistent with the high degree of responsibility required by their profession.

***Article 2***

In the performance of their duty, law enforcement officials shall respect and protect human dignity and maintain and uphold the human rights of all persons.

***Article 3***

Law enforcement officials may use force only when strictly necessary and to the extent required for the performance of their duty.

***Article 4***

Matters of a confidential nature in the possession of law enforcement officials shall be kept confidential, unless the performance of duty or the needs of justice strictly require otherwise.

***Article 5***

No law enforcement official may inflict, instigate or tolerate any act of torture or other cruel, inhuman or degrading treatment or punishment, nor may any law enforcement official invoke superior orders or exceptional circumstances such as a state of war or a threat of war, a threat to national security, internal political instability or any other public emergency as a justification of torture or other cruel, inhuman or degrading treatment or punishment.

### *Article 6*

Law enforcement officials shall ensure the full protection of the health of persons in their custody and, in particular, shall take immediate action to secure medical attention whenever required.

### *Article 7*

Law enforcement officials shall not commit any act of corruption. They shall also rigorously oppose and combat all such acts.

### *Article 8*

Law enforcement officials shall respect the law and the present Code. They shall also, to the best of their capability, prevent and rigorously oppose any violations of them.

Law enforcement officials who have reason to believe that a violation of the present Code has occurred or is about to occur shall report the matter to their superior authorities and, where necessary, to other appropriate authorities or organs vested with reviewing or remedial power.

In 1989, the General Assembly endorsed the Guidelines for the Effective Implementation of the Code of Conduct for Law Enforcement Officials<sup>93</sup> in its resolution 44/162.

The Guidelines state, *inter alia*, that:

Effective mechanisms need to be established to ensure the internal discipline and external control as well as the supervision of law enforcement officials. Additionally, they state in section B.4 that provisions for the receipt and processing of complaints against law enforcement officials made by members of the public shall be made.

Another instrument that is relevant for the police is the International Code of Conduct for Public Officials.<sup>94</sup> Detailing the full text of this Code is beyond the scope of this work. It is however worthy of mention.

---

<sup>93</sup>U.N. Economic and Social Council resolution 1989/61, annex.

The Basic Principles on the Use of Force and Firearms by Law Enforcement Officials<sup>95</sup> include principles related to accountability in relation to the use of force and firearms by police, including:

- i. The need for the availability of an effective review process with the Requirement that independent administrative or prosecutorial authorities need to be able to exercise jurisdiction in appropriate circumstances and that cases of death and serious injury or other grave consequences must be reported promptly to the competent authorities responsible for administrative review and judicial control.
- ii. The principle that persons affected by the use of force and firearms or their legal representatives and dependents should have access to an independent process, including a judicial process.
- iii. The principle that superior officers must be held responsible if they know, or should have known that their subordinates are resorting, or have resorted, to the unlawful use of force and firearms, and they did not take all measures in their power to prevent, suppress or report such use.
- iv. The principle that officials who refuse to carry out unlawful orders to use force and firearms or who report such use shall not suffer criminal or disciplinary sanction.
- v. The principle that officials may not claim that they were obeying superior orders if they knew that such orders were manifestly unlawful and if they had a reasonable opportunity to refuse to carry out the orders. In any case, the superiors who gave the unlawful orders are also to be held responsible.

---

<sup>94</sup> U.N. General Assembly resolution 51/59, annex.

<sup>95</sup> *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, 27 August-7 September 1990: report prepared by the Secretariat* (United Nations publication, Sales No. E.91.IV.2), chap. I, sect. B.2, annex. Principles 22-26 deal specifically with accountability issues.

The Principles relating to the status of national institutions<sup>96</sup> (the Paris Principles) are intended to guide the status and functioning of national institutions for the protection and promotion of human rights, stating that the mandate of such institutions should be as broad as possible. “Such institutions, whose names vary from country to country, play an important role as independent police oversight bodies.”<sup>97</sup> They typically deal with misconduct of all State officials rather than that of the police exclusively, and sometimes there are police specific bodies such as a police ombudsman or a police complaints commission.

According to the Paris Principles, the responsibilities of a national institution for the protection and promotion of human rights should include submitting, upon request or on the institution’s own initiative, opinions, recommendations, proposals and reports on any matters concerning the protection and promotion of human rights in relation to the following:

- i. Any legislative or administrative provisions, as well as provisions relating to judicial organization, intended to preserve and extend the protection of human rights, and any situation of violation of human rights which it decides to take up,
- ii. The preparation of reports on the national situation with regard to human rights in general, and on more specific matters.

A further such responsibility is to draw the attention of the Government to situations in any part of the country where human rights are violated and to submit to the Government proposals for initiatives to put an end to such situations and, where necessary, express an opinion on the positions and reactions of the Government. The composition of the national institution should reflect the plural society and guarantee independence. The national institutions should freely consider any questions falling within their competence, hear any person and obtain any

---

<sup>96</sup> U.N. General Assembly resolution 48/134, annex.

<sup>97</sup> Ibid, (A record of the institutions in different countries and their accreditation, and of the national, regional and international standards guiding their work is available from) [www.nhri.net](http://www.nhri.net). Retrieved, December 2014

information necessary to make an assessment of situations falling within their competence and publicize its opinions and recommendations.

An important police oversight mechanism is the practice of making regular visits to places of police detention and places where police interrogate suspects, as provided for by the Optional Protocol to the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment,<sup>98</sup> which entered into force in 2006.<sup>99</sup>

Article 1 of the Optional Protocol states that the purpose of the Protocol is “to establish a system of regular visits undertaken by independent international and national bodies to places where people are deprived of their liberty, in order to prevent torture and other cruel, inhuman or degrading treatment or punishment.” Such visits can play an important role in the prevention of police misconduct such as maltreatment of detainees. “The mechanics of the implementation of the provisions are left to the discretion of the State party, provided that it consults with non State actors, in particular human rights defenders.”<sup>100</sup>

The Standard Minimum Rules for the Treatment of Prisoners,<sup>101</sup> the United Nations Rules for the Treatment of Women Prisoners and Non-custodial Measures for Women Offenders (the Bangkok Rules)<sup>102</sup> and the Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment<sup>103</sup> set out basic principles on treating detainees with dignity. They require States to make known places of detention and the identities of custody and interrogation officers so as to facilitate accountability.

---

<sup>98</sup> U.N. General Assembly resolution 57/199, annex.

<sup>99</sup> Ibid, (As at 5 August 2010, it had been ratified by 54 Member States).

<sup>100</sup> Association for the Prevention of Torture, (Geneva, 2008). “Civil society and national preventive mechanisms under the Optional Protocol to the Convention against Torture”

<sup>101</sup> *Human Rights: A Compilation of International Instruments, Volume I (First Part): Universal Instruments* (United Nations publication, Sales No. E.02.XIV.4 (Vol. I, Part 1)), sect. J, No. 34. Part II.C of the Standard Minimum Rules on prisoners under arrest or awaiting trial is particularly relevant for the police.

<sup>102</sup> UN.Economic and Social Council resolution 2010/16.

<sup>103</sup> UN.General Assembly resolution 43/173, annex.

The Body of Principles, dating back to 1988, also includes a requirement for places of detention to accept a system of external visits similar to that provided for under the Optional Protocol to the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment.<sup>104</sup> Additionally, the Body of Principles provides detainees with the right to make a complaint to the authorities responsible for the administration of the place of detention and to higher authorities and, when necessary, to appropriate authorities vested with reviewing or remedial powers, and also to bring the complaint before a judicial or other authority in case it is rejected or inordinately delayed.<sup>105</sup> Finally, the Body of Principles states that whenever the death or disappearance of a detained or imprisoned person occurs during his detention or imprisonment, an inquiry into the cause of death or disappearance shall be held by a judicial or other authority, either on its own motion or at the instance of a member of the family of such a person or any person who has knowledge of the case. Such an inquiry can also be held if someone dies shortly after having been detained, the findings can be made available on request.<sup>106</sup>

Habeas corpus is another fundamental measure to hold police accountable when depriving someone of his or her liberty. Under this principle, someone who is arrested or detained has the right to be brought promptly before a judge or other judicial authority to review the lawfulness of the detention. This principle is established in a range of instruments, most notably the International Covenant on Civil and Political Rights.<sup>107</sup> The treaties and principles referred to above focus on structures that the State should set up in order to enhance or ensure

---

<sup>104</sup> Ibid, Principle 29.

<sup>105</sup> Ibid, Principle 33.

<sup>106</sup> Ibid, Principle 34.

<sup>107</sup> International Covenant on Civil and Political Rights, art. 9, para. 4. It is also included in the Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment, the Standard Minimum Rules for the Treatment of Prisoners and the Declaration on the Protection of All Persons from Enforced Disappearance (General Assembly resolution 47/133).

accountability. The Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms<sup>108</sup> focuses on the rights of the public to organize themselves in order to promote human rights, including monitoring actions performed by State agents, obviously including the police.

Article 1 of the Declaration states that everyone has the right, individually and in association with others, to promote and to strive for the protection and realization of human rights and fundamental freedoms at the national and international levels. Article 5 refers to the right of everyone to form non-governmental organizations, meet or assemble peacefully and communicate with non-governmental or intergovernmental organizations, and article 9 provides for the right to file complaints and also to have such complaints promptly reviewed and have the right to redress, including any compensation due, where there has been a violation. When filing a complaint, people have the right to professionally qualified legal assistance or other relevant advice and assistance in defending human rights and fundamental freedoms. Finally, they have the right to unhindered access to and communication with international bodies with general or special competence to receive and consider communications on matters of human rights and fundamental freedoms.

In recent years, a number of international documents signed under the auspices of the United Nations and regional organizations have acknowledged the negative effects of corruption on the protection of human rights and on development. The United Nations Convention Against Corruption obliges States to establish a wide range of measures aimed at preventing and fighting

---

<sup>108</sup>UN, General Assembly resolution 53/144, annex

corruption and at promoting integrity, transparency and accountability in its widest sense.<sup>109</sup> The purpose of the Convention is listed as:

- (a) To promote and strengthen measures to prevent and combat corruption more efficiently and effectively;
- (b) To promote, facilitate and support international cooperation and technical assistance in the prevention of and fight against corruption, including in asset recovery;
- (c) To promote integrity, accountability and proper management of public affairs and public property.<sup>110</sup>

The Convention obliges States parties to develop, implement or maintain effective coordinated anti corruption policies as well as strategies to prevent corruption and evaluate the adequacy of the measures taken periodically. It also requires States parties to establish a legal framework that criminalizes a range of corruption-related offences.<sup>111</sup> Article 6 stipulates the establishment of effective bodies that prevent corruption, article 7 deals with the recruitment, hiring, retention, promotion and retirement of civil servants, article 8 urges States parties to apply codes or standards of conduct and also to take disciplinary or other measures against public officials who violate these codes or standards, and article 13 deals with promoting active participation of society.<sup>112</sup>

The most important regional instruments related to combating corruption include the African Union Convention OF 2003 on Preventing and Combating Corruption, the Inter

---

<sup>109</sup>United Nations Convention Against Corruption Article 1

<sup>110</sup> Ibid

<sup>111</sup>Sections 9 and 10, part II, *Model Criminal Code* (2007),(Washington, D.C., United States Institute of Peace. (may give guidance to draftersof (post-conflict) criminal laws on corruption.)

<sup>112</sup> U.N. Resolution 3/1 of the Conference of the States Parties to the United Nations Convention against Corruption, held in Doha from 9 to 13 November 2009, establishes a review mechanism for the implementation of the Convention (CAC/COSP/2009/15, sect. I.A, resolution 3/1).

American Convention against Corruption of 1996,<sup>113</sup> the Organisation for Economic Co-operation and Development Convention on Combating Bribery of Foreign Public Officials in International Business Transactions of 1997<sup>114</sup> and the Agreement establishing the Group of States against Corruption (GRECO) adopted by the Committee of Ministers of the Council of Europe in 1999. The Global Standards to Combat Corruption in Police Forces/Services, adopted by the International Criminal Police Organization (INTERPOL), aim to ensure that police have high standards of integrity and promote and strengthen the development of measures needed to prevent, detect, punish and eradicate corruption in the police forces/services within its national boundaries and to bring to justice police officers and other employees of police forces/services who are corrupt.”<sup>115</sup> The Global Standards call for the establishment of a mechanism such as an oversight body to monitor the above mentioned systems and measures and their adequacy.<sup>116</sup> The Standards include a provision authorizing the INTERPOL General Secretariat to monitor their implementation in member countries. It is also inclusive of a summary of the different treaties and “soft law” principles and how they relate to the different aspects of police accountability.

The Regional efforts in this regards cannot be ignored or underestimated. However going by the scope of limitation of this work, only a brief discussion is attempted in this sub head.

Notably, there is a body of jurisprudence from the European Court of Human Rights and the Inter American Court of Human Rights on the liability of individual State agents (in most cases police officers) for ill treatment and unlawful killings as well as on responsibility for the planning and control of individual operations and proper legal frameworks for the use of force and firearms. There are also regional standards, as described below.

---

<sup>113</sup> U.N. Resolution, E/1996/99.

<sup>114</sup>United, Nations publication (*Corruption and Integrity Improvement Initiatives in Developing Countries* Sales No.E.98.III.B.18).

<sup>115</sup>Article 1. The General Assembly of INTERPOL adopted the Global Standards in 2002 by its resolution AG-2002-RES-01 at its 71st session in Yaoundé.

<sup>116</sup>Articles 4.14-4.17 of the INTERPOL Global Standards.

In Africa for instance, The African Charter on Human and Peoples' Rights<sup>117</sup> does not refer to the right to remedy, but the African Commission on Human and People's Rights adopted a resolution in 2006 on police reform, accountability and civilian police oversight in Africa.<sup>118</sup>

The preamble of the resolution states:

Concerned that in many of the African States, there exist no independent policing oversight mechanisms, to which members of the public may report police misconduct and abuse of their powers for redress and that, where they do, they are directly under police authorities, Recognizing, that police forces in African States, which do not have oversight mechanisms require reform in order to become effective instruments of security, safety, and justice and respect for human and people's rights across the continent...<sup>119</sup>

Noting that accountability and the oversight mechanisms for policing form the core of democratic governance and are crucial to enhancing rule of law and assisting in restoring public confidence in police, to developing a culture of human rights, integrity and transparency within the police forces, and to promoting a good working relationship between the police and the public at large, Encouraged by the initiative taken in the formation of the African Policing Civilian Oversight Forum (APCOF), through the collaboration of Civil Society and State Civilian Police Oversight agencies, as an African initiative to promote police reform and with it the building and strengthening of civilian police oversight in Africa .

In article 3 of the Charter, the Commission urges State parties to the African Charter to establish independent civilian policing oversight mechanisms where they do not exist which shall include civilian participation.

---

<sup>117</sup>United Nations, Treaty Series, vol. 1520, No. 26363.

<sup>118</sup>African Commission on Human and People's Rights, 40th session held in Banjul from 15 to 29 November 2006.

<sup>119</sup> Ibid

A website<sup>120</sup> with links to African regional and national legislation includes recent updates. The website also describes the accountability structures of police agencies in the countries enlisted.<sup>121</sup>

In the case of Europe, The member States of the Council of Europe are subject to scrutiny by the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment. This Committee “shall, by means of visits, examine the treatment of persons deprived of their liberty with a view to strengthening, if necessary, the protection of such persons from torture and from inhuman or degrading treatment or punishment.”<sup>122</sup>

Delegations from the Committee visit member States periodically and may organize additional ad-hoc visits. States are notified of forthcoming visits, but the Committee does not have to specify the exact time of the visit. Pursuant to the Convention, delegations have unlimited access to places of detention and the right to move inside such places without restriction. They interview persons deprived of their liberty in private and communicate freely with anyone who can provide information. The recommendations that the Committee may formulate on the basis of facts found during the visit are included in a report that is sent to the State concerned. This report is the starting point for an ongoing dialogue with the State concerned. The Committee also publishes extracts from its general reports containing minimum standards that police must observe.

In 2001, the Committee of Ministers of the Council of Europe adopted the European Code of Police Ethics, which is the most elaborate of such code in the world. The principles of the Code state that national laws relating to the police should accord with international standards

---

<sup>120</sup>[www.apcof.org.za](http://www.apcof.org.za). Retrieved, December 13, 2014

<sup>121</sup>Angola, Botswana, the Democratic Republic of the Congo, Ghana, Kenya, Lesotho, Malawi, Mauritius, Mozambique, Namibia, Nigeria, South Africa, Swaziland, the United Republic of Tanzania, Uganda, Zambia and Zimbabwe.

<sup>122</sup>European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment(Council of Europe, *European Treaty Series*, No. 126), art. 1. More information on the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment is available from [www.cpt.coe.int](http://www.cpt.coe.int). Retrieved, December 13, 2014.

to which the country is a party and must be clear and accessible to the public, and that the police should be subject to the same legislation as ordinary citizens.

The Code contains the following provisions on accountability:<sup>123</sup>

- i) The police shall be accountable to the State, the citizens and their representatives. They shall be subject to efficient external control;
- ii) State control of the police shall be divided between the legislative, executive and the judicial powers;
- iii) Public authorities shall ensure effective and impartial procedures for complaints against the police;
- iv) Accountability mechanisms, based on communication and mutual understanding between the public and the police, shall be promoted;
- iv) Codes of ethics of the police, based on the principles set out in the Code shall be developed in member States and overseen by appropriate bodies.

The Code also states that the police must be organized with a view to earning public respect, they must be under the responsibility of civilian authorities, they should normally be clearly recognizable, they should enjoy sufficient operational independence and should be accountable for the tasks carried out, police personnel at all levels should be personally responsible and accountable for their own actions or omissions or for orders to subordinates; there should be a clear chain of command and it should always be possible to determine which superior is ultimately responsible for the acts or omissions of police personnel, the police should be ready to give objective information on their activities to the public, the police organization should contain efficient measures to ensure the integrity and proper performance of police staff, in particular to guarantee respect for individuals' fundamental rights and freedoms, there should

---

<sup>123</sup>United Nations Convention Against Corruption, Articles. 59-63

be effective measures to combat corruption, and disciplinary measures brought against police staff should be subject to review by an independent body or a court, and the public authorities should support police personnel who are subject to ill founded accusations concerning their duties.

Another useful reference document, also for those operating outside the jurisdiction of the Council of Europe, is the Opinion of the Commissioner for Human Rights concerning Independent and Effective Determination of Complaints against the Police, issued in 2009.<sup>124</sup>

Overall, it is noted that International and regional treaties are binding for States that have ratified them, declarations and principles give guidance to States in implementing such obligations. A fundamental notion underlying international human rights standards is that States should enable the people living in their territory to seek redress if their rights have been violated. This right to remedy is essential in order to avoid impunity when State representatives violate internationally recognized human rights principles.

The existence of the right to remedy means that States must establish a mechanism for receiving complaints, which must be investigated thoroughly and impartially. Also, it means that States must start investigations on their own initiative when there are grounds to believe that serious misconduct has occurred. It also means that wrongdoers must be punished and that victims can receive compensation.

International standards also give direction to police officers in carrying out their duties, also advising them on conduct to be avoided. They also enable both internal and external bodies, including individuals and groups, to monitor police actions with a view to enhancing their integrity.

---

<sup>124</sup> Council of Europe (12, March 2009) commissioner for Human Rights Original Version, Available from: <https://wcd.coe.int/ViewDoc.jsp?id=1417857&Site=CommDH&BackColorInternet=FEC65B&BackColorIntranet=FEC65B&BackColorLogged=FFC679> (accessed 17, June 2015, 2.38pm).

#### 4.6 Good Practices (Strategies) in Addressing Cyber Insecurity

While no comprehensive international legal framework currently governs all cyber attacks, a patchwork of efforts provides some tools the United States and other countries can employ to control this growing threat. This sub head surveys legal mechanisms created by the United Nations, North Atlantic Treaty Organization (NATO), the Council of Europe, the Organization of American States, and the Shanghai Cooperation Organization to directly regulate cyber attacks. While both the Council of Europe and the Organization of American States have taken actions relating to cyber crime, a category of activity that overlaps in part with cyber attacks, the increased computer network protection and regulations are also relevant to efforts to combat cyber attacks. Collectively, these organizational measures demonstrate a growing interest in addressing this issue through common legal frameworks. Yet these efforts have fallen short of establishing a rigorous legal framework that can effectively govern all cyber attacks.

On the part of the United Nations, there has been only limited U.N. action on the issue of cyber security. The U.N. General Assembly has passed several related resolutions.<sup>125</sup> These resolutions, however, are vague and have not required any specific action by U.N. members.<sup>126</sup> This is equally true of the General Assembly's two related resolutions on the Creation of a Global Culture of Cyber security and the Protection of Critical Informational Infrastructures,<sup>127</sup>

In August 1999, the United Nations sponsored an international meeting of experts in Geneva to better grasp the security implications of emerging information technologies.<sup>128</sup> A

---

<sup>125</sup>U.N. G.A. Res. 58/32, U.N. Doc. A/RES/58/32 (Dec. 8, 2003); G.A. Res. 59/61, U.N. Doc. A/RES/59/61 (Dec. 3, 2004); G.A. Res. 60/45, U.N. Doc. A/RES/60/45 (Jan. 6, 2006); G.A. Res. 61/54, U.N. Doc. A/RES/61/54 (Dec. 19, 2006); G.A. Res. 62/17, U.N. Doc. A/RES/62/17 (Jan. 8, 2008); G.A. Res. 63/37, U.N. Doc. A/RES/63/37 (Jan. 9, 2009); G.A. Res. 64/25, U.N. Doc. A/RES/64/25 (Jan. 14, 2010). (These resolutions have been based on the ongoing agenda item: "Developments in the field of information and telecommunications in the context of international security).

<sup>126</sup> Oona H, Rebecca C, Philip P, et al.(2012) The Law of Cyber-attack. The California Law Review 11(16): p. 48

<sup>127</sup> G.A. Res. 58/199, U.N. Doc. No. A/RES/58/199 (Jan. 30, 2004), and Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures, G.A. Res. 64/211, U.N. Doc. No. A/RES/64/211 (Mar. 17, 2010).

<sup>128</sup> U.N. G.A. Res. 57/53, U.N. Doc. A/RES/57/53 (Dec. 30, 2002).

follow up General Assembly resolution in 2002 called for further consideration and discussion of information security. The resolution called upon Member States to:

Promote further at multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field . . . [and] . . . Invite[ed] all Member States to continue to inform the Secretary-General of their views and assessments on the following questions:

- (a) General appreciation of the issues of information security;
- (b) Definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunications systems and information resources. . .<sup>129</sup>

The resolution also called for a new study of international informational security issues,<sup>130</sup> but little action resulted. It is noted that similar exhortations appear in subsequent resolutions.<sup>131</sup> The United Nations also sponsored The World Summit on the Information Society to further consider issues including information security, but again with little result.<sup>132</sup>

The United Nations did take a step forward in July 2010, when government cyber security specialists from fifteen countries including major cyber powers like the United States, China, and Russia submitted a set of recommendations to the U.N. Secretary General as “an initial step towards building the international framework for security and stability that these new technologies require.”<sup>133</sup> The recommendations called for:

- (i) Further dialogue among States . . .

---

<sup>129</sup>Ibid. at paragraph,1-2.

<sup>130</sup>Ibid. at para.4.

<sup>131</sup> U.N. G.A. Res. 58/32, at p.4; G.A. Res. 59/61, at p.4; G.A. Res. 60/45,at p. 4; G.A. Res. 61/54, at p.4; G.A. Res. 62/17, at p.4; G.A. Res. 63/37, at p.4; G.A. Res. 64/25, at p.4.

<sup>132</sup>U.N. G.A. Res. 60/252, U.N. Doc. A/RES/60/252 (Apr. 27, 2006).

<sup>133</sup> U.N. Doc. A/65/201 (July 30, 2010). (Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security), at para. 4.

- (ii) Confidence-building, stability and risk reduction measures ...including exchanges of national views on the use of [information and communication technologies] in conflict;
- (iii) Information exchanges on national legislation and national information and communications technologies security strategies and technologies, policies and best practices;
- (iv) Identification of measures to support capacity-building in less developed countries;
- (v) Finding possibilities to elaborate common terms and definitions.<sup>134</sup>

“Though vague, these recommendations represent real progress in overcoming a long impasse between the United States and Russia over how to address cyber security issues.”<sup>135</sup> The cooperation may even suggest possibilities for a future multilateral treaty under the auspices of the United Nations, which Russia has been advocating for some time.<sup>136</sup> At the present, however, the role of the United Nations with respect to cyber security remains largely limited to discussions and informational sharing.

As for North Atlantic Treaty Organization (NATO), it only recently began to address the threat of cyber attacks. NATO did little in response to the 2007 cyber attack on Estonia, laying bare that it “lacked both coherent cyber doctrine and comprehensive cyber strategy.”<sup>137</sup> On the heels of that attack,<sup>138</sup> NATO held its first meeting “the 2008 Bucharest Summit” to formally

---

<sup>134</sup> Ibid at 8

<sup>135</sup> Oona, H, Rebecca, C, Philip, P, et al. Op.cit, 236, at p.50

<sup>136</sup> John, M, *Step Taken to End Impasse Over Cybersecurity Talks*, N.Y. TIMES, July 16, 2010, Retrieved December 13, 2014 from [http://www.nytimes.com/world/17cyber.html?\\_r=1](http://www.nytimes.com/world/17cyber.html?_r=1).

<sup>137</sup> Hughes, Rex.B (Apr. 2009), *NATO and Cyber Defence: Mission Accomplished?*, ATLANTISCH PERSPECTIEF, at p.1, Retrieved December 12, 2014 from <http://www.atlcom.nl/site/english/nieuws/wp-content/Hughes>.

<sup>138</sup> NORTH ATLANTIC TREATY ORGANISATION.(NATO) NEWS (May 14, 2008), Retrieved December 14 2014 from [http://www.nato.int/docu/update/2008/05\\_may/e0514a.html](http://www.nato.int/docu/update/2008/05_may/e0514a.html). (This followed an October 2009 meeting of NATO defense ministers after which they called for the development of a NATO cyber defense policy. NATO Opens New Centre of Excellence on Cyber Defence.)

address cyber-attacks. This summit prompted the creation of two new NATO divisions focused on cyber-attacks: the Cyber Defence Management Authority and the Cooperative Cyber Defence Centre of Excellence.<sup>139</sup>

The Cyber Defence Management Authority aims to centralize cyber defense capabilities across NATO members. Although little information is publicly available, the Authority is believed to possess real time electronic monitoring capabilities for pinpointing threats and sharing critical cyber intelligence in real time with the goal of eventually becoming an operational war room for cyber defense.<sup>140</sup> The Cooperative Cyber Defence Centre of Excellence aspires to “advance the development of long term NATO cyber defence doctrine and strategy.”<sup>141</sup> The North Atlantic Council, however, retains control of NATO cyber policy and defense.<sup>142</sup> Despite some pressure from Eastern European countries, cyber attacks still only activate Article 4 of the NATO treaty, which calls upon members to “consult together” in cases of cyber attacks, but does not bind them to “assist” each other, as would be required under Article 5.<sup>143</sup>

Although NATO’s creation of these two divisions signify concrete progress and recognition of the need for a more coherent cyber strategy, concerns persist that “these teeth may not be sufficiently sharp to ward off any mischievous cyber bears or other e-adversaries seeking to compromise or destroy NATO digital assets deployed in either the Euro-Atlantic community or the ‘near abroad.’<sup>144</sup> NATO’s cyber plans and capabilities are still nascent.

---

<sup>139</sup> Scott J. Shackelford, *Estonia Two-and-a-Half Years Later: A Progress Report on Combating Cyber Attacks*, *Journal of Internet Law*. (5),37, Retrieved December 14, 2014 from <http://ssrn.com/abstract=1499849>.

<sup>140</sup> Hughes, R.B. Op.cit P.239, at p.2.

<sup>141</sup> *Ibid*

<sup>142</sup> North Atlantic Treaty Organization. News, (Jan. 29, 2009,) *Defending Against Cyber Attacks*, Retrieved December 13, 2014 from [http://www.nato.int/issues/cyber\\_defence/index.html](http://www.nato.int/issues/cyber_defence/index.html).

<sup>143</sup> North Atlantic Treaty, arts. 4 and 5;

<sup>144</sup> Hughes, R.B. Op.cit p239, at p.5.

The position of Europe in all of these was very clear. The Council of Europe has taken the most direct approach to regulating a subset of the cyber security problem in particular, cyber crime of any international organization to date. As the first international treaty on crimes committed using the Internet and other computer networks, the 2001 Council of Europe Convention on Cybercrime (“Cybercrime Convention”) promulgated “a common criminal policy aimed at the protection of society against cybercrime,” primarily through legislation and international cooperation.<sup>145</sup> The United States ratified the Convention in 2006. The convention allows members of the Council of Europe and other invited states (among them the United States) to join the Convention.<sup>146</sup> As of November 2010, thirty countries have ratified the Convention on Cybercrime, and another 16 have signed but have not yet ratified it (including Australia, Japan, and South Africa).<sup>147</sup>

Cyber attacks implicate the Cybercrime Convention’s offenses relating to confidentiality, integrity, and availability of computer data and systems particularly illegal access, data interference, and system interference.<sup>148</sup> These rules, however, do not appear to apply to government actions, whether taken for law enforcement or national security purposes.<sup>149</sup> For example, Article 2 of the Convention requires that states adopt “legislative and other measures ...to establish as criminal offenses under [their] domestic law, when committed intentionally, the access to the whole or any part of a computer system *without right*.”<sup>150</sup> The Convention’s

---

<sup>145</sup> Council of Europe, ETS No. 185, Convention on Cybercrime, pmbl., Budapest (Nov. 23, 2001), entered into force July 1, 2004, available at <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>, accessed, 10/12/2014, 9.20pm, see also Rasha AlMahroos, (2008). *Privacy on the Internet and in Organizational Database: Phishing for the Answer: Recent Developments in Combating Phishing*, Journal of Law & POL’Y FOR INFO. SOC’Y 3 I/S: pp. 595- 613

<sup>146</sup> Declan M & Anne B, (Apr. 4, 2006, )*Senate Ratifies Controversial Cybercrime Treaty*, CNET NEWS, Retrieved December 12, 2014 from [http://news.cnet.com/Senate-ratifies-controversial-cybercrime-treaty/2100-7348\\_3-6102354.html](http://news.cnet.com/Senate-ratifies-controversial-cybercrime-treaty/2100-7348_3-6102354.html).

<sup>147</sup> Council of Europe, Convention on Cybercrime, Retrieved December 12, 2014 from <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>.

<sup>148</sup> Council of European Cybercrime Convention, at articles. 2, 4, 5.

<sup>149</sup> Arie J. Schaap, (2009) *Cyberwarfare Operations: Development and Use Under International Law*, Air Force. Law. Review. 171 ( 64);127 and 171.

<sup>150</sup> Council of Europe Cybercrime Convention, Op.cit, p240 at Article. 2

accompanying “explanatory report” clarifies that the “without right” caveat allows for classic legal defenses, such as self defense or necessity, but also “leaves unaffected conduct undertaken pursuant to lawful government authority” including acts to “maintain public order, protect national security or investigate criminal offences.”<sup>151</sup> This suggests that the Convention negotiators were aware of state interests in using cyber attacks and sought to draft the agreement to permit such governmental action.

Nonetheless, the Cybercrime Convention may still impose limited constraints on the execution of cyber attack operations by ratifying countries. Parties to the Convention have agreed to “co-operate with each other ...to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data.”<sup>152</sup> Although not explicit, this agreement to cooperate could limit the extent to which parties to the Convention could conduct cyber attacks against other state parties, since that would undermine the overall intent of the agreement. It is unclear, however, what consequences or repercussions would result from such a breach of the Convention’s intent and purpose by a state party.

For these reasons, the Convention, the most developed international legal framework directly regulating cyber attacks again addresses only a portion of the overall challenge. It is limited, in particular, both by its failure to regulate most attacks by state parties and by its largely regional membership. Yet it offers a starting point for thinking about a comprehensive international framework for regulating unlawful cyber attacks.

The Organization of American States (“OAS”) only recently began taking action to regulate cyber attacks. In April 2004, the OAS approved a resolution stating that member states

---

<sup>151</sup> Council of Europe, (Nov. 8, 2001), C.E.T.S. No. 185, Convention on Cybercrime: Explanatory Report, para. 38. Retrieved December 12, 2014 from <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>

<sup>152</sup> Council of Europe Cybercrime Convention, Op.cit, p240 at Article. 23.

should “evaluate the advisability of implementing the principles of the Council of Europe Convention on Cybercrime (2001)” and should “consider the possibility of acceding to that convention.”<sup>153</sup>The OAS also adopted a Comprehensive Inter American Cyber security Strategy, which aims, among other things, to adopt “cyber crime policies and legislation that will protect Internet users and prevent and deter criminal misuse of computers and computer networks, while respecting the privacy and individual rights of Internet users.”<sup>154</sup>To this end, the OAS agreed to deploy an Experts Group that will “provide technical assistance to member states in drafting and enacting laws that punish cyber crime, protect information systems, and prevent the use of computers to facilitate illegal activity.”<sup>155</sup>These experts only offer guidance; the OAS is not promulgating a set of uniform laws with which member states can combat cyber crime and cyber attacks.

At a January 2010 meeting, the OAS Working Group on Cyber Crime recommended that “member that had not already done so establish state bodies for investigating and prosecuting cyber crimes and adopt domestic legislation criminalizing cyber crime and enabling international cooperation to investigate and prosecute such crimes.”<sup>156</sup> “The Working Group pledged to review the progress made in implementing these measures at its next meeting.”<sup>157</sup> The OAS has begun a useful regional conversation on joint strategies for battling the portion of cyber attacks that constitute cyber crime. Yet it has not yet developed a more active program for addressing cyber attacks more generally.

---

<sup>153</sup> Organization of American States (June 8, 2004), IV(8), AG/RES. 2040 (XXXIV-O/04) Retrieved December 12, 2014 from [http://www.oas.org/juridico/english/ga04/agres\\_2040.htm](http://www.oas.org/juridico/english/ga04/agres_2040.htm).

<sup>154</sup> Organization of American States, , AG/RES. (2004) (XXXIV-O/04), *A Comprehensive Inter-American Cybersecurity Strategy: A Multi-Dimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity*, Appendix A, adopted June 8, 2004. Retrieved December 12, 2014 from [http://www.oas.org/XXXIVGA/english/docs/approved\\_documents/adoption\\_strategy\\_combat\\_threats\\_cybersecurity.htm](http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm)

<sup>155</sup> *Ibid*, at Appendix A.

<sup>156</sup> The Working Group on Cyber-Crime, (Jan, 2010,) OEA/Ser.K/XXXIV, CIBER-VI/doc.4/10 rev.1 Sixth Meeting, held in Washington D.C., Retrieved December 10 2014 from [http://www.oas.org/juridico/english/cyb\\_VIrec\\_en.pdf](http://www.oas.org/juridico/english/cyb_VIrec_en.pdf).

<sup>157</sup> *Ibid*, at para. 17.

One group that cannot be left out in this discussion is the Shanghai Cooperation Organization. The Shanghai Cooperation Organization also has taken significant preliminary steps toward cooperation in the cyber security area. In its Yekaterinburg Declaration of June 16, 2009, “the SCO member states stressed the significance of the issue of ensuring international information security as one of the key elements of the common system of international security.”<sup>158</sup> The Organization presents a possible center of gravity in international legal action on cyber attacks. As explained above, the Organization has thus far adopted an expansive vision of cyber attacks to include the use of cyber technology to undermine political stability. As such, it represents a model that is likely to be at odds with that of Europe and the United States, which have sought to avoid regulations of cyber activities that may interfere with the expression of political dissent.

As this sub head reveals, international efforts to regulate cyber attacks are still at an embryonic stage. With the possible exception of the Council of Europe’s Convention on Cybercrime, most international agreements have not proceeded beyond the stage of discussing future strategies. Nonetheless, the widespread efforts demonstrate increasing interest in establishing a set of transnational regulations to address cyber attacks. The diversity of approaches taken by these organizations also demonstrates that the central challenge at least initially will be defining the scope of the activity that should be addressed in an international agreement.

It is instructive to note that there are several international legal frameworks that are not directly aimed at cyber attacks but nonetheless regulate means that may be used in or may be a focus of a cyber attack. These include, most notably, the international law governing

---

<sup>158</sup> Shanghai Cooperation Organization, (July 9, 2009), Yekaterinburg Declaration of the Heads of the Member States of the Shanghai Cooperation Organization, Consulate General of Uzbekistan in New York City Retrieved December 13 2014 from <http://www.uzbekconsulny.org/news/572/>.

telecommunications, aviation, space, and the law of sea. These legal regimes were largely formed prior to the emergence of cyber attacks and therefore do not expressly regulate or prohibit cyber attacks. Instead, these frameworks implicate cyber attacks only so long as an attack employs the particular means regulated by the agreement. For this reason, “legal scholarship on cyber security has suggested that these bodies of international law can be used to address cyber attacks.”<sup>159</sup> Yet it is observed, once again, that these existing legal regimes provide a patchwork of laws that are likely to apply to only a small number of harmful cyber attacks.

At the domestic level, the United States domestic law, particularly domestic criminal law offers an important tool for combating cyber attacks, including those that cross international borders. Indeed, given the limited applicability of the law of war and other international legal frameworks, domestic laws addressing cyber attacks are often the best available option. “Unfortunately, the existing response to cyber attack in the domestic law of the United States and other states has for the most part not been updated to address the novel modern challenges posed by cyber attacks.”<sup>160</sup> It is also severely limited by its lack of extraterritorial reach.

Although there is no U.S. federal statute that directly criminalizes cyber attacks, the primary domestic legal tool for addressing cyber attacks is criminal law. In addition to liability through criminal law, there have been some proposals for the use of tort law to allow for civil liability for cyber attackers, or for intermediaries who are negligent in facilitating cyber attack.

Such proposals face a number of serious challenges, however, including attribution and jurisdictional problems, and, for intermediaries, causation problems and a virtual tax on

---

<sup>159</sup> Scott J. (2009) *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, BERK. Journal of International Law (27):192, Richard .A (Fall 1996), *The International Legal Implications of Information Warfare*, Airpower Journal. available at <http://www.au.af.mil/au/awc/awcgate/au/aldrich.pdf>; accessed 13/12/2014, Jason Barkham, (2001), *Information Warfare and International Law on the Use of Force*, New York University Journal of International Law & Policy (34):57, David W, (2009), *A Global Problem: Cyberspace Threats Demand an International Approach*, ISSA Journal. Aug. Retrieved December 13, 2014 from <http://www.issa.org/Library/Journals/2009/August?Wilson> A%20Global%20Problem.pdf;

<sup>160</sup> Matthew J. Sklerov, (2009). *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect their Duty to Prevent*, Mill, Law Review. 201(1), at p.6 (“Unfortunately, state responses to cyberattacks are governed by an anachronistic legal regime that impairs a state’s ability to defend itself.”).

technophobia, punishing those who do not know enough about protecting their personal computers. “Moreover, if software designers were held liable for leaving their products vulnerable to cyber attack, software costs could increase substantially.”<sup>161</sup> At the federal level, “criminal laws address fraud involving devices, computers, or e-mail”,<sup>162</sup> “malicious interference in communications lines, stations, or systems,”<sup>163</sup> “electronic communication interception,”<sup>164</sup> “illicit access to electronic communications and records,”<sup>165</sup> and “recording of dialing, routing, addressing, and signaling information”.<sup>166</sup>

The majority of the existing criminal laws bearing on cyber attack do not apply extraterritorially that is, they do not reach criminal activity occurring outside the United States. There is generally a presumption against extraterritorial application of federal law.<sup>167</sup> Nevertheless, “Congress has the authority to enforce its laws beyond the territorial boundaries of the United States,” and may do so by evidence of its intent as gauged through statutory interpretation.<sup>168</sup> In certain cases, extraterritorial reach may also be extended without explicit or implied Congressional authorization based on detrimental effects in the United States.<sup>169</sup> It is noted that the intent to cause effects within the United States makes it reasonable to apply to persons outside United States territory a statute which is not extraterritorial in scope. There are inherent limits to how much of the problem domestic law can reach, since domestic law can only be enforced against individuals that are within the jurisdiction of domestic law enforcement.

---

<sup>161</sup> Michael D. Scott, (2008), *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 Maryland Law Review p.425, Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace* 31-32, 53-58, Retrieved December 13, 2014 from [http://works.bepress.com/jay\\_kesan/4/](http://works.bepress.com/jay_kesan/4/).

<sup>162</sup> 18 U.S.C. sections, 1029, 1030, 1037 (2006). 18 U.S.C. sec. 1030 The Computer Fraud and Abuse Act.

<sup>163</sup> *Ibid.* sec. 1362.

<sup>164</sup> *Ibid.* sections. 2510-22.

<sup>165</sup> *Ibid.* sections, 2701-12.

<sup>166</sup> *Ibid.* sections, 3121-27.

<sup>167</sup> *United States v Cotton*, (1973). 471 F.2d 744, 750 (9th Cir.)

<sup>168</sup> *Equal Opportunity Empl. Comm. v. Arabian American Oil Co.*, (1991) 499 U.S. 244, 248

<sup>169</sup> *United States v Muench*, 694 F.2d 28, 33 (2d Cir. (1982) 694 F.2d 28, 33 (2d Cir.)

There are, however, some exceptions to that rule. For example, the criminal statute banning access device fraud, as amended by the USA PATRIOT Act of 2001, provides that:

Any person who, outside the jurisdiction of the United States, engages in any act that, if committed within the jurisdiction of the United States, would constitute an offense under . . . this section, shall be subject to the fines, penalties, imprisonment, and forfeiture provided in this title if:

- (1) the offense involves an access device issued, owned, managed, or controlled by a[n] . . . entity within the jurisdiction of the United States; and
- (2) the person transports, delivers, conveys, transfers to or through, or otherwise stores, secrets, or holds within the jurisdiction of the United States, any article used to assist in the commission of the offense or the proceeds of such offense or property derived there from.<sup>170</sup>

The statute banning computer fraud was also amended as part of the USA PATRIOT Act to provide for extraterritorial applicability.<sup>171</sup> “The term ‘protected computer’ [to which this statute applies] means a computer . . . which is used in interstate or foreign commerce or communications, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.”<sup>172</sup> Both of these statutes may serve as useful models for extending extraterritorial application to other domestic laws related to cyber attack.

Several recent legislative efforts in the United States tackle pieces of the cyber attack threat not addressed by criminal law. These include the Cyber security Enhancement Act,<sup>173</sup> the Executive Cyberspace Authorities Act of 2010,<sup>174</sup> the Rockefeller Snowe Cyber security Act,<sup>175</sup>

---

<sup>170</sup> 18 U.S.C. sec. 1029 (2006), U.S. Dept. of Justice, Prosecuting Computer Crimes at 94, (Scott Eltringham ed., 2007), Retrieved December 13, 2014 from <http://www.justice.gov/criminal/cybercrime/ccmanual/index.html>.

<sup>171</sup> 18 U.S.C. sec.1030 (2006)

<sup>172</sup> U.S. Dept. of Justice, Prosecuting Computer Crimes, Op cit, p140, at p.94.

<sup>173</sup> Oona H, et-al, Op.cit, p.236, at p.66

<sup>174</sup> Ibid

<sup>175</sup> Ibid

the International Cyberspace and Cyber security Coordination Act of 2010<sup>176</sup> and the Protecting Cyberspace as a National Asset Act of 2010.<sup>177</sup> The most widely discussed of these efforts has been the Protecting Cyberspace as a National Asset Act, co-written by Senators Lieberman, Collins, and Carper, which was introduced in the Senate and the House of Representatives in June 2010.<sup>178</sup>

The bill builds on the military's recent establishment of the United States Cyber Command<sup>179</sup> by proposing the establishment of an Office of Cyberspace Policy in the White House and a National Center for Cyber security and Communications in the Department of Homeland Security.<sup>180</sup> The bill also addresses a wide range of related cyber security matters, including cyber security definitions and federal information security management provisions.<sup>181</sup>

The bill has become caught up in a vigorous debate over the proper role of the government in regulating cyberspace. Dubbed the "kill switch bill" by opponents, the bill came to be seen as an effort to grant the president emergency powers over certain Internet communications.<sup>182</sup> The bill has since been reintroduced with changes meant to prevent the government from using a "kill switch" to shut off internet service as a political tool.<sup>183</sup>

Had it passed into law, the bill would likely have put in place more checks on the president's power to respond to cyber emergencies than currently exist.

---

<sup>176</sup> Ibid

<sup>177</sup> Ibid

<sup>178</sup> Ibid

<sup>179</sup> William H. McMichael, (May 22, 2010), *DoD Cyber Command Is Officially Online*, Army Times Retrieved December 14, 2014 from [http://www.armytimes.com/news/2010/05/military\\_cyber\\_command\\_052110/](http://www.armytimes.com/news/2010/05/military_cyber_command_052110/).

<sup>180</sup> Oona, H et-al at. Op.cit, p 236, at, 66

<sup>181</sup> Ibid

<sup>182</sup> Emelie R, (June 25, 2010) *Senate Committee OKs Cybersecurity Bill on Majority Leader's Radar*, Defense Daily. Retrieved December 13, 2014 from <http://www.defensedaily.com/publications/dd/10568.html>.

<sup>183</sup> Diane B, (July 27, 2011), *Reid Pushes U.S. Republicans for Cybersecurity Bill*, Reuters. Retrieved December 13, 2014 from <http://www.reuters.com/article/2011/07/27/congress-cybersecurity-idUSN1E76Q1M320110727>.

“The bill has since been reintroduced in amended form, but has not yet proceeded to a vote on the Senate floor”.<sup>184</sup> This debate offers an important lesson for reformers. Any future law must clearly indicate what activities are to be covered, put in place a transparent and high bar for emergency measures, and address well founded concerns that efforts to strengthen cyber security might simultaneously weaken the free and open access to modern technology for those engaging in political speech and organizing same.

Other domestic legal efforts to address cyber attacks are either based in criminal law or have focused on building up U.S. defensive capabilities, but none of the recent legislative efforts that might strengthen defensive capacity against cyber attack has yet been made into law. Moreover, the existing domestic law framework is insufficient for addressing the larger global problem.<sup>185</sup> In particular, the lack of extraterritorial effect in most of the criminal laws that do exist to counter cyber attacks severely limits their ability to reach those initiating such attacks, who are often located outside the United States.

Given the transnational nature of cyber attacks challenge, international cooperation is likely to be necessary to provide a solution commensurate to the problem.<sup>186</sup> Therefore, this work will at this point discuss international cooperation, especially on Evidence Collection and Criminal Prosecution. The ability to distinguish cyber warfare from cyber attack will provides a common understanding of cyber attack that individual countries could incorporate into their own domestic criminal legislation. This strategy has been applied, for example, in the international

---

<sup>184</sup> Ibid

<sup>185</sup> Oona H, et-al, Op.cit, p. 236 at p.67

<sup>186</sup> Ibid at p.70

effort to battle bribery, the OECD Bribery Convention provides a definition of bribery that state parties then integrate into national legislation forbidding the practice.<sup>187</sup>

Under the Bribery Convention, “signatories pledged to criminalize and prosecute the bribery of foreign public officials.”<sup>188</sup> The thirty eight state parties have passed implementing legislation.<sup>189</sup> A defining declaration on cyber attack could similarly provide the content for domestic criminal legislation targeting the practice.

In addition to such loose coordination, an international treaty addressing cyber attacks should provide for more extensive cooperation among states on evidence collection and criminal prosecution of those involved in cyber attacks. A useful starting point for building a universal treaty is the Council of Europe Convention on Cybercrime, earlier described in this sub head of this work which provides for harmonized regulation of a wide range of cyber crimes, many of which might be utilized in cyber attacks.

This treaty remains largely limited to Europe (though the United States has ratified the agreement) and it does not address all cyber attacks that a comprehensive agreement would ideally regulate. Canada, Japan, and South Africa are the other non European signatories, but the United States is the only one of the four that has ratified the Convention.<sup>190</sup> Nonetheless, it provides a framework from which a more comprehensive agreement might begin.

Building on the framework established in the Council of Europe Convention, the new agreement should require parties to pass domestic laws banning the cyber attack related conduct

---

<sup>187</sup>Organisation for Economic Co-operation and Development, (Dec. 18, 1997) Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, 37. I.L.M. 1 (1998). Retrieved June 12, 2015 from [www.nyupress.org](http://www.nyupress.org).

<sup>188</sup> Developments in the Law, *Extraterritorial Law and International Norm Internalization*, (2011) Harvard Law Review. (124): pp.1280, 1285, Ibid, Bribery Convention, at art 1(1) (“Each Party shall take such measures as may be necessary to establish that [bribery] is a criminal offence under its law”).

<sup>189</sup> OECD Anti-Bribery Convention: National Implementing Legislation, OECD, [http://www.oecd.org/document/30/0,3746,en\\_2649\\_34859\\_2027102\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/30/0,3746,en_2649_34859_2027102_1_1_1_1,00.html). (Unfortunately, it appears that few countries have actually been enforcing the domestic anti-bribery provisions.) Accessed, 12/06/2015, Developments in the Law, *Extraterritorial Law and International Norm Internalization*, (2011). Harvard Law. Review. (124): Pp.1280, 1285

<sup>190</sup> Council of Europe Convention on Cybercrime, *Chart of Signatures and Ratifications*, Retrieved June 13, 2015 from <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>.

prohibited under the treaty, so as to harmonize laws across states. The agreement could begin with the information sharing program, layering on additional mechanisms for fostering cooperation in identifying and stopping the sources of cyber attacks through criminal law enforcement agencies.

Member states should also be granted access to cyber related information that would not be available to non members. Information sharing would not only give states an incentive to commit to limiting their resort to armed force, but it might also aid states in identifying the source of cyber attacks. This technical challenge is a fundamental limitation of the legal framework governing cyber attack and it is essentially a problem of information. The more information that is available to states regarding sources and locations of cyber threats, the easier it will be to prevent cyber attacks. International cooperation in information sharing could be an extremely valuable complement to other regulation of cyber attack.

Finally, consistent with the Tunis Commitment<sup>191</sup> and Agenda,<sup>192</sup> a treaty could provide a foundation that would allow more technologically developed countries to assist less developed ones in responding to shared cyber threats. As the recent White House Cyberspace Strategy memo observed,

Enhancing national-level cyber security among developing nations is of immediate and long term benefits [to the United States and all nations], as more states are equipped to confront threats emanating from within their borders and in turn, build confidence in globally interconnected networks and cooperate across borders to combat criminal misuse of information technologies. It is also essential to cultivating dynamic, international research communities able to take on next generation challenges to cyber security.<sup>193</sup>

---

<sup>191</sup> World Summit on the Information Society, Tunis Commitment, Retrieved December 19, 2014 from <http://www.itu.int/wsis/docs2/tunis/off/7.html>.

<sup>192</sup> World Summit on the Information Society, Tunis Agenda for the Information Society, Retrieved December 19 2014 from <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>.

<sup>193</sup> International Strategy for Cyberspace, White House 5 (May, 2011), Retrieved December 14 ,2014 from [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/international\\_strategy\\_for\\_cyberspace.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf).

The White House's recent strategy paper on cyberspace addresses the danger that efforts to reduce cyber attacks could stifle free speech. It notes that "the ability to seek, receive, and impart information and ideas through any medium and regardless of frontiers has never been more relevant" and urges that "exceptions to free speech in cyberspace must also be narrowly tailored."<sup>194</sup> Protecting fundamental freedoms and privacy is one of the White House's seven high level policy priorities for cyberspace, and one of the three law enforcement policy priorities is to "[f]ocus cybercrime laws on combating illegal activities, not restricting access to the internet."<sup>195</sup>

Any country's cyber security can be compromised by its allies' security gaps,<sup>196</sup> therefore any attempt to prevent cyber attacks must include some efforts to improving the defenses of other countries as well.

Establishing common legal standards for cyber attacks creates a danger of over criminalization that could be used to quash legitimate dissent in some signatory states.<sup>197</sup> Any new universal treaty must therefore ensure that criminalization of cyber attacks is not used to limit legitimate dissent. So long as cyber attacks are carefully defined, as proposed at the outset of this sub head this problem should be largely preventable.

There remain other significant challenges that will have to be overcome in the effort to achieve a comprehensive cyber treaty. Indeed, some have suggested "a successful treaty may be nearly impossible to achieve, at least in the short term".<sup>198</sup> "[N]ot only do certain features of cyber-activities make international legal regulation very difficult, but major actors also have divergent strategic interests that will pull their preferred doctrinal interpretations and aspirations

---

<sup>194</sup> Ibid, at, paragraph. 23-24.

<sup>195</sup> Ibid, at, paragraphs.15, 20.

<sup>196</sup> Oona H, et-al, at, Op.cit,p.236, at,74

<sup>197</sup> Ibid

<sup>198</sup> Matthew C. Waxman, (2011). *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE Journal of International Law (36) : at 425-26

in different directions, impeding formation of a stable international consensus.”<sup>199</sup> This paper has argued that:

The fundamental clash of interests concerning the regulation of electronic communications, the deep constraints the United States would have to adopt to receive reciprocal benefits in a cyber security treaty, and the debilitating verification problems will combine to make it unfeasible to create a cyber security treaty that purports to constrain governments.<sup>200</sup>

In all of these, a scholar however has a dissenting view on the appropriate international response to cyber attack, he argued “for a duty to assist cyber-threat victims, rather than regulation of bad cyber-actors.”<sup>201</sup> First and foremost, it will be necessary to bridge fairly substantial divides between the United States and other leading cyber powers that have a more expansive view of what activity ought to be criminalized through international cooperation. Russia, for example, has been promoting an international agreement banning cyber attack for some time. John Markoff & Andrew E. Kramer, had said in a publication: “We are not the first to propose a cyber-attack treaty. Russia has for some time been proposing a treaty banning cyber-attack, though that proposal focuses on activity quite different from that addressed in the Council of Europe agreement.”<sup>202</sup> However, the character of the perceived threat it seeks to address is quite different in character from that addressed by the Council of Europe Convention on Cybercrime. In addition, a comprehensive treaty will have to address difficulties of appropriate verification.<sup>203</sup> Nonetheless, the effort is necessary. As General Keith Alexander,

---

<sup>199</sup> Jack Goldsmith, (Aug. 10, 2011.)What is the Government’s Strategy for the Cyber-exploitation Threat, Retrieved December 18, 2014 from Lawfareblog.com, at.p.12.

<sup>200</sup> Ibid

<sup>201</sup> Duncan B. Hollis, (2011) *An E-SOS for Cyberspace*, Harvard International Law Journal (52): at, 373

<sup>202</sup> John Markoff & Andrew E. Kramer, (June 27, 2009,) *U.S. and Russia Differ on a Treaty for Cyberspace*, N.Y. TIMES. Retrieved December 12, 2014 from <http://www.nytimes.com/2009/06/28/world/28cyber.html>.

<sup>203</sup> Op.cit, 107. Jack Goldsmith, at.pp.10-12.

chief of the new U.S. Cyber Command, recognized, “[w]e do have to establish the lanes of the road” for what cyber-activities governments can and cannot pursue.”<sup>204</sup>

The emergence of Stuxnet<sup>205</sup> last year heralded a new era for cyber attacks. Although the damage it caused was apparently limited to the Iranian nuclear program at which it was aimed, the vulnerabilities it revealed were immense. By the time it was discovered, Stuxnet had wormed its way into computer networks around the world, including, by some estimates, nearly half of those running electric utilities.<sup>206</sup>

Cyber attacks on vital infrastructure are already becoming widespread. Cyber security professionals report that the computer infrastructure has become more vulnerable even in just the past year. Citing a global survey of 200 computer security professionals working in critical infrastructure industries, “In the Dark: Crucial Industries Confront Cyber attacks”.<sup>207</sup> And yet, while the threat of cyber attacks has rapidly grown, the response has not kept pace. This work has shown that both the U.S. government and the international community at large have thus far largely achieved only a little in updating the legal framework for responding to cyber attacks. To face the new and growing threats, governments continue to rely on limited and piecemeal bodies of law not designed to meet modern threats.

It is past time to begin a conversation about the scope of the threat posed by cyber attacks and the best ways to meet it. By expanding the reach of domestic law abroad and developing a system for utilizing limited countermeasures, where appropriate, the United States can expand its capacity to battle this new threat. Yet the United States is restricted in what it can accomplish

---

<sup>204</sup> Siobhan Gorman, (June 4, 2010,) *U.S. Backs Talks on Cyber Warfare*, Wall Street Journal., Retrieved December 12, 2014 from <http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html>.

<sup>205</sup> “STUXNET” is a computer worm that was discovered in June 2010. It was designed to attack industrial programmable logic controllers( PLCs)

<sup>206</sup> Siobhan Gorman,Op.cit,p.253

<sup>207</sup> Mark Clayton, (2011, April 20,) *Security Lags Cyberattack Threats in Critical Industries, Report* Christian Science Monitor, p.3

alone. Cyber attacks are quintessentially transnational often designed by authors in multiple countries, run through networks across the world, undermining a computer system in a country where those designing the attack have never set foot. This global threat may only be effectively met by a global solution by the international community working together to design a new law for cyber attacks.

Every criminal justice profession and association has "codes" of ethics, "canons" of professional responsibility, "statements" of values, "principles" of conduct, "standards" of practice, and "oaths" of office, along with "pledges", "vows", "maxims", "credos", "prayers", "tenets", and "declarations". Some are directed to God, others to superiors or the profession, and still others to society as a whole. They all make promises that people commit to keeping as a standard of performance.

A code of ethics if it is to be used for occupational purposes must set a standard above ordinary morality. Otherwise there's no need for a code of ethics at all. This is especially relevant to police work where it's going to take more than just a commitment to being an ordinary, decent human being.

The ethically ideal police system would be one with integrity and nothing puzzling about it for instance, there would be no corruption nor misconduct. There would be no us against them and no disrespect for the limits of the law or how it's enforced. Everything done in private would be just as if it was done in public. Mistakes would be treated as learning opportunities but there would be less of them because of widespread adherence to the values of probity, propriety, restraint, reasonableness, and caution. Recruitment, selection, and training mechanisms would be flawless, with promotion on the basis of merit, no one being without ample supervision and the organization giving its personnel whatever resources they need to perform their work better.

There would be "open door" policies to the public, academics and the media. Nothing the police do or how they do it would come as a surprise to anyone.

The commitment to a code of ethics is unconditional. You don't lower your ideals or revise your mission statement just because circumstances in the environment have changed. The true test of character is keeping your faith in the face of adversity. There are few professions that demand so much moral fiber as policing. Police stand in "harm's way" not so much against enemies with bullets but against enemies skilled in every form of trickery, deceit, feigned ignorance, and deception. That's why the Law Enforcement Code of Ethics published by the International Association of Chiefs of Police, stands as a spirited reminder to the higher order of this calling.

It's often said that no other profession demands a higher ethical standard than that of law enforcement. Regardless of whether or not there are other careers that require a similar dedication to doing the right thing, it is undeniable that there is an understandably tremendous degree of expectations placed upon police officers, and rightly so.

Every officer knows, or at least should know by now, that they live in the eyes of the public. Friends, relatives, neighbors and strangers watch every move law enforcement officers make, both on and off duty. The fact is that the public scrutinizes police officers more than most other professions, either because they're cynical or hope to catch them committing mistakes or because they're hopeful and are looking for a good example and a strong leader. In either case, it's up to the officer to be above reproach in both his public and private life.

Yet day in and day out, stories of officers who do wrong are being published. Theft, excessive use of force, misuse of public office, abuse of authority, and even simple things like

speeding, are all examples of unethical behavior on the part of those that the public has entrusted to serve and protect them.

It must be noted that the vast majority of police officers are truly good, hard working and dedicated people who strive to serve the public and do the right thing at every turn. It's unfortunate, but the good work law enforcement does rarely make news, and when it does, it doesn't carry with it the same long memory that bad news seems to.

Unfortunate though it may be, a single awkward act committed by a single unprofessional officer can impact the entire law enforcement profession. Rarely does the public make a distinction between uniforms, at the end of the day, all police officers look and act the same in the eyes of the average citizen. That's why it is so vitally important that each and every officer does her utmost best to maintain and build on the trust that the public has given her, instead of squandering it simply for the sake of bravado, greed or self gratification.

There is no doubt that it is important to have a strong legal framework for the security sector. A sound legal framework is a precondition for effective, efficient and accountable security sector governance because:

- i. It defines the role and mission of the different security organizations;
- ii. Defines the prerogatives and limits the power of security organizations and their members;
- iii. Defines the role and powers of institutions, which control and oversee security organizations;
- iv. Provides a basis for accountability, as it draws a clear line between legal and illegal behaviour;

- v. Enhances public trust and strengthens legitimacy of government and its security forces.

For all these reasons, security sector reform often starts with a complete review and overhaul of the national security sector legislation. The point is to identify and address contradictions and the lack of clarity regarding roles and mandates of the different institutions.

Across the globe, there is a standard practice of performing police duties. All over the world, police officials or officers are expected or bound to carry out their duties under some important international instruments, rules and codes, such as the United Nations Declaration of Human Rights 1948, The Torture Convention 1987, the United Nations Code of Conduct for Law Enforcement Officials and the Guidelines for the Effective Implementation of the Code of Conduct for Law Enforcement officials adopted by Resolution of 34/169 of the U.N. General Assembly on 17<sup>th</sup> December, 1979. International standards relating to human rights in law enforcement have been promulgated by a number of bodies within the United Nations system. Foremost among these bodies have been the Commission on Human Rights, its sub-Commission on prevention of Discrimination and Protection of Minorities, and the periodic United Nations Congress on the prevention of crime and the Treatment of Offenders. The adoption of these standards by the General assembly and the Economic and Social Council, two principal organs of the United Nations, has given them the character of universality, to the extent that “they are accepted by the international community as a whole as the minimum rules for law enforcement, regardless of the legal system or municipal law framework of the member State.”<sup>208</sup> The law is

---

<sup>208</sup> United Nations Human Rights and Law Enforcement, A manual on Human Rights Training for Police (Professional Training Series No.5) at p.25

not administered in vacuum, “police must carry out their duties within the context of the prevailing economic realities faced by the people they are sworn to serve and protect”.<sup>209</sup>

---

<sup>209</sup> Ibid at p.27

## CHAPTER FIVE

### PROBLEMS AND CHALLENGES OF LAW ENFORCEMENT AGENCIES IN SECURING AND PROTECTING CYBERSPACE AGAINST CYBERCRIME

#### 5.1 Introduction

Internet provides space for a wide range of human activities. This, in turn, leads to a potentiality of disputes arising which fall under the domain of various branches of law. The principles of law for determining jurisdiction and applicable law could vary depending on the nature of the dispute and under which branch of law it falls. The dependence of society on ICTs is not limited to the western countries<sup>1</sup>. Developing countries also face challenges in preventing attacks against their infrastructure and users.<sup>2</sup> The development of cheaper infrastructure technologies such as WiMAX<sup>3</sup> has enabled developing countries to offer Internet services to more people. Developing countries can avoid the mistakes of some western countries, which have concentrated mainly on maximizing accessibility, without investing significantly in protection. US experts have explained that successful attacks against the official website of governmental organizations in Estonia<sup>4</sup> could only take place due to inadequate protection measures.<sup>5</sup> 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

---

<sup>1</sup> Organization for Economic Cooperation and Development (OECD) (2005, 26, May) Spam Issues In Developing Countries. Retrieved June 2, 2015 from <http://www.oecd.org/dataoecd/5/47/34935342.pdf>. ( With regard to the effect of spam on developing countries)

<sup>2</sup> International Telecommunication Union (ITU) (2007) Creating Trust in Critical Network Infrastructures . (Chairman's Report on Workshop Regarding the integration of developing countries in the protection of network infrastructure) Retrieved June 2, 2015 from <http://www.itu.int/osg/spu/ni/security/docs/cni.10.pdf>;

<sup>3</sup> WiMAX (Worldwide Interoperability for Microwave Access) is a technology that provides wireless data services over long distances. The WiMAX Forum, Retrieved June 2, 2015 from <http://www.wimaxforum.org> Andrews, Ghosh, Rias, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking", Nuaymi, WiMAX Technology for Broadband Wireless Access.

<sup>4</sup> Toth, (2013 October, 1) Estonia Under Cyberattack. Retrieved June 2, 2015

from [http://www.cert.hu/dmdocuments/Estonia\\_attack2.pdf](http://www.cert.hu/dmdocuments/Estonia_attack2.pdf) 125. (Regarding the attack that befell Estonia in 2007)

<sup>5</sup> See: Waterman, (2007) Who Cyber smacked Estonia. Analysis: In United Press International. Retrieved June 2, 2015 from: [http://www.upi.com/Security\\_Terrorism/Analysis/2007/06/11/analysis\\_who\\_cyber\\_smacked\\_estonia/2683/](http://www.upi.com/Security_Terrorism/Analysis/2007/06/11/analysis_who_cyber_smacked_estonia/2683/).

later point may prove more expensive in the long run.<sup>6</sup> 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. This chapter shall outline the challenges of law enforcement agencies in securing cyberspace against cybercrime.

## **5.2 Problems of Information Gathering and Sharing Relating to Cyber Techniques**

The Internet puts into question long established notions about how to investigate crime and enforce criminal law. It has led to an increasing emphasis on decentralization of intelligence gathering, privatization of enforcement, and delegation of powers to non governmental entities. To address the problem of cybersecurity, technologists, businesspeople, and government officials have experimented with public and private collaborations, self-help measures, automated enforcement, community vigilance, and collective sanctions, leading to what may well become a new system of law enforcement. But it is noted that this new model is not without its own problems. First, how can we protect civil liberties and constitutional rights when intelligence gathering is decentralized, when prevention and self-help are strategies of first resort, and the criminal law is increasingly enforced by private parties; second, how will incentive change when sanctions are invisible, decentralized, and privatized, thirdly, what is the proper role of community in sanctioning bad behavior and how can we design technology to strengthen appropriate collective enforcement and discourage inappropriate methods; fourth, what are the long-term consequences of replacing human judgment and prosecutorial discretion with automated sanctions. All these questions, regrettably, still beg for answers.

---

<sup>6</sup> ITU (2007) World Information Society Report, (Regarding Cybersecurity in developing countries). Retrieved June 2, 2015 from [http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07\\_full-free.pdf](http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf).

This however, should not pose any problem to Nigeria to the extent that Nigeria has a long standing intelligence gathering process which can still adapt to the present situation.

Although, this intelligence gathering process is not formulated for the primary purpose to fight cybersecurity, it could be conveniently carried over to deal with the arising issues in information gathering and sharing in cyber techniques.

A major theme of this subsection is that all the hype often found in books, magazines articles and news reports about cybercrime, its, investigation and prosecution does not differ substantially from that of other types of crime. Indeed many types of traditional crime increasingly involve use of computers or other types of electronics devices, a general condition that tends to compound understanding about the evolving nature and extent of cybercrimes. Moreover, inmost cases, crimes committed using ICTs are not new crimes, but scams modified to be committed online. One example is fraud, there is not much difference between someone sending a letter with the intention to mislead another person and an e-mail with the same intention. If fraud is already a criminal offence, adjustment of national law may not be necessary to prosecute such acts.

In the light of the above, the discourse here shall concentrate on the analyses of the Nigeria example of information gathering and intelligence process.

Intelligence is the combination of credible information with quality analysis. It refers to information that has been evaluated and from which conclusions have been drawn. It is data that can be used proactively for strategic and tactical purposes. Operational intelligence is intelligence that is required for planning and conducting campaigns and major operations to accomplish strategic objectives within operational areas.

Modern Intelligence gathering involves human efforts and the use of electronic devices. The gathering of intelligence is nothing more than stealing someone's secret. It is done strategically, which means according to some direction, plan or mission, and it is done competitively, which means that your opponents and allies are also most likely doing it and it is done none transparently or in secret.<sup>7</sup> The policy making process, which is informed by intelligence, may be transparent, but the intelligence gathering process is rarely disclosed. The first requirement is that your target must have something worth stealing. If they do not have anything in the form of information that is worth stealing, then all you are doing is snooping or conducting research.<sup>8</sup>

In the business world this is what is referred to as the difference between competitive intelligence and market research. The military takes intelligence gathering seriously, as it is almost always collected for the purpose of assessing risks and hazards in preparing for warfare. The whole purpose of gathering information about others and processing it into intelligence is to provide the leaders or policy makers with options, and to make policy more effective and efficient. There is no point in tasking, collecting, analyzing and distributing intelligence products if there is no policy, issue or anticipated issue on the table.

Basic intelligence gathering consists of collecting information and observations from open sources or clandestine sources. The information or observation is patiently and rigorously analyzed, evaluated, compared and integrated with other information and existing intelligence to arrive at conclusions relevant to the needs of policy makers. Trends and anomalies from the collected intelligence are processed carefully, and if the incoming intelligence seems to follow a

---

<sup>7</sup> Onovo, O,(2005) Interagency Intelligence Gathering and Sharing for Effective Crime Control: Perspective From The Police. A paper presented at the conference Organized by the Network of Police Reform in Nigeria (NOPRIN) and The Nigeria Police Force (NPF) held in Abuja on 29/6/2005.p.-3.

<sup>8</sup> Ibid

pattern that pre-existing intelligence has indicated, this is often called 'connecting the dots'. If there is an anomalous, sharp spike in the quantity or quality of incoming intelligence, this is referred to as 'increased chatter' in intelligence parlance. The key to success is that once your collection elements are deployed, the intelligence coming in from them is rapidly compared in a pre-production process 'cross cueing', which ensures the possibility for dissemination of intelligence products. When basic intelligence products are compared to the kind of collected intelligence coming in from advanced methods such as orbital or air born sensors, this pre-production process is often called 'fusion', although the terms cross-cueing and fusion are sometimes used interchangeably. In advanced countries like the United States, what is in use is a multi level intelligence community where inter operability and collaboration are important and intelligence from different collection sources can move rapidly from one collection discipline to another. "Which national system of intelligence collection will be best suited for us here in Nigeria?"<sup>9</sup>

After collection, all intelligence gathered is rated for its quality and reliability, and then exploited. In intelligence gathering and sharing parlance, it is customary to apply a simple alpha (A - F) and numeric (1 - 6) system on raw data where the alphabetical characters represent the reliability of the source (A = completely reliable, F= unknown reliability) and the numerical characters represent the accuracy of the information (1 = confirmed by other sources, 6 = truth cannot be justified). In practice, there are very few intelligence gathering sources with an A - 1 rating.<sup>10</sup> In the pre-production analysis phase, cross cueing intelligence is evaluated by what is called "analysis of competing hypothesis". Using this approach, an analyst or group of analysts, tries to identify all plausible explanations or conclusions about an issue in an effort to select the

---

<sup>9</sup> Ibid

<sup>10</sup> Ibid

correct or most correct one. There is then a simultaneous comparison of how all the available information supports each potential hypothesis. The finished product becomes a final intelligence estimate presented to the policy maker who will lay out the probabilities or possibilities. It is worthy of note that there always are caveats or provisos to intelligence products, and also, they are affected by the mindsets of the analyst who have processed them.

In inter agency criminal intelligence sharing, the former 'E' Department of the Nigeria Police code name “the Special Branch” was the first intelligence outfit to be established in the Force. It was established by the British colonial administration with the aim of checking alleged subversive activities and excesses of the early nationalist who were agitating for political independence and better conditions of service for workers. At that time, their main responsibilities included among others:<sup>11</sup>

First, Carrying out of surveillance generally, second, travel control, third, aliens’ control, and fourth, checking communist influence in Nigeria.

After the attainment of independence in 1960, the method of operation and areas of emphasis of the Department shifted slightly with general security maintenance as its principal focus. After the abortive coup of 1976, there arose an urgent need to review and overhaul the existing security system and structures in the country.<sup>12</sup> A Panel consisting of top military and civil servants was set up and charged with the responsibility of initiating a new security outfit that would effectively meet the security challenges and needs of the nation. This led to the establishment of the Nigerian Security Organisation (NSO) in 1976 by Decree No. 16. Now the crux of the matter at that time, the working cooperation between the Director General of the NSO and the Inspector General of Police was limited in scope, since the Director General was

---

<sup>11</sup> Onovo, O. (2005) Crime Control in Nigeria. In: Alemika, E.O. (ed) Crime and Policing in Nigeria: Challenges and Options. Cleen Foundation, Lagos Nigeria. Pp.180-186

<sup>12</sup> Ibid

not under any legal obligations to pass on intelligence product to the Inspector General of Police. This was also the situation between the State Directors and the State Commissioner of Police resulting in operational limitations. As at today, the nation has several security agencies with different jurisdictions.<sup>13</sup> The agencies are:

1. National Security Council
2. Nigeria Police
3. Nigerian Armed Forces
4. National Intelligence Agency (NIA)
5. Directorate of State Security Services (SSS)
6. Defence Intelligence Agency (DIA)
7. Directorate of Military Intelligence (DMI)
8. Security and Criminal Intelligence Bureau of the Nigeria Police
9. Nigeria Immigration Service
10. Nigerian Prison Service
11. National Drug Law Enforcement Agency
12. National Economic Intelligence Agency
13. Economic and Financial Crimes Commission
14. Federal, States and Local Government Security Committees.

Each of these agencies has various modes of operation designed to ensure the overall security of the nation in their own sphere of responsibilities. It is pertinent to mention here that the Directorate of State Security Service has had, and ought to continue to have, a purely civilian focus in its responsibilities, as it operate largely within the civil society. The police happen to be

---

<sup>13</sup> Ibid

and should continue to be the largest consumer of its intelligence. This important reality was undermined under the 1976 arrangement.<sup>14</sup>

Any framework for intelligence sharing in Nigeria must appreciate the fact that every agency has rules, regulations, orders and directives, designed to ensure the security of intelligence/information. “This is why those of us here present, who are very conversant with the security business will readily recall such devices as classification of information into Top Secret, Secret, Confidential and Restricted; (internal security matters are usually classified under Top Security categories).<sup>15</sup> Personnel dealing with such classified information are usually sworn on oath to prevent leakages. The necessity of limitation of access to classified information is usually guided by the principles of:

- i) Need to know
- ii) Need to hold, and
- iii) Need to take<sup>16</sup>

The resultant effect of this is, that inter agency intelligence gathering and sharing, has always been fraught with barriers.

The major problems that reduce the capacity of agencies to share criminal intelligence includes but are not limited to the following:

First, lack of a national process for generating and sharing intelligence, second, existence of laws that unduly restrict law enforcement access to information, third, the hierarchical structures of sharing information, fourth, deficits in criminal intelligence analysis, fifth, lack of good technologies to support criminal intelligence sharing.

---

<sup>14</sup> Onovo, O. Op.cit.p.262, at 184

<sup>15</sup> Ibid

<sup>16</sup> Ibid

In Nigeria, security agencies like the Military, the SSS, Customs, Immigration, NDLEA and the likes, may talk about their routine sharing of criminal intelligence with the police through the Inspector General of Police or the State Commissioners of Police, and during the monthly Joint Intelligence Board meetings. But the current framework is inadequate. In these days of threat of cyber insecurity, armed robbery, assassinations and other violent crimes, there is the dire need for a national policy on inter agency criminal intelligence sharing, a policy that will make it possible and mandatory for the various security agencies to provide unclassified information to the Police Force Headquarters, the Zonal AIGs, the State Command Commissioners, the Area Commanders and the Divisional Police officers on daily basis. The rationale is that such information will help the police act both proactively to prevent crime as well as reactively to bring criminals to face the law.<sup>17</sup>

Plans and Strategies for crime control must be subjected to periodic review at all levels, based on available criminal intelligence. This strategy is in line with the National Security Adviser's thinking elaborated in his paper on the government administration's Grand Strategy for National security at Abuja in August 2001. He advised that:

The information required for the effective management of National security is so wide and varied. It includes information on defence, politics, science, technology, economy, crime, labour, population, demography, transportation and telecommunications etc. There is the need for the information from all levels, wards, local governments, states and federal to be accessible through clusters of database.

The absence of basic data inhibits proper planning and prompt response. The "grand strategy" emphasizes the smooth flow of information among the various agencies and departments. Policy makers are expected to create the infrastructure for the collection and storage of vital data. At a later stage, the networking of the

---

<sup>17</sup>Ibid, at p.185

database is to be exploited. The creation of a national crime information database is in progress...<sup>18</sup>

Onovo concluded that while the campaign against violent crimes continues unabated, the police authorities should consider the strategy of “overhaul the Criminal Intelligence Bureau and re-orientate it to make it capable of gathering and sharing operational intelligence for planning and prompt response as recommended to and approved by government since 1981”.<sup>19</sup>

It is noted that training in criminal intelligence gathering should not be the exclusive preserve of Criminal Intelligence Bureau. Rather the Force should consider a robust training programme that encompasses crimes including cyber security for all general duty officers and men in criminal intelligence gathering, and sharing techniques. This will remove the existing barrier being faced by the Central Intelligence Bureau (CIB) as intelligence gathered is not shared with the officers and men who need them for planning and operational purposes at the grassroots level as at now.

It is arguable that information gathering and sharing could improve through Force Directives. For instance, the Force should embark on an awareness campaign within the Police to bring home to all officers and men at all levels, the crucial role of criminal intelligence in planning for the protection of cyberspace and the management of cybercrime. This connotes a situation where every Police Division should have its criminal intelligence gathering and operational planning unit responsible to the Divisional Police Officer (D.P.O) who will then be accountable to his superior authority for breaches or lapses in crime control efforts in his Division. After all, under the Police Regulations, the Divisional Police Officer is charged with the direction and administration of his area of jurisdiction.

---

<sup>18</sup> Ibid

<sup>19</sup> Ibid

In view of the large number of officers and men that will be involved in this massive training for all general duty personnel in operational intelligence gathering, planning and cybercrime management/resolution at all levels, the police authority should consider approaching the government for a special budgetary allocation for this purpose. In addition, it will not be out of place to extend the call for financial support for this criminal intelligence training efforts to all other stakeholders in the public safety and security industry.<sup>20</sup>

### **5.3 Human, Technical and Financial/Institutional Capacity to Prevent and Control Cyber Crime**

Security and privacy of information stored in systems and shared across networks and systems are of vital concerns for managers at all levels of organizations as well as individuals. Because the use of information systems and networks and the entire information technology environment have changed dramatically in the last 20 to 30 years, there has been greater emphasis on security by governments, businesses, other organizations and individual users, who develop, own, provide, and manage service and use information systems and networks.

Individuals, as fitting to their professional roles, should be aware of the relevant security risks, required preventive measures, and assume responsibility and take steps to enhance the security of information systems and networks they deal with. Each individual in an organization is important for ensuring an appropriate level of cybersecurity. Promotion of a culture of security requires both leadership and extensive participation and should result in a heightened priority for security planning and management, as well as an understanding of the need for security among all participants. Security issues should be topics of concern and responsibility at all levels of government and business and for all individual participants of the organization.

---

<sup>20</sup>Ibid at p.186

Information assurance means providing the right information to the right people at the right time. Although simplistic in concept, it involves much more than data security. For example, the reliability, availability, integrity, accuracy, and confidentiality of data are more than protecting your computer information system from internal or external disruption.

Information assurance is the systematic approach to protecting an organization's intellectual property from all potential exposures, both intentional and accidental, and minimizing the consequent effects. Information assurance assumes the responsibility of every individual in the organization, as well as every agency, firm, or company with which the organization interacts.<sup>21</sup>

The private sector has also been active in trying to enhance the ability of law enforcement officials around the world to deal with the problem of cybercrime. For example, Microsoft has invested millions of dollars in developing an international training program and technological resource for law enforcement agencies around the world to better investigate computer-facilitated crimes against children<sup>22</sup>. This project was initially developed with the help of several international police agencies in conjunction with the Royal Canadian Mounted Police (RCMP) and the Toronto Police Service<sup>23</sup>. While it has primarily been used to combat online child pornography, it can also be used to facilitate the investigation and prosecution of other kinds of offenders, such as those committing fraud and identity theft. Successes such as these indicate that the global fight against transnational cybercrime is capable of being won.

---

<sup>21</sup> Peter R. (2002, April) *Evolving Technologies: Information Assurance Core Competencies. (White Paper)* Falls Church VA, Uniformed services Journal of University of the Health Sciences Bethesda MD, USA. p.7.

<sup>22</sup> Tool Thwarts Online Predators. Retrieved June 2, 2015 from <http://www.microsoft.com/presspass/features/2005/apr05/04-07CETS.mspx>.

<sup>23</sup> Ibid, (Royal Canadian Mounted Police (RCMP). "RCMP, Toronto Police Service and Law Enforcement from Across Canada Unite to Fight the Online Sexual Exploitation of Children - Microsoft Canada).

In recent past, organizations have exhibited institutional capacity to prevent and control cybercrime. This section provides a brief overview of the cybercrime problem and examines five case studies to demonstrate this fact.

**i. Multi-State Information Sharing and Analysis Center (MS-ISAC) v QAKBOT**

The MS-ISAC's Cyber Threat Intelligence Coordinating Group, which operates as a division of the Center for Internet Security, a not-for-profit organization focused on enhancing the cybersecurity readiness and response of public and private sector entities, facilitates the development of situation awareness and identifies interrelationships between physical and cyber security activities. It features numerous representatives from law enforcement organizations at the federal, state and local levels in the United States. These include: the Federal Bureau of Investigation (FBI), United States Secret Service (USSS), Department of Homeland Security (DHS), State Homeland Security Advisors, State Fusion Centers, the Department of Defense (DoD), the National Guard, New York State Office of Cybersecurity and representatives from the New York State Police.

Although relatively new, this group already has been incredibly successful in breaking down the traditional barriers for true information sharing, taking raw intelligence on threats and making it actionable information. For example, in April 2010 the FBI provided the MS-ISAC with a forensics image of a system that was part of a financial fraud investigation involving a local college. In conjunction with the New York State Office of Cybersecurity, the MS-ISAC analyzed the system for signs of malware. The resulting analysis revealed the system was infected with a multi-component worm/Trojan malware called "Qakbot". Qakbot made its initial appearance in May 2009 and is known to spread through network shares. It downloads additional malware, opens a "back door" on compromised computers allowing for remote access and logs

keystrokes, all with the ultimate goal of stealing confidential information. The malware also contains root-kit functionality to allow it to hide its presence.

By analyzing the network traffic, the MS-ISAC was able to identify infected servers as well as high jacked usernames and passwords. With permission of the college, MS-ISA shared these findings with the FBI and all of the other members of the MS-ISAC. Through this investigation and partnership with the FBI, the MS-ISAC was able to identify and notify 17 state governments infected with this malware. One of the notified states confirmed having approximately 4,700 infected systems.

From one college to 50 states, this example of local-to-local learning identified tens of thousands of infected computers. In partnership and by sharing actionable information, MS-ISAC was able to disable the theft of credentials and denied the further invasion of privacy. In the wake of the Epsilon and Sony PlayStation breaches, where our personal information of thousands of consumers was exposed, it is likely that the MS-ISAC and its partners will face and hopefully tackle more crime rings aimed at exploiting the seams between local and national law enforcement efforts.

## **ii. Microsoft v The Rustock Botnet**

At its peak performance, the Rustock botnet sent out more than 44 billion spam messages a day including “fake Microsoft lottery scams and offers for fake-and potentially dangerous--prescription drugs.”<sup>24</sup> According to Symantec, the security software firm, Rustock constituted the largest source of spam in the world with approximately 50% market share. Spam can be a money making business because those who send it get paid for every email address they send to it.

---

<sup>24</sup>Richard Boscovich. (2012,11,October) Taking Down Botnets: Microsoft and the Rustock Botnet. Retrieved June 2, 2015 from [http://blogs.technet.com/b/microsoft\\_on\\_the\\_issues/archive/2011/02/18/taking-downbotnets-microsoft-and-the-rustock-botnet.aspx](http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/02/18/taking-downbotnets-microsoft-and-the-rustock-botnet.aspx).

Microsoft decided that the Rustock botnet, the largest generator of spam in the world, was causing an Internet nuisance because it was damaging Microsoft products as well as its reputation. Accordingly, Microsoft turned to the courts to address the issue. On March 16, 2011, U.S. Marshals accompanied employees of Microsoft's digital crimes unit into Internet hosting facilities in five U.S. cities.<sup>25</sup> Using a federal court order, they seized the command-and-control servers that were responsible for manipulating an estimated one million computers worldwide. Microsoft was not alone in its efforts to take down the Rustock infrastructure. The effort required collaboration between "industry, academic researchers, law enforcement agencies and governments worldwide."<sup>26</sup> Microsoft worked with pharmaceutical company Pfizer, the network security provider Fire Eye, Malware Intelligence Labs and security experts at the University of Washington, each of whom attested in court to the dangers posed by Rustock and the impact on the Internet community. Additionally, Microsoft also worked with the Dutch High Tech Crime Unit within the Netherlands Police Agency to help dismantle part of the command structure for the botnet operating outside of the United States. Microsoft also worked with China's Computer Emergency Response Team (CN-CERT) to block registrations of domains in China, a pro-active approach aimed at preventing the stand-up of future command and control servers.

However, Microsoft did not stop there. The Microsoft digital crimes unit continued to work with global Internet Service Providers (ISPs) and CERTs around the world to remediate the infections. As of early June 2011, nearly sixty days after the initial takedown of the servers, Microsoft's international efforts had cleaned up approximately 60% of the infected infrastructure.<sup>27</sup>

---

<sup>25</sup> Bruce Sterling. (2011, 28 March) Microsoft versus Rustock Botnet. Wired Magazine (online) Retrieved June 2, 2015 from [[http://www.wired.com/beyond\\_the\\_behind/2011/03/microsoft-versus-rustock-botnet/](http://www.wired.com/beyond_the_behind/2011/03/microsoft-versus-rustock-botnet/)]

<sup>26</sup>Ibid

<sup>27</sup>Jeff Williams, (2011, 14 June ) Microsoft Malware Protection Center.( the 23rd Annual FIRST Conference, Vienna, Austria). Retrieved June 2, 2015 from [www.wired.com/beyond\\_the\\_behind/2011/03/microsoft-versus-rustock-botnet/](http://www.wired.com/beyond_the_behind/2011/03/microsoft-versus-rustock-botnet/)

Microsoft used the power of the law combined with its global network and presence and demonstrated that a multinational corporation can lead by example. Their efforts relied on multi-party private-public collaboration using legal and technical measures to arrange a coordinated takedown of cybercrime followed by a coordinated clean up of the infection.

### **iii. FBI v The Coreflood Botnet**

The Coreflood botnet was designed to record the keystrokes and Internet browsing activity of victims. It collected banking credentials and passwords intended for use by criminals to direct fraudulent wire transfers and rob victim's bank accounts. In a seminal case, U.S. District Judge Vanessa Bryant determined that "allowing Coreflood to continue running on the infected computers will cause a continuing and substantial injury to owners and users of the infected computers, exposing them to a loss of privacy and an increased risk of further computer intrusions."<sup>28</sup>

To target the Coreflood botnet, the FBI obtained multiple criminal seizure warrants to deactivate the existing Coreflood command and control servers. Simultaneously, a temporary restraining order was obtained, directing the defendants to stop engaging in fraud. The order also authorized the U.S. Marshals Service, with the assistance of the FBI, to operate and respond with "stop" commands to infected computers as a substitute command and control server. This approach provided the FBI with time to identify and notify as many of the 2.4 million infected victims as possible of the fraudulent activity and their role in the scheme. By holding the botnet static, anti-virus vendors were able to develop solutions for detecting and removing the Coreflood virus before a new variant was released. These activities collectively, reduced the botnet by approximately 80% domestically and 45% internationally.

---

<sup>28</sup>Kim Zetter. (2011, 13 April ) U.S. Wins Court Order to Seize Control of 'Coreflood' Botnet, send kill Signal. Wired Magazine Online. Retrieved June 2, 2015 from [http://www.wired.com/threatlevel/author/kimzetter/]

The Executive Assistant Director of the FBI's Criminal, Cyber, Response and Services Branch, Shawn Henry, stated that "these actions to mitigate the threat posed by the Coreflood botnet are the first of their kind in the United States and reflect our commitment to being creative and proactive in making the Internet more secure."<sup>29</sup> The joint operation to take down Coreflood involved information sharing between the U.S. Marshals Service and the FBI's regional offices located in New Haven, Connecticut, Dallas, Texas, Richmond, Virginia, Atlanta, Georgia, Cincinnati, Ohio, Phoenix, Arizona, Los Angeles, California, New York and New Jersey. It also benefited from international participation by the Estonian National Police. This unique cooperative effort across state lines and international borders used a legal framework that may pave the way for future botnet mitigations by the FBI.

**iv. The National Cyber Forensic and Training Alliance (NCFTA) v Pump and DumpScam**

NCFTA is a non-profit corporation with a mission of facilitating collaboration between private industry, academia, and law enforcement to identify, mitigate and neutralize complex cyber related threats. In addition to its state and local law enforcement and industry representatives, it enjoys international representation from Canada, Australia, England, India, Germany, the Netherlands, Ukraine, and Lithuania. It provides streamlined and timely exchange of intelligence cyber threat data to corporations.

In 2006, NCFTA began an exchange of information on pump-and-dump scams that were pillaging some investment brokerages. These scams involved using compromised account credentials to artificially inflate the price of a stock by purchasing or influencing the purchase of large quantities of a stock and selling that stock at an artificially inflated high price. NCFTA served as the focal point for sharing actionable information related to malware, botnets being

---

<sup>29</sup> Shawn H.( 2011, 12 April) (comment on seizure operations by FBI of Coreflood Botnet materials) Federal Bureau of Investigation Press Release April, 2011

utilized, commodities that were being targeted, and other technical information surrounding the criminal behavior. The NCFTA partnered with the FBI, Federal Trade Commission (FTC) and the Securities and Exchange Commission (SEC) to quickly share information related to this fraud trend.

In February 2009, federal agents executed six search warrants at five locations throughout the United States. Ultimately, the FBI found that initial loss estimates were low, as further warrants were executed, the government found that criminals had manipulated or attempted to manipulate approximately 290 stock symbols resulting in millions more in estimated losses. As a direct result of this collaborative effort, five people pleaded guilty to mail fraud, wire fraud, and CAN-SPAM Act violations for running an international stock spamming operation that forwarded billions of illegal e-mail advertisements to inflate Chinese 'penny' stocks then reaped substantial profits by trading away these same stocks while others bought them at inflated prices.<sup>30</sup>

In the wake of the NASDAQ breach, the NCFTA may be called upon again to focus efforts to ensure that NASDAQ doesn't experience fraudulent activity. NCFTA's focus on the black market infrastructure that supports cyber threats and crimes, including botnets, hosting companies, malware, money laundering, and shipment/money mule recruitment takes on even more importance as the private sector is suffering more and more breaches that harvest personal credentials and passwords to gain access to financial institutions.

#### **v. INTERPOL and ICANN, Partnering for Internet Security**

The International Criminal Police Organization (INTERPOL) performs a significant amount of behind-the-scenes work and facilitates law enforcement cooperation in cyber matters by leveraging its worldwide network of law enforcement officials, agencies, partners, and

---

<sup>30</sup> Ibid

technology. With 188 member countries, INTERPOL is the second largest Intergovernmental organization after the United Nations. On internet security matters, INTERPOL is partnering with the Internet Corporation for Assigned Names and Numbers (ICANN), the non-profit corporation responsible for the global coordination of domain names and Internet protocol addresses.

These two politically neutral, global entities are partnering to enhance common means for preventing and addressing Internet crime. Secretary General Noble recently noted, “the Internet has no borders, and neither do the criminals who exploit it. As the Internet’s role in society continues to increase in scope and importance, it is vital for INTERPOL to help create bridges between the international law enforcement community it represents and ICANN in order to advance Internet security practices for the benefit to all.”<sup>31</sup> For example, a secure worldwide communications network, known as 24/7, that enables INTERPOL’s members to access each other’s national databases to facilitate law enforcement information sharing, is one such bridge that can be used to establish situation awareness and information sharing on particular Internet issues (e.g., hijacking border-gateway protocols or exploitation of the Domain Name System (DNS) registries).

This network could be further enhanced by INTERPOL’s initiative to merge the domains of cyber security, digital forensics, cybercrime investigations and information security into one global cybersecurity focused function. As INTERPOL joins ICANN’s Governmental Advisory Committee as an observer -- coupled with its active membership of the information security committee of the International Standards Organization (ISO), where it helps drive global cybersecurity standards for the law enforcement community INTERPOL may be able to enhance

---

<sup>31</sup>INTERPOL and ICANN (2011, 23 May) Press Release / Communiqué de Presse - advance cooperation on Internet security. New York Police Bulletin, May 2011. Pp. 7-12

local law enforcement efforts and drive down the time from incident detection to interdiction and prosecution.

While there are not yet any published reports of joint operations from these organizations, this international partnership demonstrates INTERPOL and ICANN's commitment to leverage their collective access and global reach to amplify their common goals to improve the safety and stability of the Internet of the future.

All of these case studies serve to remind us of the importance of cooperation in cyberspace. Individually, law enforcement agencies will never be able to defeat the clever tactics and agile criminal infrastructures behind the episodes described above.

Each example shows that by sharing actionable information across borders and across jurisdictions, and using novel approaches and applications of the law, progress can be made in reducing cybercrime. These few examples can be the blue-print for local entities and global institutions to follow. Individual states must recognize that success against international cybercrime will be achieved only if they are willing to commit more to the law enforcement communities and update the laws governing cyberspace and cybercrime.

There are a number of reasons why industry, government and law enforcement need to be brought together to tackle cyber crime. The internet infrastructure is owned by the private sector, and the business community operates services over it. The industry is the repository of technical skills and attack trend information, and has the knowledge to help deliver a safer internet. In return, industry needs to have access to information and intelligence that will be developed

through the National Fraud Intelligence Bureau (NFIB), to both protect itself and to develop defenses<sup>32</sup>.

#### **5.4 Evidentiary Problems**

Evidence is the means by which facts relevant to the guilt or innocence of an individual at trial are established. Electronic evidence is all such material that exists in electronic, or digital, form. It can be stored or transient. It can exist in the form of computer files, transmissions, logs, metadata or network data.<sup>33</sup> Digital forensics is concerned with recovering often volatile and easily contaminated information that may have evidential value. Forensics techniques include the creation of “bit-for-bit” copies of stored and deleted information, “write-blocking” in order to ensure that the original information is not changed, and cryptographic file “hashes”, or digital signatures that can demonstrate changes in information.<sup>34</sup>

Detailing specific evidentiary problems is beyond the scope of this work, however, it is worth noting that “there are special evidentiary problems which arise in cybercrime cases largely related to the nature of the electronic evidence which is often times critical to proving who committed the crime”<sup>35</sup>. The problems include the facts that the recently repealed Nigerian Evidence Act did not make computer generated documents admissible in law and has the effect of ascribing the status of secondary evidence to such documents.

Telegrams and documents produced through teletype machines have been held not to satisfy the requirement of writing and signature as required by the now repealed Evidence Act.

---

<sup>32</sup>Kew R.( 2010, March) Cyber Crime Strategy Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty, the Office of Public Sector Information, Information Policy Team, Surrey TW9 4DU. Retrieved from [licensing@opsi.gsi.gov.uk](mailto:licensing@opsi.gsi.gov.uk). June 2, 2015

<sup>33</sup> UNODC (2013) Comprehensive Study of the Problem of Cybercrime and Responses to it by Member States, the International Community and the Private Sector. Report - Expert group conduct a Comprehensive Study on Cybercrime in Vienna, 25-28 February 2013, p.8

<sup>34</sup> Ibid at p.9

<sup>35</sup>David, Icove, Karl Seger & William Vonstorch,(1995). Computer crime: A crime fighter’s Handbook. O’Reilly & Associates, Inc. USA. Pp.263-308

Section 2(1) of the Evidence Act<sup>36</sup> defines documents to include books, map, drawings, figures or marks made by one of these things intended to be used or which may be used for the purposes of recording that matter. Hence, the evidential status of computer generated evidence had remained an unsolved question for a long time.

In the case of *Anyaebosi v R.T. Briscoe Ltd*,<sup>37</sup> the Supreme Court reluctantly endorsed the admissibility of the computerized statement of account as secondary evidence. In the absence of Evidence Act to specifically recognize computer generated document, the Court of Appeal in *Ogolo v IMB (Nig.) Ltd* merely took a judicial notice of computerized system of keeping accounts and doing business in Nigeria<sup>38</sup>.

In Nigeria, the upsurge in technology crime and the helplessness of the conventional security outfits in apprehending the skilled criminals has propelled the Federal Government to enact multitude of legislations that are aimed at combating the financial and economic crimes.<sup>39</sup>

Evidentiary problems as an issue in cyber crimes have been addressed by several scholars<sup>40</sup> as has the Council of Europe<sup>41</sup>. The problems are of such a nature that any treaty that assisted in the prompt collection and preservation of electronic evidence, especially tracking

---

<sup>36</sup> Evidence Act CAP.E14 L.F.N. 2004(now repealed and replaced with Evidence Act, 2011)

<sup>37</sup> (1997) 3 NWLR pt 59 at 84

<sup>38</sup> *Chief Joseph Ogolo v. International Merchant Bank (Nigeria) Ltd. (1995) 9 NWLR pt.7 at 317.* Hon. Justice Moronkeji Omotayo Onalaja, J.C.A. read the leading judgment, on judicial notice of computerized system of keeping accounts. Said, “The commercial and banking operation in the keeping of accounts by the old system has been changed to computer which makes Nigerian business to be modernized and in keeping with the computer age which system is so notorious that judicial notice of it can be taken under section 74 of the Evidence Act, (P. 324, Paragraph B)”.

<sup>39</sup> Gbenga A. (2003 – 2005 ) Adequacy and Efficacy of Penal Sanction for Financial and Banking Offences in Nigeria, 2(ii) (Electronic Technology Related Crimes in Financial Institutions and Banks in Nigeria) Ahmadu Bello University Journal of Commercial Law. 2(2):104, See also, T.A.I. Osipitan. (1998) Legal Impacts of Technology on Rules of Evidence in Banking and Commercial Litigation. Nigerian Commercial Laws: Essays in Honour of Chris Ogunbanjo. Chap. 29 at p 435.

<sup>40</sup> Clifford Miller. (1992 May) Electronic Evidence- can you prove the Transaction Took place?, computer Law .Prentice Hall Law and Business. U.K. at 21, John T, Soma Elizabeth et,al, (1996). Computer crime: Substantive statutes & Technical & Legal search considerations. F.L. REV. 39A (225):46-52

<sup>41</sup> Council of Europe(COE’S), Recommendation No R (81) 20 of the committee of ministers on the Harmonization of laws Relating to the Requirement of written proof and To the Admissibility of Reproductions of Documents And Recordings on computers; Recommendation No R (85) 10 on Letters Rogatory for The Interception of Telecommunications; Recommendation No. R(87) 15 Regulating The use of personal Data in The police state, and Recommendation No. R (89) 9 on computer- Related crime.

evidence, would be highly beneficial to the projection of a more credible criminal enforcement mechanism which would increase its deterrent effect as well.

It is worthy of note that even the newly amended Evidence Act<sup>42</sup> is not spared of these controversies. For example, a columnist in one of the local news papers<sup>43</sup> said: “the current legal regime is inadequate to regulate e-Commerce in Nigeria and there is no sufficient legislation to prosecute offenders”.<sup>44</sup> He argued that in Section 84(1) of the Evidence Act 2011, the Evidence Act appears to support the admissibility of computer generated evidence in court but that there are too many conditions attached to the section<sup>45</sup> which have made it impossible to strictly enforce it. He further argued that for instance, it provides that there has to be proper foundation as to the working condition of the computer used in producing the piece of evidence, and that the section equally request that a certificate must be issued by the person who has the technological know-how about operations of the computer. His opinion is that it will be difficult for someone to know the state of his bank’s computer in a case where his bank is to be a defendant. Because what the section implies is that if you are suing your bank, your bank has to certify that the computer used in producing the document (e.g. statement of account) was in excellent condition as of the time it was produced. He concluded that “So, you, as a plaintiff, have to go to the defendant (the bank) to certify the evidence you are presenting in court against the bank. This is ridiculous”.<sup>46</sup>

Logical as the above argument may sound, with all due respect, this research is unable to align with the position of the writer that the new Evidence Act, 2011 is not helpful to the extent of dealing with electronically generated documents.

---

<sup>42</sup> Evidence Act, 2011

<sup>43</sup> Chiedu A. (2012, December 27) Tackling the Cybercrime Menace in Nigeria. The Punch News Paper Nigeria. p.20

<sup>44</sup> Ibid

<sup>45</sup> Section 84 (2) (a-d) Evidence Act, 2011

<sup>46</sup> Chiedu A. Op.cit. p281.at,35

It is noted that the present Evidence Act<sup>47</sup> have provided a cure for the problems earlier discussed in this subhead above to the extent that Section 84(1) provides for admissibility of documentary statement in document produced by computers. Under the interpretation clause, the description of document under Section 258(1)(b)(c)(d) also define document to include materials produced by electronic means or devices. It is arguable that the benefit of the current Evidence Act, 2011, lies in combine reading of the sections or when relevant sections are read in conjunction with one another and not when read in isolation.

As more and more information is kept in digital form, electronic evidence is relevant to both cybercrime investigations and traditional investigations. Computer and network technology have become a part of everyday life in developed countries and are increasingly becoming so in developing countries as well. The increasing capacity of hard drives<sup>48</sup> and the low cost<sup>49</sup> of the storage of digital documents as compared to the storage of physical documents have led to a growth in the number of digital documents.<sup>50</sup> Today, a significant amount of data is stored only in digital form.<sup>51</sup> As a consequence of this increase, electronic documents such as text documents, digital videos and digital pictures<sup>52</sup> are playing a role in cybercrime investigations and related court proceedings.<sup>53</sup>

---

<sup>47</sup> Evidence Act, 2011

<sup>48</sup>Abramovitch, R. (2002) A Brief History of Hard Drive Control. Control Systems Magazine, EEE, vol. 22, Issue 3, p. 28, Coughlin/Waid/Porter,( 2005,) The Disk Drive, 50 Years of Progress and Technology Innovation, Retrieved June 2, 2015 from [www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf](http://www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf).

<sup>49</sup>Giordano S. (2006.)Electronic Evidence and the Law, Information Systems Frontiers Journal 6( 2): 161-174, Willinger/Wilson, (2004 )Negotiating the Minefields of Electron ic Discovery. Richmond Journal of Law and Technology. X (5):98.

<sup>50</sup>Lange/Minster. (2011) Electronic Evidence and Discovery. (UNODC) Working Paper on the Collection of Topics- United Nations Office on Drugs and Crime. 17-21 January 2011 in Vienna at Pp.1-18

<sup>51</sup>Hosmer C. (2002) Proving the Integrity of Digital Evidence with Time, International Journal of DigitalEvidence 1 (1): p1-7.

<sup>52</sup> Kwiatkowski J. (2002) Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images, Journal of Law and Policy. 267: 1-32.( Regarding the admissibility and reliability of digital images)

<sup>53</sup> Casey E. (2011 April) Digital Evidence and Computer Crime. Third Edition Academic Press. USA. P.128. (Regarding the legal frameworks in different countries).

Electronic evidence presents a number of challenges, at both the stage of its collection and that of its admission as evidence.<sup>54</sup> During the process of evidence collection, investigators must satisfy certain procedures and requirements, such as the special treatment required for the protection of the integrity of data. Law enforcement agencies require specific measures in order to carry out successful investigations. The availability of such measures is especially relevant if traditional forms of evidence such as fingerprints or witness identification are not available. In those cases, the ability to successfully identify and prosecute an offender is based on the correct collection and evaluation of the digital evidence.<sup>55</sup>

Digitalization also influences the way in which law enforcement agencies and courts deal with evidence.<sup>56</sup> Whereas traditional documents are simply handed out in court, digital evidence may require specific procedures that are not suitable for conversion into traditional evidence, for example, Printouts of files.<sup>57</sup>

## **5.5 Investigative Techniques**

In order to carry out effective investigations, law enforcement agencies need to have access to investigative procedures that enable them to take the measures necessary to identify the offender and collect the evidence required for criminal proceedings.<sup>58</sup> These measures may be the same as those used in traditional investigations not related to cybercrime. However, given that the offender does not necessarily need to be present at or even near the crime scene, it is

---

<sup>54</sup> Ibid

<sup>55</sup> Leigland R, Krings W.(2004), A Formalization of Digital Forensics. *International Journal of Digital Evidence*. 3 (2): 231-283. ( Regarding the need for a formalization of computer forensics)

<sup>56</sup> Moore R. (2004) To View or not to View: Examining the Plain View Doctrine and Digital Evidence. *American Journal of Criminal Justice*. 29(1): 57-73. (Regarding the difficulties of dealing with digital evidence on the basis of the traditional procedures and doctrines)

<sup>57</sup> Vacca J. (2005) *Computer Forensics, Computer Crime Scene Investigation*, 2nd Edition, Charles River Media Publisher. U.K. pp. 200-250, Robinson ... (1970) The Admissibility of Computer Printouts under the Business Records Exception in Texas. *South Texas Law Journal*. 12: 291. (Regarding the early discussion about the use of printouts).

<sup>58</sup> Görling S. The Myth of User Education, (2006, October 19) *Social Science Electronic publishing, inc.* Stockholm Sweden. at,p. 355. (Regarding user-based approaches in the fight against cybercrime), see also Jean-Pieree Chevenement.(2000) French Minister of the Interior, (the comment made) at the G-8 Conference in Paris in 2000: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

very likely that cybercrime investigations will need to be conducted in a different way from traditional investigations.<sup>59</sup>

In addition to provisions relating to substantive cybercrime offences, most comprehensive regional frameworks set up to address cybercrime also contain a set of provisions specifically designed to facilitate cybercrime investigations. Standard provisions include specific search and seizure procedures, the expedited preservation of computer data, the disclosure of stored data, the interception of content data and the collection of traffic data.

Some States have adopted measures beyond these standard provisions to address specific challenges such as the interception of VoIP communication.<sup>60</sup> Although most States have provided for investigation measures, such as wiretapping, that enables them to intercept landline as well as mobile phone communications,<sup>61</sup> these measures are usually not sufficient to allow for the interception of VoIP communications. The interception of traditional voice calls is usually carried out through telecommunications providers.<sup>62</sup> Applying the same principle to VoIP, law enforcement agencies generally operate through Internet service providers and service providers supplying VoIP services. If, however, the VoIP service is based on peer-to-peer technology, service providers may be unable to intercept communications.<sup>63</sup>

Given the ever changing nature of technology, it is virtual impossible for police in most parts of the world to keep up with criminals in their constant efforts to exploit technology for personal and illegal gains. With this in mind, it is critical that

---

<sup>59</sup> International Telecommunication Union (2009) Understanding Cybercrime: A Guide for Developing Countries chapter 3.2.7 of report. Retrieved June 2, 2015 from [www.itu.int](http://www.itu.int). (Regarding the independence of place of action and the result of the offence)

<sup>60</sup>The term “voice over Internet protocol”(VoIP) is used to describe the transmission technology for delivering voice communication by using packet-switched networks and related protocols.

<sup>61</sup>Karpagavinayagam B, Nancy S, Festor O.( 2007 July ) “Monitoring Architecture for Lawful Interception in VoIP Networks, being a seminar paper presented at the Second International Conference on Internet Monitoring and Protection” (ICIMP) held in San Jose, from 1-5 July 2007.at p.5

<sup>62</sup> Seedorf J. (2008) Lawful Interception in P2P-Based VoIP Systems: Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks. lecture notes in computer science. Springer link vol. 5310, pp. 217-235 . (Regarding the differences between PSTN and VoIP communication)

<sup>63</sup> Bellovin S.( 2006 June 13 ) Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP. ITAA Publications USA.Pp.1-21.

police work closely with other elements of the criminal justice system, the public at-large, the private sector and non-governmental organizations to ensure the most comprehensive approach to the problem.<sup>64</sup>

In the history of police investigation of computer crime and cybercrime INTERPOL<sup>65</sup> has since the 1980s been the leading international police agency in this field. INTERPOL has established Regional Working Parties for regions in Africa, Asia, Latin America, and Europe. These working parties consist of the heads or experienced members of national computer crime units. INTERPOL also organize international conferences on cybercrime for the global law enforcements, and global training courses specializing in cyberspace investigations such as investigations of botnets, malicious codes and cases where Voice over IP is involved.

INTERPOL has established a rapid information exchange system for cybercrimes, an international 24hour response system including National Central Reference Points (NCRPs) in more than 120 countries for a global cooperation on cybercrime investigation that also has been endorsed by the G8 High Tech Crime Sub-group. The 24hour system enables police in one country to immediately identify experts in other countries and obtain assistance in cybercrime investigations and evidence collections. The General Assembly of INTERPOL has recently at their meeting in 2010 approved the creation of the INTERPOL Global Complex (IGC), based in Singapore. It is expected to go into full operation in 2013 or 2014, and to employ a staff of about 300 people. Singapore may have been chosen since it is a trusted city in a region that may be the new centre of economic activities, and the anticipated corresponding increase in criminal activity.

---

<sup>64</sup> Ibid, (Marc Goodman is the Senior Advisor to INTERPOL's Steering Committee on Information Technology Crime, his presentation as chair of the organizations working group on Next Generation Cyber Threats)

<sup>65</sup> INTERPOL, (2006) bulletin. Retrieved June 2, 2015 from [www.interpol.org](http://www.interpol.org). (The headquarter is in Lyon, France)

The IGC is an integral part of the INTERPOLs efforts to reinforce its operational platform and will focus on developing innovative and state-of-the-art policing tools to help law enforcement around the world, especially in enhancing preparedness to effectively counter cybercrime. The IGC will also include a 24-hour Command and Co-ordination Centre (CCC).

The Group of Eight States (G8) established in 1997 the Subgroup of High-Tech Crime (the Lyon Group). At the meeting in Washington in 1997, Ten Principles was adopted in the combat against computer crime, including a 24hour network for the assistance in global cybercrime investigations. This network consists of more than 40countries around the world, and work also in cooperation with INTERPOLs 24hours network. The goal was to ensure that no criminal receives safe havens anywhere in the world.

Since then several statements have especially been adopted at the G8 Meetings for the combat against cybercrime and terrorists use of Internet. In a 2004 Meeting one of the G8 adopted goals was: *to ensure that law enforcement agencies can quickly respond to serious cyber-threats and incidents.*

At the Moscow Meeting in 2006 for the G8 Justice and Home Affairs Ministers a statement was made including: “We will instruct our experts to generate unified approaches to fighting cyber criminality, and we will need an international legal base for this particular work.”<sup>66</sup>

At the 2009 Meeting a statement was made: “Criminal misuse of social networks, encryption services, VoIP services, the Domain Name System, and other new and evolving

---

<sup>66</sup>Stein Schjøberg and Solange Ghernaoui-Hélie. (2011) A Global Treaty on Cybersecurity and Cybercrime. Second edition. p.58.Retrieved June 2, 2015 from [www.hec.unil.ch/sgh](http://www.hec.unil.ch/sgh).

criminal attacks on information systems, pose increased challenges to law enforcement and are spreading.”<sup>67</sup>

In an effort to policing the cyberspace, some countries have well established units to police the Internet. FBI<sup>68</sup> in the United States has been in the forefront on investigating computer crime and cybercrime since the 1970s. FBI has offered courses for police investigators, also including police officers from other countries. Many countries in Europe and Asia have established such units, also in United Kingdom with the Metropolitan Police Central e-Crime Unit (PCeU). In the UK a “Virtual Task Force” has been established, including additional participation from banks, payment service sector, Internet and Telecommunications industry, and universities. The Task Force is working to predict, prevent and respond to cyber threats.<sup>69</sup>

Cyberspace is “patrolled” today by many law enforcements around the world. One of the most actual areas is offences against children, where many police investigators poses as children when policing child sex offenders in cyberspace.

In Europe, it is assumed that countries like the Netherlands and Germany are in the forefront of developing policing on the Internet, but the special police units in the Nordic countries have also been discussing a “Virtual Police Station” and to develop best practices for intelligence work, surveillance and investigation on the Internet.<sup>70</sup>

## **5.6 Prosecutorial Skills and Knowledge**

The Internet has tested the limits of regulation, prompting some to declare ‘independence’<sup>71</sup> and yet others to declare it beyond the limits of governance.<sup>72</sup> One of the

---

<sup>67</sup> Ibid.

<sup>68</sup> Federal Bureau of Investigation (FBI) (2008) Information Bulletin. Retrieved December 18, 2014 from [www.fbi.gov](http://www.fbi.gov).

<sup>69</sup> Sir Paul Stephenson. (2010 October), *E-Crime Detectives as Vital as Bobbies on Beat*. Retrieved June 2, 2015 from [telegraph.co.uk](http://telegraph.co.uk).

<sup>70</sup> Stein Schjøllberg and Solange Ghernaoui-Hélie .Op-cit. p.111, at.p.59

<sup>71</sup> John Perry Barlow (1996, February) A declaration of the Independence of Cyberspace. Retrieved December 18, 2014 from <http://www.eff.org/pub/publications>.

purposes of Johnson's text is to build a global community of people who are thinking about all this in a serious way. As time passes, one aspect of governance is clearly visible, the will of governments to be seen and felt on the Internet. Governments across the world seem eager to put to rest the notions that cyberspace can't be governed.

Traditional legal systems have had great difficulty in keeping pace with the rapid growth of the Internet and its impact throughout the world. While some laws and objectives have been enacted and a few cases have been decided that affect the Internet, they leave most of the difficult legal issues to the future.<sup>73</sup>

Given that network computing power has increased the offender's reach and overall capacity to exploit criminal opportunities with high aggregate return on investment, it is hardly surprising that concern about law and order have long dominated debates about Internet. These concerns are perpetuated by the future shock of public feelings of helplessness or anxiety generated by the poisonous combination of society's increasing reliance on networked technologies, the necessary steep learning curve demanded of users, and the popular public misperception that internet misuse cannot be controlled. Indeed, the fact that there appear to be hundreds of thousands of reported cybercrime incident each year compared with very few prosecutions would seem to substantiate fears that attempt to control internet behavior are failing. It is noted that during the first decade following the introduction of the Computer Misuse Act 1990 in the United Kingdom there were only about 100 or so prosecution against hackers and even fewer convictions. This disparity is not only to be found in the UK, but elsewhere in the

---

<sup>72</sup> Johnson David, Post R, David G (1996) Law and Borders: The Rise of Law in Cyberspace, Stanford Law Review. 48:1367-1402.

<sup>73</sup> Rodney D. (2007) Guide to Cyber Laws.(3<sup>rd</sup> edition) Wadhwa and Company Law Publisher, New Delhi India. (See, preface to second edition).

world.<sup>74</sup> Despite the low prosecution rates, the UK police and Justice Bill in 2006 sought to further increase the penalties for computer misuse to a maximum of ten years in prison.<sup>75</sup>

Faced with a jurisdictional or evidential disparity, police or prosecutors engage in sort of policing arbitrage and used their resourcefulness to ‘forum shop’<sup>76</sup> to increase the prospect of maximizing the potential for obtaining a conviction.<sup>77</sup> This process was very evident in the case of *United States of America v Robert A. Thomas and Carleen Thomas*<sup>78</sup> where the prosecutors ‘forum shopped’<sup>79</sup> to seek a judicial site where they felt a conviction would best be secured. They chose Tennessee rather than California because of the greater likelihood of conviction. In *R. v Fellow; R. v Arnold*<sup>80</sup> the investigation was passed from the US to the UK police because the former believed that the latter was more likely to gain a conviction because the defendants were resident in the UK. These cases illustrate some successful examples of prosecutorial skills and knowledge of inter-jurisdictional cooperation and both cases were relatively unproblematic because they concerned extreme pornography. Where cooperation tends to fall down is with the more contentious types of non-routine offences. Either the gravity of the offence may be recognized in only one jurisdiction and not the other, or the police will simply not pass on the case because they claim ownership over it.

## **5.7 Appraisal of the Peel Theory of Community Policing: Whether Applicable in the Context of Cyber Security and Protection**

The current model for policing and law enforcement as proposed by Peel in 1829 is based on four characteristics that shaped how conventional offline crimes are committed. The theory is

---

<sup>74</sup> Smith R, et al, (2004) *Cyber Criminals on Trial*. Cambridge University Press. UK. p.30

<sup>75</sup> David S. (2007) *Cybercrime: The Transformation of Crime in the Information Age*. Polity press, Cambridge. UK. p.158.

<sup>76</sup> Braithwaite J, Drahos P. (2000) *Global Business Regulation*. Cambridge University Press. p.68.

<sup>77</sup> Walls D. (2002, March) *Internet Related Fraud and Deceptions upon Individuals within the UK*. (Final Report to the Home Office) United Kingdom Home office unpublished Report-2000

<sup>78</sup> (1996) 74 F.3d 701; 1996 US. App. Lexis 1069; 1996 Fed App.0032P (6<sup>th</sup> Cir.)

<sup>79</sup> Forum Shop- When multiple courts have concurrent jurisdiction over a plaintiff's claims the plaintiff may forum shop, or chose the court that will treat his or her claims most favorably.

<sup>80</sup> (1997) 2 All ER 548

founded on the fact that criminals and victims are proximate, there are limitations in the scale and extent of crime that can be committed per time; physical constraints such as planning the crime and visiting the crime scene prior to the crime poses a challenge to criminals; and the ability of law enforcement to profile or study the crime pattern can aid detection and apprehension. Although Cyber crimes share a few of the attributes of conventional crimes, it deviates completely in terms of its operation. For instance, cyber crime is automated, thus it has in its intrinsic nature, the potential to attack multiples of victims per time at different location. Spatial confinement is therefore negated as a means for detection and apprehension. Another interesting but disturbing phenomenon on the webs cape is that cyber criminals can subtly turn their victims to criminals by using anonymous proxies when they hijack their systems. Such systems are used to propagate the crime in order to reach more victims and escape detection. Crimes of this nature are committed across international boundaries, hence sovereignty of states are violated making prosecution extremely difficult. Building on a previous work by Longe et al<sup>81</sup>, this work takes a critical look at the Peel theory of policing in the context of cyber crime. The work identified the Achilles heel in the model and make recommendations that will assist in scaling up the theory to be able to respond appropriately to the challenges of fighting crime in the information age.

The definition of crime from different schools of thought varies as much as there are differing perceptions of the issue in different societies. For this discussion crime is viewed as act(s) committed or omitted in violation of ethics, norms and (or) laws forbidding or commanding it and for which punishment is imposed upon conviction. These acts threaten

---

<sup>81</sup>Longe O, Osofisan A, Kvasny L, Jones C. and Nchise A. (2010). Towards A Real-Time Response (RTR) : Model for Policing the Cyberspace. *Journal of Information Technology in Developing Countries*. 20 (3):1-10

social, economic, political and other social structure in a society. Crime could be against persons, organizations, institutions, states and even global.

Examples are theft, rape, assault, murder, fraud, arson and the likes. Crime has plagued societies from time immemorial and new forms of crimes evolve with societal advancement. Crimes such as terrorism, espionage, spying and many more can implicate a society's relations with other societies and create international disorder and tension. Law enforcement remains a potent means for maintaining order and dealing with the crime problem in conventional society set-ups. Cybercrimes are crimes committed on the cyberspace using computer and networking technology provided by Information and Communication infrastructures. In a century where "everything" runs on the internet, cybercrime is a new wave of criminal activities that, if not controlled, threatens the very usefulness and survival of the cyber space as a tool for socio-economic development of nations.<sup>82</sup> The bane of the Peel model of law enforcement is that it makes citizens assume minimal responsibility for crime and internal order. Citizens in the twenty-first century therefore see this as the sole responsibility of law enforcement agents and quasi-military police forces who maintain internal order by reacting to completed crimes.<sup>83</sup>

Crime control refers to a theory of criminal justice that places emphasize reducing crime in society through increased police and prosecutorial powers and. Before 1829 crime control is based on social structures that:

- (a) Use general societal condemnation of violations and the violators
- (b) Exact punishment on affront and appease the victim

---

<sup>82</sup>Chawki M. (2009). Nigeria Tackles Advance Free Fraud. *Journal of Information Law &Technology* No. 1. Retrieved June 22, 2015 from [http://go.warwick.ac.uk/jilt/2009\\_1/chawki](http://go.warwick.ac.uk/jilt/2009_1/chawki)>., see also, Longe O, Ngwa, Wada F, Mbarika V. & Kvasny L. (2009). Criminal Use of Information and Communication Technologies in Sub- Saharan Africa: Trends, Concerns and Perspectives. *Journal of Information Technology Impact*, Vol 9, (3). Retrieved June 22, 2015 from [www.jiti.net](http://www.jiti.net)

<sup>83</sup>Brenner S . (2005) Distributed Security: A New Model of Law Enforcement. *John MarshalJournal of Computer and Information Law* VOL.XXIII (4).(article written in 2004), Retrieved June 22, 2015 from <http://www.jcil.org/journal/ articles/ 434.html>.

- (c) Deter future violations by sanctions and new pronouncement appropriate to the instance or new instances or genre of crime
- (d) Reconcile violators and victim(s)

The disorganization of primary societies, urbanization and increase in the scale of crime rendered this method inadequate in dealing with crime on a large scale. In 1829 Rob peel came up with the current conventional model of law enforcement and policing.<sup>84</sup>

Furthermore, four characteristics of real-world crime shaped the way the way the Peel model approach the issue of crime and criminality. These are:

- (a) Proximity between criminals and victims
- (b) The scale of the crime
- (c) Physical constraints that can discourage the criminal(s)
- (d) Patterns of crime with which investigator are familiar.

These facts can be explained by looking at how conventional crimes occur. Violators or criminals and their victims are usually physically proximate in most occurrences. Theft cannot occur neither is rape unless the victim and the criminals have contact. The extents of the crimes are limited by the number of criminals and victims.

Also reality and distance can impose constraints unphysical human activities such as breaking a safe room in a bank robbery, increasing the exertion and resources needed to commit crime thereby aiding the apprehension of criminals and contributing to evidence needed for prosecution.<sup>85</sup>

---

<sup>84</sup>Longe O & Osofisan O. (2011). On the Origins of Advance Fee Fraud Electronic Mails: A Technical Investigation Using Internet Protocol Address Tracers. *The African Journal of Information Systems*: Vol. 3: Iss. 1, Article 2. Pp.1-2. Retrieved June 22, 2015 from <http://digitalcommons.kennesaw.edu/ajis/vol3/iss>.

<sup>85</sup>Brenner S and Clarke (2005). Prosecution of Information Technology Crimes *John Marshal Journal of Computer and Information Law VOL.XXIII*. (4). Retrieved June 22, 2015 from <http://www.jcil.org/journal/articles/434.html>.

For instance, criminals can drop business cards or purchase receipts at the crime site unknowingly; they can even leave DNA<sup>86</sup> evidence which can aid law enforcement in tracking them down. Demography and criminal profiling can contribute to apprehension and tracking criminals. For instance, there are certain forms of crime common to resource poor environment or individuals while others can only be committed by economically vibrant individuals or organizations and economically advantaged individuals.

Spatial limitation is an aid to real world crime and the one to one relationship between victims and violators yields the assumption that crime is committed on a limited scale.

Cybercrime poses a lot of challenges to the Peel Model. These challenges are not more of adopting or creating new laws that criminalize certain cyber activities but more of law enforcements' ability to react to cybercrime. This is because cybercrime does not share some of the characteristics of conventional crimes that shaped the current Peel model of law enforcement.

The cyberspace invalidates the very basic tenets on which the Peel Model is built. For instance in the cyberspace, the following statements are valid:

- a. No proximity is required between victims and violators. These crimes are committed, in various forms and guises, across continents. Anonymity is a factor on the cyberspace that the criminal use to their advantage.
- b. Cybercrime is faceless crimes unless the criminal chose to meet the victims as is the case with fraudulent cyber transactions, pedophiles and online pornography.
- c. One to one victimization therefore becomes invalid as the crime process is automated.

---

<sup>86</sup> "DNA" stands for deoxyribonucleic acid. DNA profiling or genetic finger printing, reveals a suite of variations in the genetic code of every cell in the body. Retrieved June 22, 2010 from en.wikipedia.org/wiki.DNA.

- d. The criminal(s) can move from one location to another to beat the best internet address protocol location tools or to avoid phone call traces. They can engage a proxy server to mask or masquerade their actual locations.
- e. The criminal(s) can commit crimes against individual or individuals in multiple of places at the same time therefore, there is multiple victimization from multiple locations or from a single location.
- f. Therefore there is a one to many scenarios in this case which clearly invalidates the conventional crime tenets.
- g. These criminal (s) can use systems and other unsuspecting people or organization systems' as zombies or detours without their knowledge thus incriminating other victims in the course of committing these crimes. This means victims can be turned to criminals even without their knowledge and further used to commit multiple crimes in multiple locations. This creates a chain effect and more victims through a singular event.
- h. In cybercrime, the theory of pseudo-resource ownership is established as the cybercrime scenario since these criminals possess the potential to defraud individuals and organizations of different kinds of resources without their knowledge while such individuals or organizations still hold the physical or evidence that the resources is still in their possession. This is the case when credit card information are hacked and funds transferred in sequence out of such accounts over a period of time without the owner of such account suspecting any foul play since the so called cards and the security or pin numbers are still in "their possession".

From the foregoing, it is obvious that the current model of law enforcement cannot effectively militate against cybercrime as cybercrime deviates in nature, radically, from the

characteristics of conventional crime. Anonymity, jurisdiction of law, the pseudo-resource ownership theory, global reach and multiplication of crime and its victims in multiple locations poses a great challenge to the application of current policing strategies to address cybercrime.

The response of law enforcement to conventional crime is subtly patterned after how the military responds to external aggression. Law enforcements effectiveness is aided by the stochastic but localized occurrence of these crimes.

Unfortunately, technology, especially the internet, now necessitates the need for a paradigm shift from policing concepts and models that focused on localized crime to those that can deal with crimes that radically deviate from the localized trend. Technology has produced a new social structure that flattens conventional crime structure thereby eroding the boundaries between internal and external threats.

A writer's opinion<sup>87</sup> is that, amongst other, in the efforts to fight cybercrimes, users must be empowered as the last line of defense as compared to the Peel model where the most responsibility rests on the Police and other law enforcement agents. He proposed a User centric socio-technological model that employs technology, social theory, policy, education and awareness as tools to mitigate the cybercrime problem. This model offers an interactive real time challenge, demand response platform that aids identification, reporting, apprehension and prosecution.

His model takes into consideration the fact that cybercrime does not share the common characteristics on which the *Peel theory* rests and that the criminals plug into the webs cape through remote proxies. The model provides valves that assist users identify malicious intentions through a multi level access control mechanism. Wada employ the cyber infrastructure as a tool

---

<sup>87</sup> Wada F. (2012, May). Policing the Cyber-Space – Is the Peel Theory of Community Policing Applicable? *Computing, Information Systems & Development Informatics Journal*. 3(2):51-56.

that can provide synergistic interactions between users and law enforcement. These infrastructures consist of the user interface, web browsers, the internet service provider (ISP) and the likes and subsequently proposed that ISPs should send report about suspicious traffic to law enforcement and e-mail interface should have facilities that can automatically connect users to law enforcement to report suspicious cyber invasion and criminal activities. “In fact, users should be empowered through e-mail interfaces to report phishing. Scamming and other cyber violations in real time. Law enforcement should be connected through a distributed network such that cybercriminals can be tracked anywhere in the world thus providing a global response”.<sup>88</sup> The reaction to information input into the system will create an effective mechanism for tracking, identification and apprehension of cybercriminals.

Cyber crime has added to the dilemma of the Peel theory for crime control. Though another form of crime, it does not have a one-to-one mapping nature to conventional crimes nor does it share the common characteristics on which the Peel theory rests. The ubiquitous nature of the web coupled with the cloud of users presents a new form of challenge to system security and demand a paradigm shift in the perception, design and implementation of security measures<sup>89</sup>.

Unfortunately, Internet security and web design issues have continued to toe the lines of previous approaches that concentrated on technicalities and usability without scaling security issues in the light of today’s challenges thereby providing a fertile ground for cyber crime to breed. To secure the internet from cyber crime and other abuses, users must not only be made aware of the existence of security flaws and vulnerabilities on the webs cape, they must be empowered in a holistic manner through design, policies, practices and technology to mitigate

---

<sup>88</sup> Ibid

<sup>89</sup> Straub D. and Welke R. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. MIS Quarterly Journal. 22(4);441-469. See also, Schlienger T, Teufel S. Information Security Culture : The Sociocultural Dimension in Information Security Management. In: IFIP TC11 International Conference On Information Security, Cairo, Egypt, 7-9 May 2002. (Report) on Pp. 305-340.

against these risks and to understand the criminals. The performance of such protective schemes and policies must also be measurable as this will provides the basis for enhancements and improvements. Law enforcement must also be willing to revisit its mechanism for reporting, apprehension and prosecution in the light of emerging technologies, issues and concerns.

Furthermore, the challenge in fighting cyber crimes stems from the fact that cyber crimes have been in existence for only as long as the cyber space exists. This explains the unpreparedness of society in general towards combating them. It is noted that the Peel model of community policing suffer some inadequacies with regards to facing the challenges posed by cybercrime. The Internet community must engage in a collective effort to curb the Internet of the demeaning crimes it is helping to fuel. To ignore these important issues is at the society's risk.

The earlier discussion situated the police as a relatively minor, but important, player in the broader network of security that constitutes the policing of cyberspace. By outlining the various challenges faced by local police with regard to globalized offences online, the preceding analysis suggest that the police are in fact ill equipped organizationally, occupationally and culturally to deal with it. However, that is only part of the story. As Crawford and Lister<sup>90</sup> have observed, “during the past decade or so increasing pluralization of the terrestrial policing have been witnessed.”

The public police are becoming part of a more varied and complex assortment of organization and agencies with different policing functions together with a more diffuse array of processes of control and regulation.<sup>91</sup> Crawford and Lister showed that while much policing is now taking place beyond the auspices of the public police,<sup>92</sup> it would be premature to view the

---

<sup>90</sup>Crawford A and Lister S. (2004) The Patchwork Future of Reassurance Policing in England & Wales: Integrated Local Security Quils or Frayed, Fragmented and Fragile tangle web?. An International Journal of Police Strategies & Management, 27 (3):413-430.

<sup>91</sup> Ibid at p.414

<sup>92</sup> Ibid at p.426

partnerships that form plural policing as facilitating a form of ‘networked governance’. In the British terrestrial policing context, the reality, at the moment at least, is that crime and disorder partnerships remain state dominated institutions’.<sup>93</sup> These observations can still inform societal understanding of the police role in cyberspace because of its networked and nodal architecture. The earlier discussion about situating the police demonstrated pluralism in the policing of cyberspace beyond the auspices of the public police. However, the emerging role of the police as digital information brokers<sup>94</sup> has led, during the past decade, to a new neo-peelian role for the public police in which the original peelian principles and values are promoted, but within the networks and nodes of multi agency cross sector partnerships, forums and coalitions. Just as ideas about crime have become globalized, then so have ideas about policing.

It is noted that, not only does internet related offences take place within a global context while crime tends to be nationally defined, but the public police mandate prioritizes some offences over others, particularly where there is a dangerous ‘order’, as in the production of child pornographic images. Furthermore, policing the internet is a very complex affair by the very nature of policing and security being networked and nodal. It is also complex because within this framework the public police play only a small part in the overall policing process, yet the peelian heritage of the police that has long defined their relationship with the state and the public has caused the police instinctively to assert ownership over the policing function.

Cyberspace thus places the public police in a rather contradictory position. On the other hand, the characteristics of cybercrimes of cybercrimes contradict the basic peelian principles of policing, yet those very same principles lead the public to rely upon the police for protection.

---

<sup>93</sup> Ibid

<sup>94</sup>Ericson R and Haggerty K. (1997). Policing the Risk Society. Oxford University Press. United Kingdom .p.238.

This contradiction can be observed in most jurisdictions where policing takes place by consent and even in some where the consent is less apparent. Cybercrimes generate many questions about whether the public police's cultural heritage and traditional constitutional position actually fits them organizationally for a role in policing cyberspace.

However, the contradiction faced by the police, particularly the 'reassurance gap' between crimes experienced and those felt,<sup>95</sup> has led to public concern about cybercrime. This has subsequently shaped the demands made of the police for reassurance, which has been reconciled with the constitution of the peelian principles of policing and the emergence of a neo-peelian agenda across a global span. While this resituates the police as an authority within the networks of security, it nevertheless creates a range of instrumental and normative challenges for them. One of those challenges is to temper the potentially dangerous drift towards the very edge of ubiquitous law enforcement<sup>96</sup> and excite a range of opposing debates. But there is also optimism in the potential for those same technologies to provide important opportunities for police reform.<sup>97</sup> The surveillant characteristics that make technology a powerful policing tool also make it a natural tool for overseeing police practice and for increasing broader organizational and public accountability.<sup>98</sup>

## **5.8 Constitutional and Human Rights Issues**

In the attempt of law enforcement agencies to protect and secure cyberspace against cybercrime, there are often several areas of conflicts with constitutional and human rights

---

<sup>95</sup> Innes M. (2004) Reinventing Tradition? Reassurance, Neighbourhood Security and Policing. *Criminal Justice Journal*. 4 (2):151-157

<sup>96</sup> Vinge V. (2000) The Digital Gaia: As Computing Power Accelerates, The Network Knows All and it's everywhere, *Wired*, publication 8 (1), Retrieved June 22, 2015 from [www.wired.com/wired/archive/8.01/forward.html](http://www.wired.com/wired/archive/8.01/forward.html).

<sup>97</sup> Chan J, Brereton D, Legosz M and Doran S. (2001) E-Policing: The Impact of Information Technology on Police Practices. a paper presented to the Queensland Criminal Justice Commission in Brisbane, at p.9

<sup>98</sup> Newburn T and Hayman S. (2001) *Policing CCTV and Social Control: Police Surveillance of Suspects in Custody*, Cullpton: Willan Publications. UK. p.79.

provisions. This work identified some of these arm-strings to law enforcement and they are discussed below.

Part 1 of The Constitution of Federal Republic of Nigeria 1999 (as amended), provides for the supremacy of the constitution<sup>99</sup> and section 1(3) provides thus: *“If any other law is inconsistent with the provisions of this Constitution, this Constitution shall prevail, and that other law shall to the extent of the inconsistency be void.”*<sup>100</sup>

The legislators in enacting the recent Cybercrime Act, 2015<sup>101</sup> and the drafters of the National Cybersecurity Policy<sup>102</sup> must have been guided by the provision of the Constitution. A cursory look at the cybercrime Act, 2015, reveals that it cleverly avoided any area of inconsistency with the 1999 constitution especially as it concerns first, right to personal liberty and second, right to private life<sup>103</sup> as provided in the 1999 constitution of Federal Republic of Nigeria. The implication of any clash with the constitution is that such area of conflict would have afforded defense lawyers to take undue advantage of the provisions under fundamental rights in the Constitution to argue the cases of their clients and this, arguably, can be fatal to the effectiveness of the Act.

Nigeria, no doubt, have taken the right step by enacting a legislation to control cybercrime domestically. This has put Nigeria among the comity of Nations with a cybercrime Act, Globally and Regionally. However, cybercrime being a global phenomenon, there is need for bilateral and multilateral agreements and treaties with other countries in order to achieve the full potentials of the provisions of the Act. Therefore, collaborations and co-operations with other countries will be necessary to be able to effect some sections of the provision of the Act.

---

<sup>99</sup> Section,1 (1) Constitution of the Federal Republic of Nigeria 1999 (as amended).

<sup>100</sup> Ibid at Section 1(3)

<sup>101</sup> Cybercrime Prohibition Prevention etc Act, 2015. For a detail analysis of this Act, see chapter 3.5 iii,(q) of this work.

<sup>102</sup> National Cybersecurity Policy, 23, December 2014. See chapter 3.4 iii (o) of this work for a brief analysis.

<sup>103</sup> Sections, 35(1) and 37 (1999) Constitution as amended

For instance, section 51<sup>104</sup> provides that “Offences under this Act shall be extraditable under the Extradition Act”.<sup>105</sup> Section 52<sup>106</sup> (1) (a) (b) (2) (3) provides for request for mutual assistance from any agency or authority of a foreign State. Section 53 (1) also provides thus: “Any evidence gathered, pursuant to a request under this Act, in any investigation or proceeding in the court of any foreign State,- - -. Similarly, section 54<sup>107</sup> provides for a form of request from a foreign State. All of these will require collaboration and co-operations with the State concerned in any given case or time. For these provisions to be executable there must be appropriate and adequate treaties between Nigeria and such countries.

Again, just like the process of enacting the domestic statute, care needs be taken in entering into any treaty, bilateral or multilateral agreement with countries so that the provision of such treaties and agreements on cybersecurity do not conflict with the provisions of the 1999, Constitution of Federal Republic of Nigeria as amended.

It is submitted that if imitation is the best formula for survival in competitive global trend, then, the mimic of legal tadpoles of other technologically developed countries and their experiences are required therapy to guide our decisions in this regard.

Undoubtedly, United States of America is a more experienced and technologically developed country than Nigeria in the area of cyber space. This work will therefore examine the Constitutional issues with treaties and foreign agreements of United States as it relate to cyber crime. Although the United States Constitution does not apply in Nigeria, its guidelines can serve as a major impact on entering into foreign agreements and treaties by Nigeria.

---

<sup>104</sup>Cybercrime Act, 2015Op.cit.p126

<sup>105</sup> Cap. E25,LFN,2004

<sup>106</sup>Cybercrime Act, 2015Op.cit.P.126

<sup>107</sup> Ibid

Worthy of note is the fact that, the Constitution of United States of America has some similarity with the Constitution of the Federal Republic of Nigeria 1999 (as amended) to the extent that; “*A rule of international law or a provision of an international agreement of the United States of America will not be given effect as law in the United States if it is inconsistent with the United States’ Constitution*”<sup>108</sup>

This provision is in-pari-materia with section 1(3) of the 1999 Constitution of the Federal Republic of Nigeria as amended. To the extent of the above provisions any cyber treaty that conflicts with the United States Constitution will not be given effect, even though such a failure does not excuse the United States under international law.<sup>109</sup> It is therefore submitted that countries should identify potential conflict areas early in the negotiation process.

The scope of this research does not permit an exhaustive review of all of the potential constitutional issues of United States that could arise under various treaty proposals to cover cyber crime and information terrorism but it is instructive to note in passing a few salient concerns.

*First Amendment*, how the first Amendment applies in cyber space is an issue that has only recently been addressed directly by the courts. Perhaps the most significant decision in this area to date is *Reno v American Civil Liberties Union*,<sup>110</sup> which recognized First Amendment Protections for Internet Communications comparable to the expansive protections afforded print publications, while striking down as unconstitutional a portion of the Communication Decency Act (CDA).<sup>111</sup> However, the Supreme Court summarily affirmed another case that upheld a

---

<sup>108</sup> Section, 115 (3) United States Restatement of Foreign Relations Law.

<sup>109</sup> Ibid, at section 115,

<sup>110</sup> 117 S.ct. 2329, 2344 (1997).

<sup>111</sup> Pub. L. No. 104- 104, Title v, Section 501- 561, 110 stat. 56, 133 –43 codified at 18 U.S.C.Sections,1462, 1462 note, 1465, 2422..

different portion of the Communication Decency Act, which appeared to share a similar First Amendment Deficiency.<sup>112</sup>

Thus the first Amendment may pose problems for a computer crime treaty,<sup>113</sup> especially as to content-related computer crimes. This is not unique to computer crimes treaties it has been a consideration in some other treaties. For instance in the United States Senate hearings on the Genocide Convention there was concern that the prohibition on “direct and public incitement to commit genocide” could run a-foul of the First Amendment.<sup>114</sup>

The United States did eventually ratify the Genocide Convention in 1986 with a reservation that appeared to “finesse” the potential conflict. It stated that “noting in the Convention requires or authorizes legislation or other action by the United States of America prohibited by the Constitution of the United States as interpreted by the United States.”<sup>115</sup> Nevertheless, as noted above, other than the computer related child abuse proscription and possibly a racial hatred proscription, other content related crimes under the treaty would merely be extensions to the cyber sphere of those offenses that are already criminalized in United States. Thus, the United States would not be required to create new content-related crimes in areas subject to being trumped by the First Amendment.

There is arguably a comparable issue under International Law. Under article 19 of the Universal Declaration of Human Rights, there is a right “to seek, receive and impart information

---

<sup>112</sup> *Apollo media corp. v. Reno*, 19f. Supp. 2d 1081 (N. D.cal.1998) aff’d 1999. U.S. LEXIS 25 75 (U.S.April 19, 1999).

<sup>113</sup> Anne Wells Branscomb (1995). Anonymity, Autonomy and Accountability: Challenges to the first Amendment in cyber space. *Yale Law Journal* 104 (1639):98-130.

<sup>114</sup> See, United State Senate Committee (1971, May 4) on Foreign Relations International Convention on the Prevention and Punishment of the Crime of Genocide, S. EXEC Rept. No 92 –6, 92d Cong. 1<sup>st</sup> Sess.1-18

<sup>115</sup> Jordan J. Paust, Bassiouni M, Michael S, Jimmy G, Leila S, Bruce Z. (1996, June) *International criminal Law: Cases and Materials*. Carolina Academic Press. at p.104 .( The authors reproduced a1986 Lugar/Helms/Hatch ,provisions as Approved by Foreign Relations Committee)

and ideas through any media and regardless of frontiers”<sup>116</sup>. This right, however, is “peppered” with exceptions. Thus:

- a) It cannot be exercised in opposition to the principles and purposes of the United Nations;
- b) It may be subjected to certain restrictions provided by the law and which are necessary for the protection of national security territorial integrity, public safety, public health and public morals;
- c) It may be also restricted in order to prevent crime and disorder, as well as the disclosure of information received in confidence, and for maintaining the authority and impartiality of the Judiciary, meeting the just need for general welfare in a democratic society or protecting the rights of the others.<sup>117</sup>

*Fourth Amendment*, any effective treaty addressing Cyber Crime must also address the mutual assistance that will be provided in searches and seizures. These issues raise potential conflicts under the fourth Amendment to the United States Constitution. The fourth Amendment prohibits unreasonable searches and seizures conducted by the government and require probable cause for the issuance of warrants.<sup>118</sup> It Emphasizes:

The right of the people to be secured in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.<sup>119</sup>

---

<sup>116</sup> Universal Declaration of Human Rights, article. 19,(1948)

<sup>117</sup> Universal Declaration of Human Rights, arts. 19 and 29, the covenant on civil and political Rights, art. 19; and the European convention on Human Rights, article 10.

<sup>118</sup> U.S. Const. amendment. 1v.

<sup>119</sup> Ibid

These requirements cannot be overridden by treaty. Nevertheless, the searching and seizing of computer data has created unique issues under the Fourth Amendment.<sup>120</sup> Many of which have still not been resolved authoritatively by the courts<sup>121</sup>

Computer data takes many forms, including the content of stored data, e-mail, chatroom discussions, net meetings, Internet Telephone Calls, newsgroup postings, and more. Nor are these categories exclusive. Thus, for example an e-mail message may be pulled off a server and stored, either read or unread, on a local hard drive as stored data. Analogizing computer data to the contents of personal mail or a private phone call, documents in a file cabinet or a closed container, or entries in a personal address book or a diary have attempted to fit modern concepts into older, established ones. The fit has not always been satisfactory.<sup>122</sup>

The ease with which data can be deleted, modified or moved outside the jurisdiction of any particular warrant-granting judge or magistrate all raise additional problematic issues. Nevertheless, the lead proponent for a treaty in this area, the Draft Convention on cyber crime, largely skirts these issues by requiring cooperation among states party by resort to either existing international agreements or the convention, whichever is most favorable, within the limits of a state's domestic law.<sup>123</sup>

*Fifth Amendment*, special problems may be encountered when investigating authorities attempt to obtain evidence from encrypted files. An appendix to a recent European recommendation on how to deal with procedural issues related to computer crimes included the following paragraph:

---

<sup>120</sup> U.S. Department of Justice (1994) Federal Guidelines for searching and seizing computers. Retrieved June 13, 2015 from <http://www.ignet.gov/ignet/library/search.html>.

<sup>121</sup> Francis A. Gilligan & Edward J. (1998) Cyber Space: The Newest Challenge for Traditional Legal Doctrine. 24, Rutgers computer & Technology Law Journal. p.305, (1996-1997) keeping secrets in cyber space: Establishing fourth Amendment protection for Internet Communication. Harvard Law Review. 1591(110):83.

<sup>122</sup> Raphael winick. (1994). Searches and Seizures of Computers and Computer Data. Harvard Journal of Law & Technology. 8 (75):76.

<sup>123</sup> Council of Europe Convention (COE's) Draft Convention, Op cit, p. 280 at Article. 7.

(10) Subject to legal privileges or protection, investigating authorities should have the power to order persons who have data in a computer system under their control to provide all necessary information to enable access to a computer system and the data therein. Criminal procedure law should ensure that a similar order can be given to other persons who have knowledge about the functioning of the computer system or measures applied to secure the data therein.<sup>124</sup>

This provision does not necessarily produce any conflict with existing law in the United States because of its lead in qualifying phrase. Nevertheless it is important to understand how the overall provision would be interpreted within the United States. Current case law in the United States which holds that requesting the computer password from a suspect in order to access the suspect's computer data is covered by the Fifth Amendment's right against self-incrimination.<sup>125</sup> *In Doe v United States*,<sup>126</sup> the majority agreed with the dissent that "be[ing] compelled to reveal the combination to his Wall safe"<sup>127</sup> would be testimonial compulsion, even though compelling the production of the key to a safe containing incriminating documents would not. The court in an earlier judgment in the case of *Couch v United States*<sup>128</sup> had approved the citing of *United States v Gutema*<sup>129</sup> for the contention that the privilege against self-incrimination existed with respect to memorized combination to a safe. Necessarily, this also means that absent a proper advisement of rights under *Miranda*,<sup>130</sup> prior to the request for the computer password its divulgence may be deemed "fruit of the poisonous tree".<sup>131</sup> This does not preclude the government from obtaining the same information through a search or seizure conducted in

---

<sup>124</sup> *Ibid*, Appendix to Recommendation No.R (95) at Para. 17

<sup>125</sup> *See, Doe v. United States*, 487 U.S. 201, 210 n.a (1998).

<sup>126</sup> *Ibid*.

<sup>127</sup> *Ibid*

<sup>128</sup> *Couch v. United States* 409 u.s. 322, 333 & n.16 ( 1973)

<sup>129</sup> *United States v. Gutema*, 272f. 2d 344 (2d cir 1959).

<sup>130</sup> *Miranda v. Arizona*, 384 U.S. 436 (1966)

<sup>131</sup> *Oregon v Elstad*, 470 U.S. 298. 306 (1985)

compliance with the Fourth Amendment if the password has been recorded and there exists probable cause as to its where-about.<sup>132</sup> It also does not preclude the government from compelling an innocent third party from divulging the password, Since the Fifth Amendment only protects against self-incrimination.<sup>133</sup> And of course, an appropriate grant of immunity could even compel the disclosure from the suspect, though the immunity would necessarily have to be broad enough to foreclose the use of any evidence gained directly or indirectly from its use.<sup>134</sup> The United States Justice Department's Federal Guidelines for searching and seizing computers suggest that limited immunity could disgorge a computer password from a suspect:

“In some cases it might be appropriate to compel a third party who may know the password (or even the suspect) to disclose it by subpoena (with limited immunity, if appropriate)”.<sup>135</sup> The conclusion that limited immunity would be sufficient does not logically follow from the case law, though the issue is not foreclosed due to some inconsistencies in the Supreme Court's decisions in this area.

Cryptography may provide a technical fix for Supreme Court's allowing the invasion of one's private papers. However, the effectiveness of that fix will depend on whatever the court holds that immunity from the compulsory production of cryptographic key extends to the incriminating documents decrypted with the key. Logic suggests that the court should so hold. However, the court's inconsistencies in this area suggest the limits of logic. The court has consistently reconstructed Fourth and Fifth Amendment precedents to move away from historical practice. This reconstruction is in part responsible for the court's inconsistencies.<sup>136</sup>

---

<sup>132</sup>Reitinger P. (1996) Compelled Production of Plaintext and Keys. University of Chicago Legal Forum (u.chi Legal f.171) LexisNexis.USA. pp.227-229.

<sup>133</sup>*Couch v. United States*, 409 U.S 322, 328 (1973). (The constitution necessarily does not proscribe incriminating statements elicited from another)

<sup>134</sup> *Wong Sun v. United States*, 371 U.S. 471(1963).(See ,for the beginning of line of cases on doctrine of “ the fruit of the poisonous tree”)

<sup>135</sup>US. Department of Justice (1994) Federal Guidelines (No.55) for searching and seizing computers. Retrieved March 18, 2014 from, <http://www.ignet.gov/ignet/library/search.html>.

<sup>136</sup> Sergienko G. (1996) Self Incrimination and Cryptographic Keys. University of Richmond Journal of Law & Technology. 2 (I):138-142.

**(i) Conflicts between Cybersecurity Law and Free Speech**

The right to freedom of speech is enshrined in section 39 (1) and (2) of Nigerian Constitution 1999 as amended<sup>137</sup> and also in a number of treaties, of which article 10 of European Convention on Human Rights is naturally the most important.<sup>138</sup> The rules governing freedom of speech are well defined in Nigeria. Freedom of speech does not in-itself justify every utterance. When assessing whether a given publication is wrongful, it is necessary to weigh two social concerns. On the one hand, the concern that individual citizens should not be exposed to grossly defamatory comments through publications in the press, and on the other, the concern that scandals or abuse of power should not be allowed to continue because the population at large is unaware of them. In principle neither of these two fundamental rights has priority.<sup>139</sup> Which of the two rights is decisive in a given case depends on the circumstances and in particular on the gravity of the defamatory comments and the extent to which the comments were supported by the facts available at the time the article was published or the television program was broadcast. Moreover, cyberspace is a new community, but one which closely resembles the ordinary world. Many worldly activities have a digital variant, for example, mail, shopping, gambling, sex and many more. Cyberspace adds a new dimension to the gathering and dissemination of information.

The freedom of expression assumes even larger forms. For instance the dissemination of information is faster, easier and takes place on a global scale. By the same token, however, dubious and even indisputable objectionable opinions like Nazism and racism are also disseminated faster and on a larger scale.

---

<sup>137</sup>Constitution of the Federal Republic of Nigeria 1999 (as amended)

<sup>138</sup> See, also art. 19, International Convention on Civil and Political Rights and art. 19, Universal Declaration of Human Rights.

<sup>139</sup>See, HR 4 March, 1998, NJ (Dutch case Law) 1989, 361, HR 6 January 1995, NJ 1995, 422 and HR 21 January 1994, 473. (According to the Netherlands Supreme Court (HR) there is no reason to accept any ranking of these two rights)

The internet is regarded by many as a legal vacuum in which the only norms are those imposed by self-regulation or netiquette. The assumption that the rules of the normal legal system do not apply is particularly prevalent within the internet community itself. The users tend to think of themselves as on the high seas, beyond the reach of any national law.

However, they conveniently forget that the inhabitants of cyberspace are also citizens of different countries. Under the law of these countries, the users of the internet have rights and duties. The cyberspace inhabitants are being forced to face reality in various ways. In the area of copyright, for example, the collecting society for performing rights in musical works (BUMA) has announced that it wishes to receive a sum of 10 guilders a month from every internet user who puts a musical fragment of less than 30 seconds on his web site. This would be for the use of the work. Needless to say, this proposal has provoked a hostile reaction and an anti-BUMA page has been opened on the internet.<sup>140</sup>

No specific legislation geared to the internet exists in the Netherlands and a case law that exists indicates that the rules of the ordinary world apply. For example, the police recently arrested a man suspected of distributing child pornography on the internet. And a firm by the name of Vuurwerk was confronted with a copy right infringement claim. It had offered its subscribers access to its so-call Webtel-service, through which telephone numbers and other data from subscribers to push to talk (PTT) telecom could be obtained. For this service, Vuurwerk had copied a compact drive (CD) phone guide developed by PTT telecom. Vuurwerk was ordered to desist because it was infringing the copyright of PTT Post.<sup>141</sup>

In another case, however, an action brought on the ground of copyright infringement was dismissed. This concerned proceedings brought by the Church of Scientology against various

---

<sup>140</sup> Retrieved June 18, 2015 from Facebook/ bumanetherland

<sup>141</sup> Haarlem. (10 July 1996) Verdict in summary proceedings.( sitting as President of the District Court of Netherland) ( unreported suit nr. 27409/KGZA 960358)

service providers and a single information provider.<sup>142</sup> The scientology case was often portrayed in the media as a battle about freedom of expression. The church of scientology was said to be using the copyright laws to gag its critics. However, the case was in fact concerned solely with copyright. The claim by the church of scientology to copyright protection in no way detracted from the right to freedom of expression. The defendants remained free to criticize the church in their own words, but in doing so they could not make use of certain protected works.

Opponents of the church of scientology had put the full texts of document written by L. Ron Hubbard, the founder, on their own home page. The document had been obtained from the so-called Fishman Affidavit, which had been lodged in litigation in the United States. The church of scientology sought an order that the material be removed. The defendants entered a defense that the documents did not enjoy copyright protection and that the dissemination was permitted by virtue of article 10 of the European Convention. At the time of the interim injunction proceedings, however, the defendants had replaced the original text on the internet by alternative texts which merely contained quotations from the documents. The president of The Hague District Court held that publication of these quotations did not constitute a copyright infringement. The president did not rule on the relationship between copyright and the right to freedom of expression.

In a recent news broadcast,<sup>143</sup> an artist in South Africa painted the picture of the President of South Africa, Jacob Zuma, with the zip of his trousers down and his genital protruding out, all in the name of freedom of expression. This was at the time that the President was being criticized by some citizens in South Africa for marrying a sixth wife. Arguably, the right of the artist to

---

<sup>142</sup> Marcel D. (1996) Internet Providers not Held Responsible for Wrongful Acts of Internet Users. Institute for information law Journal, University of Amsterdam. 4 (3/2):1 (Scientology vs XS4ALL cs, the verdict in a summary judgment of 12, March 1996, the President of District Court of Hague, Den Haag, ruled that internet providers can in principle, not be held responsible for wrongful acts of users,...)

<sup>143</sup> James G. (Executive producer). (2012, May 27). Focus Africa (television program United Kingdom BBC, Africa Unit.

freedom of expression at this juncture has conflicted with the president's right to private and family life and he should be sanctioned appropriately.

**(ii) Data Protection and Privacy Infringement Liability Regimes: Civil and Criminal**

Eighty nine countries have adopted privacy or data protection laws.<sup>144</sup> A critical element of many of these laws is how they regulate international data flows as a mechanism for protecting individual privacy and enforcing national policies.

The Organization for Economic Co-operation and Development (*OECD*) adopted Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data in 1980. Data protection laws were passed in a number of European countries in the 1970s. At a regional level, Convention 108 of the Council of Europe was passed in 1981 and the original EU Data Protection Directive was enacted in 1995 (*European Directive*)<sup>145</sup>. The European Directive places significant emphasis on the location of data, restricting its transfer to countries that do not have similar privacy protections. In contrast, the Asia-Pacific Economic Co-operation (*APEC*) enacted its voluntary Privacy Framework, which provides protection for personal data on an accountability basis in 2004.

When the OECD Guidelines were adopted, the Internet had not emerged. Protecting privacy by restricting the geographic movement of personal information was possible. The data was typically in a physical form whether it is written, tapes or other physical medium. This continued to be the case in 1995 when the European Directive was implemented.

At this time, business, the economy and technology have fundamentally changed. The economy is increasingly international. Data processing is growing dramatically in importance due to increased data usage and the value of different forms of data. The global economy is

---

<sup>144</sup>Graham G. (2012, 6 February) Global Data Privacy Laws: 89 Countries, and Accelerating. Social Science Research Network. Retrieved June 22, 2015 from <http://www.itu.int> > GSR12 >

<sup>145</sup> European Union, Directive, 95/46/EC.

currently undergoing an “information explosion” which can “unlock new sources of economic value, provide fresh insights into science and hold governments to account.”<sup>146</sup>The advent of the Internet and now the proliferation and potential value of cloud services require a careful re-evaluation of whether the provisions of these guidelines and regulations for the protection of privacy need to be fundamentally re-evaluated, re-constructed and harmonized to be “fit for purpose” at a global level.

This part will make a brief review of the existing privacy and data protection frameworks in Nigeria, the European Union, generally, and as implemented in the UK and the United States. It is noted that several countries have also implemented this framework, but the scope of this research is limited to the above mentioned countries.

Nigeria is the initial focus with a very recent Act, enacted only on 15<sup>th</sup> of May 2015.<sup>147</sup> Section 16 provides for unauthorized modification of computer systems, network data and system interference. Section 16(1) particularly provides that: “A person who, with intent and without lawful authority, directly or indirectly modifies or causes modification of any data held in any computer system or network, commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦7,000,000.00 or both.” Other sub sections under this section 16 expressly stated the various conditions under which a person may run foul of this provision.

Europe is the next focus and the most extensive because many countries that have adopted or are considering the adoption of data protection regulation have followed the European model. The model is also useful to illustrate the problems presented to business and the economy by the lack of clear and consistent laws implemented seamlessly across international borders.

---

<sup>146</sup> Kenneth C. (2010, 27February) Data, data everywhere, A special report on managing information. The Economist Newspaper Ltd. at Pp.1-13.

<sup>147</sup> Cybercrime Prohibition Prevention etc Act,2015

The focus is on the aspects of the frameworks that are relevant and particularly problematic in the cloud environment. The aspects of privacy and data protection legislation that fundamentally affect cloud computing are: (i) the duties of the party controlling the relevant data, (ii) trans-border data transfer restrictions, (iii) data security and (iv) applicable law.

The recent Global Cloud Computing scorecard published by the Business Software Alliance (*BSA Scorecard*) surveyed 24 Countries to map their relative “cloud readiness”.<sup>148</sup> The scorecard rated seven policy areas the BSA determined to be beneficial to cloud services. The study found a sharp divide between developed and developing countries. “The Republic of Korea and Japan were high on the list, where as Brazil and South Africa were at the bottom.”<sup>149</sup>

First is the review of the frame work under the European Union which, for the purpose of clarity is further discussed under the following subhead:

- a) **Privacy-** The fundamental principle of privacy in the European Union (EU) is set out in Article 8 of the European Convention on Human Rights which states that “everyone has the right to respect for his private and family life, his home and his correspondence.” This right to privacy is not absolute, however, and can be restricted under certain circumstances.

EU privacy law itself has a particular focus on the protection of this personal data and seeks to balance the privacy debate in an era where online content, especially personal data and access to it have developed exponentially. The International Data Corporation

---

<sup>148</sup> Robert H. (2012, February 22) (BSA) Global Cloud Computing Scorecard: A Blueprint for Economic Opportunity. . Retrieved, July.26,2015 from [http:// portal.bsa.org/cloudscorecard](http://portal.bsa.org/cloudscorecard)

<sup>149</sup> ITU (2012, October 19) The Cloud: Data Protection and Privacy Whose Cloud is it Anyway? GSR12 Discussion Paper. p.9. Retrieved July 10, 2015 from [gsr@itu.int](mailto:gsr@itu.int).

(IDC) predicts that the amount of information and content created and stored digitally will grow from 1.8 zettabytes (ZB) in 2011 to over 7 ZB by 2015.<sup>150</sup>

Cloud computing is just the latest technological development driven by this expansion and in turn it brings fresh challenges to the protection of personal data. Data in the cloud may be easy to access and to manipulate, but it is also harder to locate and maintain control over - which makes compliance with EU legislation and, indeed enforcement, particularly difficult.

The EU's e-Privacy Directive<sup>151</sup> is targeted at public communication network providers and states that personal data should only be accessed by authorized personnel for legally authorized purposes, that stored or transmitted personal data should be protected against accidental or unlawful destruction, accidental loss or alteration and unauthorized or unlawful storage processing, access or disclosure. Communication providers are required to implement a security policy for the processing of personal data and national authorities are granted rights to audit such policies. Notification requirements for personal data breaches are also imposed upon the providers.

This has particular and high profile significance in the context of cookies which can be used by operators to gather personal data without the knowledge of the individual user. The amended e-Privacy Directive,<sup>152</sup> which came into effect in 2009, states that Member States may only permit the use of cookies if the data subject has given their consent and has been provided with clear and comprehensive information, particularly in

---

<sup>150</sup>International Telicommunication Union (ITU) (2012, March) "Privacy in Cloud Computing," ITU-T Technology Watch Report, Retrieved July 10, 2015 from <http://www.itu.int/en/ITU-T/techwatch/Pages/cloud-computing-privacy.aspx>.

<sup>151</sup> European Union,(EU) 2002/58/EC.

<sup>152</sup> Ibid at, Article, 5(3).

relation to the purposes of the processing. It is unclear to what extent the legislation will be enforceable from a practical perspective.

- b) **Data Protection-** The current European Directive applies to the collection and processing of personal data within the EU. Personal data is defined broadly as “any information relating to an identified or identifiable natural person,” whilst processing involves “any operation or set of operations which is performed upon personal data”.<sup>153</sup>

The implementing law of an EU Member State is applied to the processing of personal data by an entity established within that state or by equipment situated within that Member State. Entities that determine the purpose and means of the processing of personal data are termed “data controllers”, whilst entities that process the personal data on behalf of the data controller are called “data processors”.

The European Directive specifies minimum measures to be implemented, leaving Member States the option of putting stricter requirements in place. This has resulted in significant variations in data protection laws across the EU, which cause complex and divergent compliance issues for businesses controlling or processing personal data in Europe, and in fact internationally.

- c) **Duties and Responsibilities of the Cloud Client and the Cloud Service Provider (CSP)-**Under the European Directive, data protection obligations are generally imposed upon data controllers, whilst data processors are only subject to specified security requirements. Differing Member State definitions and translations, along with the blurred categorization of a CSP as a controller or processor make this ambiguity particularly significant.

---

<sup>153</sup> International Telecommunication Union (ITU), 2012, October 19) Op cit p.314, at p.10

The cloud client decides the purpose and organization of any processing and thus, as a data controller must accept responsibility for abiding by data protection obligations. The CSP will claim that simply hosting the service gives little control over the nature of any processing by the client and thus it cannot also be a controller. The lack of control means that the CSP will attempt to avoid liability for data quality, compliance with individual rights or the obtaining of any consent in relation to personal data and will often include provisions to reflect this within its terms and condition of service which must be in writing.

The client is often responsible for the full burden of data protection obligations and compliance, despite having little control over the actions of the provider or movement of the data.

d) **Trans-border Data Transfer Restrictions-** Under the European Directive, personal data must not be transferred to non EEA countries that are adjudged to have inadequate personal data protection measures in place. The European Commission has deemed Andorra, Argentina, Canada, the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey and Switzerland to have adequate protection.<sup>154</sup> The US Safe Harbor Scheme is also accepted as adequate for the purposes of transferring certain personal data, subject to some notable exceptions and now to specific due diligence.

Though there are some exceptions to the rule available, cloud computing is typically conducted without a stable location and providers are unlikely to be based only in the specified countries. The customer may not be able to ascertain the real time location of

---

<sup>154</sup>International Telecommunication Union(ITU, 2012, October 19),Op.cit. p.314 at.78 (Subject to the application of the Personal Information Protection and Electronic Documents Act.)

data that is being processed or stored. Of course, neither will regulators be obliged to enforce the restriction be able to ascertain this information.

The Independent Data Protection Working Party established under Article 29 of the European Directive (*Working Party*) has recently stated that the US Safe Harbor Certification alone may not be deemed adequate. Cloud providers should therefore obtain and retain evidence that certification is both up to date and their cloud provider is compliant with safe harbor requirements.<sup>155</sup>

If transfers need to be made to countries outside those that have “adequate” laws, Standard Contractual Clauses (*SCCs*) may be utilised. The *SCCs* contain non-negotiable provisions that set out transfer and security measures that have been deemed adequate by the Commission under Article 26(4) of the Directive. The benefit of using the provisions is reduced by registration and approval requirements that apply in some EU Member States. Registering or obtaining approval can be a very time consuming and bureaucratic process.

International businesses can adopt binding corporate rules (*BCR*) which require approval, for the regular transfer of data throughout their corporate networks.

- e) **Data Security-** As data controllers, cloud clients have an obligation to take “appropriate technical and organizational measures to protect personal data”<sup>156</sup>, thus data security forms an important aspect of the cloud computing contract.

The Working Party has put forward standardized data protection safeguards to be included in such contracts.<sup>157</sup> These safeguards include technical and organizational

---

<sup>155</sup>Ibid at, Article, 29. (2012, 1 July ) (Working Party WP196 on Cloud Computing).

<sup>156</sup>Ibid at, Article 17(1), Data Protection Directive.

<sup>157</sup>Ibid at, Article 29 Data Protection Working Party Opinion 05/12.

measures that aim to preserve the availability, confidentiality, integrity, ability to isolate, accountability, portability and individual rights to the personal data.

Accountability is particularly key to ensuring compliance and thus audit rights are becoming increasingly important to clients. However, the granting of these rights presents a practical problem for providers who use shared infrastructure for their clients. Granting access may itself compromise the confidentiality and security of data belonging to other clients.

Accountability can also be an issue in circumstances where sub-processors are used by the primary cloud provider. Most Member States leave the determination of appropriate technical and organizational measures to data controllers and processors. However, some Member States have prescribed onerous obligations such as requiring data controllers to independently authorize each subcontractor and enter into direct contracts with all processors in the chain.

- f) **Applicable Law-** The nature of cloud computing with shared resources, constantly moving data and multiple processors and subcontractors means that locating data and the processing of it is inherently difficult. The divergent implementation of the European Directive across the EU causes further problems when considering data protection compliance and which law or laws apply to its movement or processing.
- g) **Compliance with Data Protection Requirements-** In a cloud service relationship, as outlined above, clients will typically bear the risk of data protection compliance despite the providers being responsible for the security and transferring of data. A controller must take appropriate technical and organizational measures to be confident of its compliance.

Smaller businesses or individuals may have limited contractual power to negotiate the provider's terms.

Cloud clients are required to exercise due diligence with respect to choosing a provider who offers sufficient guarantees of reliability, competence and security safeguards for the client to be confident it is complying with relevant laws.

CSPs have an opportunity to differentiate their services and enhance business prospects by adopting terms of business and providing assurances to customers as to these processes and compliance. For example, Amazon has created a European Cloud to provide customers with confidence that data will not cross borders in breach of the European Directive. A number of self regulatory codes of practice are being established to address this issue.

Second is the example of the patchwork in the United Kingdom. In the UK, the Data Protection Act 1998 (the *DPA*) forms the primary legislation that implements the Data Protection Directive. The DPA is regulated in the UK by the Information Commissioner's Office (*ICO*). The ICO's role is to provide guidance on data protection compliance, maintain a register of data controllers and investigate and sanction breaches of the DPA.

The UK Courts have narrowed the meaning of personal data in comparison to mainland Europe<sup>158</sup> so that for the data to be subject to the provisions of the DPA, the data must (i) be biographical in a significant sense, and (ii) "focus" on the individual, rather than some other person or transaction or event.

The ICO has wide ranging enforcement powers which include requiring the production of information, requiring a change of operating practices (a breach of which would be contempt of court), audit powers over central government departments, entry and inspection powers (with a

---

<sup>158</sup> Michael John Durant v Financial Services Authority [2003] EWCA. (Court of Appeal)

court warrant) and monetary penalty notices of up to £500,000. Criminal sanctions are rare but remain available in certain circumstances, such as a failure to notify the ICO of a DPA breach. Undertakings from a data controller's CEO are now also seen as a low cost method of enforcement. These undertakings state the failings of the company along with remedial steps that will be taken and are published on the ICO's website.

In the UK the Financial Services Authority is also able to enforce data protection breaches under its own regulatory regime under the Financial Services and Markets Act 2000 (*FSMA*). FSMA places wide obligations on financial services organizations including specific operational rules around data security and handling in its Systems and Controls Rules.

Finally, the patchwork on the United States Privacy and Data Protection. US Legislation changed dramatically following the terrorist attacks of 11 September 2001 with the introduction of the US Patriot Act.<sup>159</sup>

The US Patriot Act permitted the sharing of personal data of anybody suspected of involvement with terrorism or money laundering activities and introduced a requirement for financial institutions to implement anti-money laundering systems. This combination, in conjunction with multi chain processes, has resulted in the possibility of broad access and sharing of personal information. The US Patriot Act has been viewed by Europe as a significant risk to data privacy and has put the Safe Harbor scheme in jeopardy.

The right to privacy has been recognized by the US Supreme Court based on the US Constitution, despite there being no explicit constitutional right contained within it.<sup>160</sup> Many

---

<sup>159</sup>US Patriot Act, 2001. (Uniting and strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism became Public Law no. 107-58)

<sup>160</sup> See for example, *Katz v United States*, 389 U.S. 347 (1967)

states have privacy protections within their own constitutions. Only California has extended the protection of data from government interference into an obligation on the private sector.<sup>161</sup>

The United States has spawned a wide range of narrowly applicable federal and state laws relating to the use of personal data. This patchwork, similar to the lack of harmony in Member State implementation of the European Directive, is incompatible with the nature of cloud computing. However, businesses and government are working to establish and implement credible self regulation and guidelines.

Nationally, the Federal Trade Commission Act<sup>162</sup>(*FTC*) prohibits unfair practices. This has been applied to online and offline privacy as well as data security policies. The FTC also monitors and enforces any breach of the Safe Harbor Rules. However, doubts have been raised about the FTC's enforcement effort with respect to the Safe Harbor Rules. The FTC's first action for breach of the Safe Harbor principles was only in 2011 against Google regarding its Buzz service, for not giving notice or choice to users when it used information collected through Gmail for different purposes.

The Financial Services Modernization Act (*FCMA*) and Health Insurance Portability and Accountability Act (*HIPAA*) regulate the collection and use of financial and medical information, respectively. Among the range of federal legislation, there are specific acts that regulate, for example, the collection and use of email addresses<sup>163</sup> and telephone numbers<sup>164</sup>.

At state level, there are many laws relating to data protection and most states have enacted some form of privacy legislation. Forty-six states have enacted laws requiring notification of security breaches involving personal data. California leads the way with a

---

<sup>161</sup> PLC, Data Protection, USA. (Full list of content ) Retrieved July 26 2015 from, [www.practicallaw.com/dataprotection-mjg](http://www.practicallaw.com/dataprotection-mjg).

<sup>162</sup> U.S.C.15.

<sup>163</sup> Controlling the Assault of Non-Solicited Pornography and Marketing Act. Of 2003. (Long title)

<sup>164</sup> Telephone Consumer Protection Act, OF 1991

developed framework that includes an established Office of Privacy Protection and laws comparable to those in Europe. These include requirements for companies to maintain reasonable security measures to protect personal data<sup>165</sup> and to disclose details of third parties with whom they have shared the personal information<sup>166</sup>.

There has also been a move toward a more European approach at federal level with the issuing of a Consumer Privacy Bill of Rights in February 2012. This is the first comprehensive privacy bill introduced to the Senate in over a decade. The bill sets out fundamental principles that companies should observe, namely that individuals should control the use of their data whilst maintaining access and correction rights, data use should be secure, transparent and consistent with the context of collection, there should be reasonable limits on what data is collected and retained and companies must remain compliant and accountable. There are also proposals for a national security breach notification law<sup>167</sup> and a requirement for reasonable security policies and procedures to protect computerized personal data.<sup>168</sup> These proposals signal dramatic change to American privacy laws. However, they are yet to gain the requisite support in Congress.

It is instructive to note that the EU had in 2012 proposed a reform on Data Protection. Attempt is made here to briefly discuss the proposals.

On 25 January 2012, the Commission published its proposed reforms for data protection legislation within the EU.<sup>169</sup> The proposals contain a Regulation (for general and commercial data protection) and a Directive (for processing in the areas of police and criminal justice). The draft

---

<sup>165</sup> California A.B. 1980 Data Security Law.

<sup>166</sup> California SB. 27 “Shine the Light” Law. Of 2003, (Civil Code Ss,1798.83(b)(1)(A)and (C).)

<sup>167</sup> SAFE Data Act, H.R. 2577. Of ( 2011, July 18) (To protect consumers by requiring reasonable security policies and...)

<sup>168</sup> Data Accountability and Trust Act of 2011, H.R. 1841.

<sup>169</sup> European Union, European Commissions: Commission proposes a comprehensive reform of the data protection rules in EU. (full list of proposal) available at: [www.ec.europa.eu >data-protection](http://www.ec.europa.eu >data-protection). Retrieved, July 26,2015.

Regulation will replace the European Directive which is seen as out of date following numerous technological developments.

The proposals aim to increase an individual's online privacy rights and introduce new obligations on organizations. Contained within a Regulation, the changes will be directly applicable within the Member States in an attempt to harmonize the current "fragmented and outdated" data protection legislative framework. Co-operation between Member States is encouraged with the view that a single data protection regime should reduce red tape whilst ensuring that individuals and organizations are clear on their respective rights and obligations. It is also intended to make compliance more straight forward and consistent.

The key changes that have been proposed include:

- a) National regulatory authorities will have the power to take action against organizations in other Member States in certain circumstances and may issue fines of up to €1million or 2% of a company's annual turnover in some cases.
- b) An expanded definition of personal data that captures any information relating to a data subject and a requirement that an individual's consent must be explicit.
- c) The draft Regulation will have a wider application and include non-EU entities that process personal data that relates to EU citizens.
- d) Organizations will be required to report data breaches without undue delay and, if feasible, within 24 hours of the breach.
- e) There will also be requirements on data controllers to carry out data protection impact assessments, appoint data protection officers and inform third parties of any breaches.
- f) Individuals will be given a new "right to be forgotten" under certain circumstances and will no longer be subject to a fee for subject access requests.

g) Finally, international data transfers will be subject to a more detailed regulatory framework requiring safeguards to be in place and authorities to undertake prior checks, whilst the derogations available to data controllers will be more restrictive.

The proposals were announced at the start of 2012. Their controversial nature has and will attract significant lobbying and debate which could mean long delays before implementation. Indeed, the UK Government is already reported to have stated that Member States should have more flexibility over the implementation of the reforms and has questioned the £3billion value of benefits projected by the Commission.<sup>170</sup>

Finally, it is to be remembered that only these acts are crimes which the law has chosen to forbid. An act, however reprehensible it may be, is not a crime unless prohibited by law.

Section 2 of the Criminal Code defines offences (or crime) as “act or omissions which render the person doing the act or making the omission liable to punishment under this code.” One of the hallmarks of criminal punishment is the establishment of blameworthiness on the part of the accused person before he can be subjected to criminal punishment. Also, the law prescribing an offence and the punishment thereto must be certain<sup>171</sup>. It is noteworthy that statutory problems as it relate to cyber crime are not peculiar to Nigeria. Unlike the constitutional conflicts considered in detail in (sub section 5.8) of this chapter, to the extent a newly executed treaty conflicts with existing domestic statutes, the treaty would supersede the statutes.

Generally, existing treaties provide only sporadic and piecemeal assistance in pursuing cyber criminals across state borders. As examined under jurisdictional issues in chapter two (2.5) of this work, the mutual legal assistance treaties (MLAT) have general application to the

---

<sup>170</sup>International Telecommunication Union (ITU 2012, October 19) Op.cit.p.314, at.13.

<sup>171</sup> See section 36 (12) C.F.R.N. 1999. See also the case of *Aoko v Fagbemi (1961) 1 A.N.L.R. 490*, The Latin maxim is “Nolla poena Sina Lge” see also *Josiah v. state (1985).I.N.S.C.C. ratio 40 at 145* where Oputa J.S.C (as he then was ) likened justice to a 3 way traffic i.e. Justice for the accused, Justice for the complainant and justice for the society whose law is broken. (This presupposes that except an act is criminalized by law it cannot be an offence.)

investigation of any crime, including cyber crimes. The character of such assistance often needs to be qualitatively different in cyber crime cases. Nonetheless, there would be a great benefit from a cyber crime treaty that addressed these concerns. The response to information terrorists that threaten the national security of nation-states may vary from or be in addition to the remedies provided under traditional computer crime statutes or treaties. This is to say that while a proposed computer crime treaty may be an adequate starting, it must be realized that on the spectrum of information Acts, information terrorism may more closely resemble information warfare than cybercrime and as such may have additional remedies.

The law enforcement entities will face ever-increasing challenges in investigating and prosecuting Internet and other high-tech crimes. The Internet and high-tech telecommunications have created an environment in which interpersonal and commercial relationships will increasingly involve internal (inter-state) and international transactions, while national authorities remain bound by much narrower jurisdictional limitation.

Critical infrastructure protection is an issue with which the law enforcement will have to contend in the future. As critical national functions increases, it will depend on information networks and are thus susceptible to disruption or security breaches by unauthorized persons. Moreover, it is now possible to attack these infrastructures with far less preparation and expense than in the past. Going by the experience of advanced countries in this area, state and local law enforcement agencies are frequently the recipient of threats against critical infrastructure components and many times are the first responders to attacks on them.

The most prevalent form of cybercrime in Nigeria is the use of internet to defraud residents within and outside the country. This is big challenge to e-Commerce as transactions are now carried out with a high level of fearful caution. This developed skepticism is unfavorable to

business, coming on the heels of recent transition to cash-less economy. Strategies for combating crime and money laundering within cash-less economy constitutes a major additional task created for the police by the system.

Addressing these issues must become a high priority. The enactment of the Cybercrime Prohibition Prevention Etc Act, 2015 is the right step in the right direction. The establishment of Federal Training and Technology Programs should be the next logical step. Both actions and future study are essential if law enforcement is to realistically combat this crime.

## CHAPTER SIX

### SUMMARY AND CONCLUSION

#### 6.1 Summary

The burgeoning threat posed by cyber crime and information terrorism will require those who increasingly rely on computers and the Internet, to become more vigilant and to employ greater protective measures. It will also require effective laws that can be used to prosecute those who attempt to disrupt cyber activities. As cyber criminals have become progressively more sophisticated and internationalized, the ability of a single state to effectively prosecute those who attack it from and through other states has become increasingly complex. In today's highly networked world, state's borders pose no obstacles to cyber criminals, but do create huddles for prosecutors and law enforcement agents.

Existing jurisdictional principles recognized under customary international law provide potential avenues for applying a state's domestic law to cyber criminals abroad under certain circumstances. Where there are existing mutual legal assistance treaties between member state and "letter rogatory", they provide a patchwork of support for the collection of and preservation of evidence in criminal cases generally. Thus, there is already a rudimentary basis for dealing with cyber criminals and information terrorist. However, the increasingly ominous threat posed by cyber crime calls for a more comprehensive, cohesive and effective approach for dealing with this recent but growing problem. It is submitted that while a domestic legislation on cyber crime is the primary approach, there is no doubt that a multilateral treaty is the ultimate and an "apropos" response to all of these.

One of the first challenges will be to adequately define the spectrum of cyber crimes. The current Draft Convention may be overshooting the mark by including content-related offences

and intellectual property crimes. To that extent, the inclusion of these crimes needlessly bogs the process down; it would be preferable to go forward with the treaty without them at this time. Protocols can supplement the treaty at such time as these issues become better worked out. The crimes must also be written without technology – specific language and concentrate on broadly proscribing the harm caused rather than the technology or methodology used. Otherwise, any resulting treaty will promptly become obsolete as technologies change or criminals alter their methods to circumvent the specific proscription. Overall, the current Draft Convention appears to meet this challenge fairly effectively.

The next most important objective of an international treaty should be to establish broad bases for the exercise of prescriptive, adjudicatory and enforcement jurisdiction. The Draft Convention falls short in the first two and achieves only mixed results on the last. The Draft Convention addresses jurisdiction without further modification. In context it appears to be addressing prescriptive and adjudicatory jurisdiction only. In fairness, it is evident that the section-addressing jurisdiction is still being re-worked. The current provision would appear to limit jurisdictional bases already available under customary law without even adding the benefit of consensual jurisdiction. Thus, the only real benefit jurisdictionally is that the convention would standardize cyber crimes thereby making extradition easier by overcoming dual criminality roadblocks. It does not, however, proscribe other setbacks to jurisdiction, such as the political exception or the exception some countries interpose for nationals of their own country.

Enforcement-wise, the Draft Convention appears to address some of the unique concerns to the prompt collection and preservation of computer data. Its view to advancing an international form of “hot pursuit” is a boom to investigators, but a bane to privacy rights advocates, especially if this Convention were to be eventually opened to any country, which

would seem to be the necessary end goal. As currently drafted, the hot pursuit provision is quite narrow, and under the conditions authorized, may have been a course some countries would have afforded themselves anyway, so the provision may merely be a way of providing regulation and additional safeguards. This issue requires additional review due to the significant potential ramification.

Overall, the Draft Convention is a welcome first step in responding to the worldwide growth in cyber crime. The standardization it provides in defining cyber crimes is a definite step forward. Its constriction of jurisdictional bases may be a half step backwards.

Worthy of note is the fact that other treaties have also been generally plagued by definitional issues, yet have overcome them. Assuming the international community can overcome the definitional complication, what would treaty dealing with cyber crime have to offer? First, it would clarify jurisdiction over cyber crimes and information terrorism. While existing treaties and our statutes may be capable of pulling selected cyber crimes within their ambit, there is little uniform treatment for cyber crimes. Thus, a new cyber crime treaty could help provide the basis for criminalizing the vast array of cyber offences that do not cleanly fit within traditional crimes. It would also aid extraditions by overcoming the dual criminality problem.

Even more importantly, a new treaty could establish agreed principles of enforcement jurisdiction to enable law enforcement to quickly, easily, and legally obtain the evidence necessary for the prosecution of cyber offences, computer crimes and information terrorism.

The window of opportunity for law enforcement to keep pace with electronic crime offenders (let alone get ahead of the problem) is quite short. The capacity of technology used by these offenders is increasing geometrically and at a pace that significantly challenges public and

private sector. It is both practical and logical to adopt a coordinated approach as there is little time and few resources available to address this increasingly significant problem. The greatest impact will be generated if near-term solutions can be crafted and delivered through existing structures that have a broad reach and include most key stakeholders.

First, the most important aspect of these challenges is the time sensitivity. Unless a national effort is launched in the near term, electronic crimes will outpace the resources of law enforcement agencies. Secondly, there is need to maximize investments in new or expanded tools, training, onsite assistance, and research with regard to electronic crime and cyber-terrorism initiatives.

At the domestic level, the focus should be priority issues in policing in Nigeria and promoting and measuring effectiveness of the police. One of the critical challenges here is how to make police officers internalize the standards for law enforcement, which are embodied in the United Nations Code of Conduct for Law Enforcement Officials and other international instruments which are discussed in chapter (4) of this work. It is also important to establish clear guidelines and channels for securing police accountability to the public. Furthermore, the country must consider the issue of community policing, the complimentary role of civil society and informal policing structures as well as the role of the business community and private security outfits. The importance of this lies in the fact that policing the society is too important to be left to any single agency no matter how well equipped. There is no doubt that the effectiveness of the police is directly proportional to the cooperation and support they enjoy from the community. This cooperation can no longer be taken for granted. This work has raised an awareness of the challenges involved and makes practical suggestions for strengthening police-public cooperation and community involvement in policing.

It is educative to recognize that the police cannot be ‘an island unto itself’, therefore, emphasis must be placed on issues of inter-agency cooperation, information gathering and sharing as discussed in chapter (5) of this work. One of the problems of law enforcement in this country has been the lack of effective coordination amongst the various agencies of state security and law enforcement. The findings and recommendations in this work should help to resolve some of the challenges in this aspect of crime and policing.

## **6.2 Findings**

Having realized the powers of the menace of cyber insecurity and the inadequacy of law enforcement agencies in fighting it, the following suffice as the findings of this research and which if adequately addressed can help in at least ameliorating cybercrime and its numerous effects.

The key findings from this study are:

- (a) Fragmentation at the international level, and diversity of national cybercrime laws, may correlate with the existence of multiple instruments with different thematic and geographic scope. While instruments legitimately reflect socio-cultural and regional differences, divergences in the extent of procedural powers and international cooperation provisions may lead to the emergence of country cooperation “clusters” that are not always well suited to the global nature of cybercrime,
- (b) Reliance on traditional means of formal international cooperation in cybercrime matters is not currently able to offer the timely response needed for obtaining volatile electronic evidence. As an increasing number of crimes involve geo-distributed electronic evidence, this will become an issue not only for cybercrime, but all crimes in general,

- (c) In a world of cloud computing and data centers, the role of evidence “location” needs to be re-conceptualized, including with a view to obtaining consensus on issues concerning direct access to extraterritorial data by law enforcement authorities,
- (d) Analysis of available national legal frameworks indicates insufficient harmonization of “core” cybercrime offences, investigative powers and admissibility of electronic evidence. International human rights law represents an important external reference point for criminalization and procedural provisions,
- (e) Law enforcement authorities, prosecutors, and judiciary in developing countries, require long-term, sustainable, comprehensive technical support and assistance for the investigation and combating of cybercrime,
- (f) Cybercrime prevention activities in all countries require strengthening, through a holistic approach involving further awareness-raising, public-private partnerships and the integration of cybercrime strategies with a broader cybersecurity perspective.
- (g) As long as there is an absence of a centralized 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 heavy challenge to law enforcement agencies. There is therefore the need for a national database collated from the various Federal Government agencies. There is already enough data from the Federal Road Safety Commission, Independent National Electoral Commission, National population Commission, SIM card registration data, bank accounts (BVN) and voter registration data. It is regrettable that the National Identity card process has not been as successful as expected due to several issues, including residence of the data. Nonetheless, it is observed that an integration of the

various data to develop a national database is critical to security and could help to ease the job of cybercrime investigation and consequently effective law enforcement.

### **6.3 Recommendations**

The legislature of several nation-states including Nigeria have already passed computer crime laws of varying effectiveness. This work determined “seven critical” or top priority needs. They are listed below, without reference to priority or ranking:

**6.3.1 Public awareness-** A solid information and awareness program is needed to educate the general public, elected and appointed officials, the criminal justice community, and the private sector about the incidence and impact of electronic crimes. With many cases being undetected or unreported, and with the dearth of hard data on electronic crime trends, most individuals are unaware of the extent to which their financial status, businesses, families, or privacy might be affected by electronic crime. Neither are most people aware of how fast the threat is growing.

A multifaceted information and awareness campaign is needed to clearly document and publicize how electronic crimes affect society. Unless the public is made aware of the shift in crime to the whole new arena of the Internet, individuals will continue to be subjected to a number of crimes, including fraud, identity theft, child abuse and denial of services.

**6.3.2 Uniform Training and Certification Courses** -Law enforcement officers and forensic scientist need specific levels of training and certification to correctly carry out their respective roles when investigating electronic crimes, collecting and examining evidence, and providing courtroom testimony. This training should reflect public and private priorities. There is need for both entry-level and advanced training for law enforcement officers and investigators, prosecutors and defense attorneys and judges.

**6.3.3 Management Assistance for Onsite Electronic Crime Task Forces**-Law enforcement agencies need immediate assistance in developing computer investigation units, creating regional computer forensics capabilities, organizing task forces and establishing programs with private

industry. Financial institutions in the country should for security reasons, develop fraud detective departments.

A majority of the materials reviewed in this work<sup>1</sup> called for a regional investigative task force approach to the technically challenging and time-consuming job of investigating crimes involving computers. In some developed countries, agencies are known to seek hands-on assistance from experts in electronic crime and in criminal task force development to enhance their ability to combat electronic crime at all levels. Simply stated, investigative task forces are extremely effective crime fighting tools. This has been proven with drug and arson task forces<sup>2</sup> in the United States of America and at our local level, with the National Drug Law Enforcement Agencies (NDLEA) and National Agency for Foods, Drugs, Administration and Control (NAFDAC).<sup>3</sup> EFCC have also at different times worked closely with their overseas counterparts when occasion demand for such collaboration.<sup>4</sup> Combining forces among agencies make it more affordable to acquire the high-tech tools used in analyzing computer evidence to coordinate strategies and procedures to deal with electronic crime.

**6.3.4 Cooperation with the High-tech Industry-** Crime solvers needs the industry's full support and cooperation to control electronic crime. Industry support is needed to develop and maintain trusted relationships and cooperative agreements to help sponsor training, joint task

---

<sup>1</sup>See, literature review (1.7) in chapter one of this work

<sup>2</sup> D.J. Icove, V.B. Wherry, and J.D.Schroeder, (1998) *Combating Arson-For-Profit: Advanced Techniques For Investigators*, 2<sup>nd</sup> Edition, Battelle Press, Columbus OH:LINK U.S.A. at Pp.329-346.

<sup>3</sup>Oladele J. (2007, Thursday, June 7) *Detecting Counterfeit Drug*. The Guardian News paper, at p.3 (The NAFDAC Director General was invited to present a keynote address on "Detecting counterfeit Drugs" at a three-day International workshop jointly organized by United States Foods and Drugs Administration (USFDA), U.S. pharmacopoeia and York college, City University New York.)

<sup>4</sup>Biodun. S. (2007, Friday, June 8) *EFCC Collaborate With International Anti- Corruption Agency*. The Punch News paper, at p.8 (An official of the Economic and Financial Crime Commission (EFCC) disclosed in a recent press interview, that the anti-corruption agency had drawn the attention of the "Financial Action Task Force" (FTF), the global regulatory body on moneylaundering issues to work together for the repatriation of some former governors who are taking refuge outside Nigeria after being indicted for corruption charges).

forces and share equipment for the examination of electronic evidence. These cooperative relationships can also encourage the reporting of electronic crime.

For instance, Michael A. Vatis, commented on a joint Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) annual study that assessed the levels and costs associated with computer crime.

Vatis stated, “This year’s CSI/FBI study confirms the need for industry and government to work together to address the growing problem of computer intrusions and cyber crime generally. Only by sharing information about incidents, and threats, and exploited vulnerabilities can we begin to stem the rising tide of illegal activity on networks and protect our nation’s critical infrastructure from destructive cyber attacks”<sup>5</sup>.

Many technology firms have their own information security units that, among other responsibilities, detect and investigate electronic crime. It is submitted that collaborative efforts between industry and government will provide the best opportunity to control electronic crime and protect the Nation’s critical infrastructure, some of which heavily relies upon computer technology.

**6.3.5 Special Research and Publications** -Investigations, forensic laboratory specialists, and prosecutors need a comprehensive directory of electronic crime information, training and resources to help them combat electronic crime.

The Federal government, colleges and universities, trade associations and private industry should all respond to the need for diverse training in the field of electronic crime. It is critical to communicate the availability of training and professional seminars if these offerings are to be used to their maximum advantage.

---

<sup>5</sup>Michael A.Vatis,( 1999) Issues and Trends: Computer Crimeand Security Survey. Commentsregarding csi/fbi. FBI Bulletin, p.1. San Francisco. C.A.1999. (Micheal A Vatis is the Director ofUnited Statesof America’s National Infrastructure Protection Center “FBI” headquarters Washington D.C.)

Many investigators and prosecutors are calling for a clearinghouse of online information and technical guidance on methods, investigative technologies and research. Examples of specialized technologies include the ability to detect and break encryption, image disks, and index important information.

In countries where law on cyber crime is firmly established, law enforcement agencies also are asking for a clearinghouse of national and state experts and resources. A “who is who” of electronic crime investigators, unit managers, prosecutors, labs, equipment, expert witnesses, and so forth would be a well-received guidebook for many practitioners who frequently noted the need for information on how to contact colleagues in other communities. This approach is recommended for Nigeria. A training directory citing current sources of electronic crime training offerings [print, online, and compact disc read only memory (CD-Rom) versions] would be extremely valuable.

One such successful nationwide law enforcement network, which supports the dissemination of information on electronic crime, is the United States of America’s Federal Bureau of Investigation’s Law Enforcement Online (LEO). However, this is not a total solution in itself as many law enforcement officers need access to broader information than is contained in Law Enforcement Online, including private-sector specialists and technical data. A multi level secure network could address this need.

**6.3.6 Investigative and Forensic Tools-**The additional challenge before the law enforcement agency in cybercrime investigation is that the evolution of technology is consistent and at the introduction of every new method, the criminals devote energy and resources to detecting the shortcomings of such inventions. Those involved in cybercrime are well organized and very vast

on the matters of technology. They are well ahead of some security investigation agencies in Nigeria.

There is a significant and immediate need for up-to-date technological tools and equipment for law enforcement agencies to conduct electronic crime investigations. Most electronic crime cases cannot be properly investigated and developed without essential cyber tools, software, and exposure to higher end computer technology. Computer systems, software, hardware, intrusion detection tools, decryption technology, and other forensic equipment are expensive and beyond the budgets of most law enforcement agencies. Even when special equipment is available, it is frequently out of date or incapable of being used for forensic investigations. Insufficient data storage capacity- to properly copy and analyze evidence is a common problem too.

**6.3.7 Electric Power Supply-** The federal government must as a matter of priority improve in the generation and supply of electricity in the country. This will encourage more persons to take interest in computer studies and at the same time broaden computer literacy. More importantly, the availability of steady electric power supply will aid the efficiency of law enforcement agencies in tracing and tracking suspected hackers especially in situations where a rapid response is required to investigate and collect necessary data that can help the case of the prosecution. It is therefore recommended that the nation should ensure regular and steady supply of electricity as this is the power base of all electronic devices without which the optimum output of any electronic gadget cannot be achieved.

Nigeria now has a cybercrime “specific” Act but there is fresh concerns over implementation of the Act. This work has therefore, in addition to the first “seven” above,

recommended the following as implementation strategy for the newly promulgated cybercrime Act, 2015 and the national policy on cybersecurity:

- (1) The court should play down on the proof of specific intent, because the requirement to proof these specific intents significantly narrows the scope of each offence and also makes proving each offence more difficult.
- (2) Exceptions for law enforcement, military or intelligence activities must be addressed in order to avoid these categories from falling victim of the penal provision of section 14(1).It should be enough cover if the law enforcement authorities access a computer under a valid authorized search warrant.
- (3) Section 50(1) vested jurisdiction in all matters bordering on this Act on the Federal High Court, the concern here, therefore, is for the Judges of this court. The judges must be indoctrinated to understand that maximum sentence must be given in all cases where the accused person is found guilty. This will heal the non specific term of punishment especially prison terms as is prevalent in most provision of the Act. It is noted that a sentence that seems to be like a pat on the wrist will not serve as a deterrent to other criminally minded persons.
- (4) In a case of fraud against a financial institution, the court should not rely solely on the evidence of such financial institution to the extent that it have in place all imaginable security measures to forestall fraud. Arguably, this might seem a difficult task being a statutory provision and going by the decisions of courts on plethora of cases on statutory provisions. For instance in *Amaechi v INEC*<sup>6</sup> the court, per P.O. Aderemi (JSC), held that where a statute has made provisions for the steps to be taken, no other steps than those prescribed must be followed. This is also the position of the court in *Ehuwa v*

---

<sup>6</sup> (2009) 4 EPR 117

*O.S.I.E.C.*<sup>7</sup> and a parallel report as *Ehuwa v INEC*.<sup>8</sup> These positions of the court notwithstanding, the court in dealing with fraud concerning financial institution under section 19(3) of this Act should treat each case on its merit by also considering the testimony of the investigating law enforcement officer in the matter.

On the whole, if the Government take the above recommendations seriously and observe them diligently it will help as a smooth implementation strategy for the newly promulgated cybercrime Act, 2015 and the national policy on cybersecurity.

---

<sup>7</sup> (2006) 18 NWLR (pt.1012) 544 at 568 (Para. H) and p.569 (Paras. A-D)

<sup>8</sup> (2006) 28 NSCQR 551

## BIBLIOGRAPHY

### A. BOOKS

Amnesty International,(2009) “International Police Standards” Geneva Centre for the Democratic Control of Armed Forces (DCAF)Amnesty International Publication United Kingdom.

Beck,U. (1992).Risk society, London Sage.

Bell, D. (2001). An introduction to Cyber Cultures. London Routledge.

Boon J. [2002.April] *Stalking and Psychosexual Obsession: Psychological Perspectives for Prevention, Policing and Treatment* John Wiley& sons, Ltd. U.K.

In: Balkin M, etal. (ed.) *Cybercrime Digital Cops in a Networked Environment*. New York University Press.

Brierly J.L. (1978, Jan. 5) *The Law of Nations: An introduction to the international law of peace*, Humphrey Waldo (ed). Oxford Univ. Press 6th ed.

Bellovin S. ( 2006, June 13 ) *Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP*. ITAA Publications USA.

Chubey, R. (2009) *An Introduction to Cyber Crime and Cyber Law*. Kamal Law House, Kolkata India.

Chukkol,K.S (2010) *The Law of Crimes in Nigeria*. Ahmadu Bello University, Zaria. (Revised Edition).

Chirillo, J. (2001) *Hack Attacks Encyclopaedia: A Complete History of Hacks, Cracks, Phreaks and Spies*. John Wiley & sons. Inc. Publishers. U.S.A

Clifford M.(1992 May) *Electronic Evidence- can you prove the Transaction Took place?*, computer Law .Prentice Hall Law and Business. U.K.

Casey E. (2011, April) *Digital Evidence and Computer Crime*. Third Edition Academic Press. USA.

Daniel J.S. (2007).*The future of Reputation Gossip, Rumor, and Privacy on the Internet*. Yale University press. New Haven & London.

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

David, S.W. (2008) *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press. 2<sup>nd</sup> Edition U.K.

- Douglas E, Ralph E. Computer Network and Internets, Fourth Edition prentice Hall. U.K
- Ericson R. and Haggerty K. (1997). Policing the Risk Society. Oxford University Press. United Kingdom
- Finnemann. N. (2002) perspectives on the internet and modernity; late modernity, post modernity or modernity modernized? In N. Brugger and H. Bodker (eds.) The Internet and society? Papers from centre for Internet Rresearch, University of Aarhus, Denmark.
- Gidden, A. (1990). The Consequences of Modernity, Cambridge: Polity, (press) London.
- Grimes R. (2001. August) *Malicious Mobile Code, Virus Protection for Windows* .O'Reilly Media Publishers. U.S.A
- Gorling S. The Myth of User Education, (2006, October 19) Social Science Electronic Publishing, Inc. Stockholm Sweden.
- Garland, D, (2001).The Culture of Control: Crime and Social Order in Contemporary Society. The University of Chicago Press.
- Grabosky, P.N, Smith. R.G and Dempsey, G. (2001) Electronic Theft: Unlawful Acquisition in cyberspace. Cambridge University Press.
- Icove, D.J, Wherry, VB and Schroeder, J.D. (1998) Combating Arson-For-Profit: Advanced Techniques For Investigators, 2<sup>nd</sup> Edition, Battelle Press, Columbus OH:LINK U.S.A.
- Jordan,T.(1999).The culture and Politics of cyberspace and the Iinternet. London: Routledge.
- Jordan J. Paust, Bassiouni M, Michael S, Jimmy G, Leila S, Bruce Z. (1996, June) International criminal Law: Cases and Materials. Carolina Academic Press.
- Jemibewon, D. M. (2001) The Nigeria Police in Transition: Issues: Problems and Prospects, Spectrum Books Limited, Abuja.
- Levi, M. (2001) Between the risk and the reality falls the shadow, evidence and urban legend in computer fraud; In D.S Wall (ed.) crime and the internet, London: Routledge.
- Ladan, M. T (2006) Introduction to Jurisprudence: Classical and Islamic. Faith printers and Publishers Limited, Zaria.
- Ladan ,M.T (2008) Introduction to Jurisprudence: Classical and Islamic. Faith Printers and Publishers Ltd. Zaria.

- Ladan ,M.T. (2015) *Cyberlaw and Policy on Information and Communications Technology in Nigeria and Ecowas*. Ahmadu Bello University Press Limited Zaria.
- Marshall McLuham, (1962) *The new electronic interdependence recreates the world in the image of a global village*. The Gutenberg Galaxy.
- Marshall McLuham & Bruce, (1989). *Powers, The Global village: Transformation in World Life and Media in The 21<sup>st</sup> century* The Gutenberg Galaxy.
- Mullen P. (2000. April 27).*Stalkers and their Victims (First edition)* Cambridge University Press. U.K..
- Newburn T and Hayman S. (2001) *Policing CCTV and Social Control: Police Surveillance of Suspects in Custody*, Cullopton: Willan publications. UK.
- Newman, G.R and Clark, R.V. (2003) *Superhighway Robbery: Preventing e-commerce crime*. Cullompton William Publication.
- Onovo, O. (2005) *Crime Control in Nigeria*. In: Alemika, E.O. (ed) *Crime and Policing in Nigeria: Challenges and Options*. Cleen Foundation, Lagos Nigeria.
- Oxford dictionary of computing fourth eds (1996) U.K Oxford University Press.
- Parker D. (1998.September) *Fighting Computer Crime: A New Framework for Protecting Information*. John Wiley & sons. Inc. Publishers. U.S.A.
- Raymond E (1991)*The New Hacker's Dictionary*. The MIT Press. U.S.A
- Ramberg C. (2002)*Internet Marketplaces, The Law of Auctions and Exchanges Online*. Oxford University, Press.
- Robert S. Greenfield, Albert J. Marcella, ,( 2002). *Cyber Forensics: A field manual for collecting, examining, and preserving evidence of computer crime*, Computer Research Center (CRC) Press, UK.
- Standage, T. (1998). *The Victorian internet: The remarkable story of the Telegraph and the Nineteenth century's online pioneers*, London: Phoenix.
- Sue, T.R. (2009). *Criminal Law the Essentials*. Oxford University Press. New York.
- Sterling B. (1993 November 1,) *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. Batman Publishers.
- Sieber U. (1998).*Legal Aspects of Computer Related Crime in Information Society*. European Commission. S.S. Wimbledon U.K.

Spinello R. [2002. June 30] *Regulating Cyberspace: The Policies and Technologies of Control* Praeger Publishing .U.S.A.

Shinder, D. (2008) *Scene of The Cybercrime*. Elsevier Ltd; 2<sup>nd</sup> Edition.

Smith R, et al, (2004) *Cyber Criminals on Trial*. Cambridge University Press. U.K.

Taylor, P. (2001) *Hackitivism: In search of lost ethics?* In: D.S Wall (ed.) *Crime and the Internet*, London Routledge.

Tyrone A, Sharon S. (2005) *Internet Effectively: A Beginner's Guide to the World Wide Web*. Addison Wesley.U.K

United Nations, New York and Geneva (1997) *Human Rights and Law Enforcement ( A manual on Human Rights Training for the police)* professional training series No. 5.

United Nations Office on Drugs and Crime (UNODC) (July 2011) *Handbook on police accountability, oversight and integrity (Criminal Justice Handbook Series)*UN New York.

UN. (New York 2011), *Handbook on police accountability, oversight and integrity, Criminal Justice Handbook Series in summary*.

Vacca J. (2005) *Computer Forensics, Computer Crime Scene Investigation, 2nd Edition*, Charles River Media Publisher. U.K.

Wall, D.S. (1997) *Policing the virtual community: the internet, cybercrimes and the policing of cyberspace*. In P.Francis, P.Davis and V. Jupp (eds), *policing futures*, London Macmillan.

Wall, D.S. (2000) *The Theft of Electronics Services: Telecommunication and Teleservices, Essay on the C.D-Rom annex to DTI, Turning the corner*. Department of Trade and Industry. London.

Wall, D.S. (2005) *The Internet as a conduit for criminals*. In A. Pattavina (ed.) *Information Technology and the Criminal Justice System*, Thousand Oaks, Massachusetts, U.S.A.

Webster, F. (2002) *Theories of the Information Society, 2<sup>nd</sup> edition*, London Routledge.

## B. ARTICLES IN JOURNAL PUBLICATION

- Abel, E (2006), *Regulating Internet Banking In Nigeria: Some Success Prescriptions – Part 2*, *Journal of Internet Banking and Commerce*.11:33.
- Akuta E, Ong’oa I, Chanika J. (2011, May) *Combating Cybercrime in Sub-Sahara Africa: A Discuss on Law, Policy and Practice*. *Journal of Research In Peace, Gender and Development*. 1(4):129-137
- Aldesco I.A. , (2002), *The demise of anonymity: A constitutional challenge to the convention on cybercrime*, *Loyola of Los Angeles Entertainment Law Review*. p.81
- Anneke Osse,(2006) *Understanding Policing: A Resource for Human Rights Activists* Amsterdam, Amnesty International Nederland, chapter 4.
- Arie J. Schaap, (2009) *Cyberwarfare Operations: Development and Use Under International Law*, *Air Force. Law. Review*. 171( 64);127 and 171.
- Anne Wells Branscomb (1995). *Anonymity, Autonomy and Accountability: Challenges to the first Amendment in cyber space*. *Yale Law Journal* 104 (1639):98-130.
- Brenner, S (2001) “Is there such a thign as “virtual crime””? *California Criminal Law Review*, 4 (1); 11 (para.1)
- Brenner, S. (2002) *Organized Crime? How Cyberspace May Affect the Structure of Criminal Relationships*. *North Carolina Journal of Law and Technology* 4(1):1-50.
- Chawki, M. (2009) ‘Nigeria Tackles Advance Free Fraud’, *Journal of Information, Law & Technology (JILT)* (1):7.
- Castells, M. (1997b) *The Information Age: Economy, society and culture*. In: Oxford, B. (ed) *The power of identity*. (2):19.
- Castells, M. (2000a) *Materials for an Explanatory Theory of the Network Society*: *British Journal of Sociology*, 51 (1): 5-24
- Cyber Law Research Unit, (1999) *University of Leeds, U.K. (College Brochure)*. P.3
- Crawford ,A and Lister S. (2004) *The Patchwork Future of Reassurance Policing in England & Wales: Integrated Local Security Quils or Frayed, Fragmented and Fragile tangle web?*. *An International Journal of Police Strategies & Management*, 27 (3):413-430.
- Duncan B. Hollis, (2011) *An E-SOS for Cyberspace*, *Harvard International Law Journal* (52): at, 373

- Ezeoha Abel (2006, April) Regulating Internet Banking in Nigeria: Some Success Prescriptions-part 2. *Journal of Internet Banking and Commerce*. 11(1):1-17
- Francis A. Gilligan & Edward J. (1998) Cyber Space: The Newest Challenge for Traditional Legal Doctrine. 24, *Rutgers computer & Technology Law Journal*. p.305
- Goodman M. D. and S. Brenner, (2000) The Engineering Concesus on Criminal Conduct in Cyber Space. *Oxford International Journal of Law and Information Technology* (10):173.
- Gbenga, A. (2003-2005) Adequacy and Efficacy of Penal Sanctions for Financial and Banking Offences in Nigeria. *ABU Journal of Commercial Law*. 2(2):98
- Huey L. and Rosenberg R.S. (2004). Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention. *Canadian Journal of Criminology and Criminal Justice* 46: 597-631.
- Hopkins L.S. (2003), Cybercrime Convention: A positive beginning to a long road ahead, *Journal of High Technology Law*, p.101
- Hosmer C. (2002) Proving the Integrity of Digital Evidence with Time, *International Journal of Digital Evidence* 1 (1): p1-7.
- Ibrahim Baggil (2003) The Fight Against Transnational Cybercrime, *Business & Economics platyplus Magazine: Journal of the Australian Federal Police*. (80): 4-6.
- Innes M. (2004) Reinventing Tradition? Reassurance, Neighbourhood Security and Policing. *Criminal Justice Journal*. 4 (2):151-157
- James, R. (2003, October). For the Veteran Officers: Leadership, Ethics, and Wellness Training. [Electronic Version]. *The Police Chief*, vol. 79, no. 10.p.5
- Jason Barkham, (2001), *Information Warfare and International Law on the Use of Force*, *New York University Journal of International Law & Policy* (34):57,
- Jones, R (2003) "Review of Crime in the Digital Age" by P. Grabosky and R. Smith, *International Journal of Law and information Technology*, 11:98
- Johnson D and Post D. [1996] *Law and Borders: The Rise of Law in Cyberspace* .*Stanford Law Review* (1378):16
- John T, Soma Elizabeth et,al, (1996). Computer crime: Substantive statutes & Technical & Legal search considerations. *F.L. REV.* 39A (225):46-52
- Keeping secrets in cyber space: Establishing fourth Amendment protection for Internet Communication. (1996-1997) *Harvard Law Review*. 1591(110):83.

- Keyser M. (2003), Common Goods and Evil?: The Formation of Global Crime Governance, *Transnational Law and Policy Journal*, (12): 324-326
- Kristina M, Lyn H and Jenny F, (2008 June), "Encouraging public cooperation and support for police", *Policing and Society*, vol. 18, No. 2 pp. 136-155.
- Kwiatkowski J. (2002) Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images, *Journal of Law and Policy*. 267: 1-32.
- Leigland R, Krings W.(2004), A Formalization of Digital Forensics. *International Journal of Digital Evidence*. 3 (2): 231-283
- Longe O, Osofisan A, Kvasny L, Jones C. and Nchise A. (2010). Towards A Real-Time Response (RTR) : Model for Policing the Cyberspace. *Journal of Information Technology in Developing Countries*. 20 (3):1-10
- Li, X. (2007). International Actions Against Cybercrime: Networking Legal Systems in the Networked Crime Scene. *Webology*,4(3):1-45.
- Marcel D. (1996) Internet Providers not Held Responsible for Wrongful Acts of Internet Users. *Institute for information law Journal, University of Amsterdam*. 4 (3/2):1
- Michael A.Vatis, ( 1999) Issues and Trends: Computer CrimeandSecuritySurvey.Comments regarding csi/fbi. *FBI Bulletin*, p.1. San Francisco. C.A.1999.
- Mann, D and Sutton, M. Netcrime: (1998), More change in the organization of thieving: *British Journal of Criminology*, 38 (2): 210-229.
- Maitanmi O, Ogunlere S, Ayinde S, Adekunle Y. (2013 May) Cyber Crimes and Cyber Laws in Nigeria. *The International Journal Of Engineering And Science (IJES)*2( 4):19-25
- Matthew J. Sklerov, (2009). *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect their Duty to Prevent*, *Mill, Law Review*. 201(1), at p.6
- Michael D. Scott, (2008), *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, *67 Maryland Law Review* p.425,
- Matthew C. Waxman, (2011). *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, *36 YALE Journal of International Law* (36): at 425-26
- Marshall J.J. (2005)The Convention on cybercrime: A harmonized implementation of international penal law: what prospects for procedural law process?, *Computer & Information Law Journal*, p. 329

- Moore R. (2004) To View or not to View: Examining the Plain View Doctrine and Digital Evidence. *American Journal of Criminal Justice*. 29(1): 57-73.
- Obada, R, Oke, M, (2012. . May,30)Cyber Capacity without Cyber Security: A Case Study of Nigeria's National Policy for information Technology (NPFIT). *The Journal of Philosophy, Science & Law*. 12: 1-11.
- Oona H, Rebecca C, Philip P, et al.(2012) The Law of Cyber-attack. *The California Law Review* 11(16): 48
- Osipitan. T.A..I (1998) Legal Impacts of Technology on Rules of Evidence in Banking and Commercial Litigation. *Nigerian Commercial Laws: Essays in Honour of Chris Ogunbanjo*. Chap. 29 at p 435.
- Peter R. (2002, April ) *Evolving Technologies: Information Assurance Core Competencies. (White Paper)* Falls Church VA, Uniformed services Journal of University of the Health Sciences Bethesda MD, USA. p.7.
- Rheingold, H. (1994). *The virtual community: Homesteading the Electronic frontier*, New York: Harper Perennial. pp.19-204.
- Richard, A. (1999) How Do You Know You Are at War in the Information Age?" *Houston Journal of International Law*, (fall). p. 88.
- Robinson ... (1970) The Admissibility of Computer Printouts under the Business Records Exception in Texas. *South Texas Law Journal*. 12: 291.
- Raphael W. (1994). Searches and Seizures of Computers and Computer Data. *Harvard Journal of Law & Technology*. 8 (75):76.
- Scheiner J.L. (2003) Hiding in plain sight: on Exploration of the illegal (?) activities of a drug newsgroup.
- Sterling B. (1993 November 1,) *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. Batman Publishers. pp. 50 -51.
- Skoudis , E. (2003. November) *Malware, Fighting Malicious Code*. Prentice Hall publisher, U.K .p. 25.
- Seedorf J. (2008) *Lawful Interception in P2P-Based VoIP Systems: Principles, Systems and Applications of IP Telecommunication*. Services and Security for Next Generation Networks. lecture notes in computer science. Springer link vol. 5310, pp. 217-235 .
- Straub D. and Welke R. (1998). *Coping with Systems Risk: Security Planning Models for Management Decision Making*. *MIS Quarterly Journal*. 22(4);441-469

Sergienko, G. (1996) Self Incrimination and Cryptographic Keys. University of Richmond  
Journal of Law & Technology. 2 (I):138-142.

The Howard Journal of Criminal Justice, 42 (4): 374-389

United Nations Human Rights and Law Enforcement, A manual on Human Rights Training for  
Police (Professional Training Series No.5) at p.25

Volokh (2001) Freedom of Speech, Religious Harassment Law, and Religious Accommodation  
Law. Loyola University Chicago Law Journal, 33:57.

Wells, J. [2002] Cybercrime ranges from computer fraud, theft and forgery. The Computer and  
Internet Fraud Manual (Annual) publication. Austin, Texas, p. 3.

Woo/So, (2002)The case for Magic Lantern: September 11 highlights the need for increasing  
surveillance, Harvard Journal of Law and Technology. 15 ( 2):530,

Weber M.A. (2003),The Limit of Peer Production: Some Reminders for The Network Society,  
Yale Technology Law Journal, p.254

Wada F. (2012, May). Policing the CyberSpace – Is the Peel Theory of Community Policing  
Applicable? Computing, Information Systems & Development Informatics  
Journal. 3(2):51-56.

### **C. NEWSPAPERS**

Chiedu A. (2012, December 27) Tackling the Cybercrime Menace in Nigeria. The Punch News  
Paper Nigeria. p.20

Eugene R, Dana, P. (1998 August, 22) Reports of U.S. Strikes' Destruction Vary, Sudan Plant  
Leveled, Washington Post, final Edition, at. p. A1

Ikeocha D, (2004 August 2,) Nigeria Move to Protect ICT Infrastructures, Daily Sun Newspaper  
p.11 ,

Joseph Erunke. (2014, July 20) Senate Okays Death Penalty For Terrorists. Vanguard  
newspaper. P3

Jim Hoagland, (Aug. 26, 1998, ) Law of the Jungle as used in Anti-Terrorism, Houston  
Chronicle, at A32

John Leydon, (2003 Tuesday, January 21, ) Weish Virus Writer Vallor, jailed for two years, The  
Register (News Paper) p.2.

James Risen, (1998, Sept.6) Militant Leader was a U.S. Target since the spring, New York  
Times, Late Ed - final, sect.1 ,p, & col.6.

Ken Nnamani. Senate President, as he then was ( 2006. Sept.12,) Daily Trust News paper. at p.5

Kenneth C. (2010, 27February) Data, data everywhere, A special report on managing information. The Economist Newspaper Ltd. at pp.1-13 .

Oladele .J. (2007, Thursday, June 7) Detecting Counterfeit Drug .The Guardian News paper, at p.3

Ribadu N, (2003, December 4) Vanguard Newspaper, p.7 (During an interview with Disu,M. as then Chairman of EFCC.)

Samuel, C.M. (2006) Understanding and Managing Cybercrime. Library of congress cataloging in publication data. Pp.1-187.

Shina B. (2005, January, 14) “Nigeria and IT laws: progress made” Techtimes news.p.1

#### **D. INTERNET MATERIALS**

Ashaolu D (2011 December, 24 & 27) Combating Cybercrimes in Nigeria I & II. [ Web log post]. Retrieved August 8, 2015 from <http://blogs.McAsh'sThoughts>.

Abramovitch, R. (2002) A Brief History of Hard Drive Control. Control Systems Magazine, EEE, vol. 22, Issue 3, p. 28, Coughlin/Waid/Porter,( 2005,) The Disk Drive, 50 Years of Progress and Technology Innovation, Retrieved June 2, 2015 from [www.tomcoughlin.com/Techpapers/disk%20drive%20history,%20TC%20Edits,%20050504.pdf](http://www.tomcoughlin.com/Techpapers/disk%20drive%20history,%20TC%20Edits,%20050504.pdf).

Archick K. (2002) Europe Convention on Cybercrime of November 2001. A report of Congressional Research Service (CRS) on cybercrime presented to the Congress in USA on 26, April, (2002), The Council of Europe Convention, Retrieved February 16,2014 from <http://www.usembassy.it/pdf/other/RS21208.pdf>

Brenner S . (2005) Distributed Security: A New Model of Law Enforcement. *John Marshal Journal of Computer and Information Law Vol. .XXIII* (4).(article written in 2004), Retrieved June 22, 2015 from <http://www.jcil.org/journal/articles/434.html>.

Brenner S and Clarke (2005). Prosecution of Information Technology Crimes *John Marshal Journal of Computer and Information Law Vol. .XXIII*. (4). Retrieved June 22, 2015 from <http://www.jcil.org/journal/articles/434.html>.

Bill Googwin and Tim Berners Lee, The Law must be Changed to Redefine Criminal Activities. Retrieved February 16, 2014 from, [www. Computerweekly.com](http://www.Computerweekly.com). p.1 .

- Borone, M (2004, 24 March) "The National interest: absence of evidence is not evidence of absence; US, News & World Report. Retrieved June 2, 2012 from [www.usnews.com/usnews/opinion/baroneweb/mb040324.htm](http://www.usnews.com/usnews/opinion/baroneweb/mb040324.htm).
- Bicknell C. [,2000 August], *Sex.Com : It Wasn't Stolen*. Retrieved June 10, 2012. From <<http://www.mediaesq.com/new31857.php>>
- Burren J. (2001) *European Commission Wants to Tackle Cybercrime*. Retrieved June 19, 2012 from <<http://www.heise.de/tp/r4/artikel/4/4658/1.html>>
- Bruce Sterling. (2011, 28 March) Microsoft versus Rustock Botnet. Wired Magazine (online) Retrieved June 2, 2015 from [[http://www.wired.com/beyond\\_the\\_behind/2011/03/microsoft-versus-rustock-botnet/](http://www.wired.com/beyond_the_behind/2011/03/microsoft-versus-rustock-botnet/)]
- Chawki, M. (2005. April ) A Critical Look at The Regulation of Cyber Crime. A Comparative analysis with suggestions for Legal Policy, Droit-tic, 11 P.20. Available on mohamed [chawki@hotmail.com](mailto:chawki@hotmail.com). Accessed 2<sup>nd</sup> June 2012
- Chawki M. (2009). Nigeria Tackles Advance Free Fraud. *Journal of Information Law & Technology* No. 1. Retrieved June 22,2015 from [http://go.warwick.ac.uk/jilt/2009\\_1/chawki](http://go.warwick.ac.uk/jilt/2009_1/chawki)>.,
- Chris Onyemenam, (then NIMC's Director General and Chief Executive Officer) (Public Awareness Campaign) Retrieved 2014 February 22 from <http://3.blogspot.com>.
- Denning D. [2000. May 23,] Cyberterrorism ( U.S.A, Special Oversight Panel on Terrorism), P.2 Retrieved August 8, 2012, from <http://www.stealth-iss.com>>documents.
- Goodman, M and Breaner, S (2002), "The emerging consensus on criminal conduct in cyber" UCLA Journal of Law and Technology,3:28.Retrieved June 2, 2012 from [www.lawtechjournal.com/articles/2002/03-020625\\_goodmambrenner.pdf](http://www.lawtechjournal.com/articles/2002/03-020625_goodmambrenner.pdf).
- Graham G. (2012, 6 February) Global Data Privacy Laws: 89 Countries, and Accelerating. Social Science Research Network. Retrieved June 22, 2015 from <http://www.itu.int> > GSR12 >
- Gasser, U; Cortesi, S; Malik, M. and Lee, A. (2012. February 16,.) Youth and Digital Media: From Credibility to Information Quality Havard Law School, Berkman Center Research Publication No. 2012-1. Retrieved June 5, 2012 from SSRN: <http://ssrn.com/abstract=2005272> or <http://dx.doi.org/10.2139/ssrn.2005272>.
- Gibson S. *The Strange Tale of the Denial of Service*. Retrieved, June 6, 2012 from <<http://grc.com/dos/grcdos.htm>>

- Grabosky, P. (2006) Editor's Postscript, *Crime, Law and Social Change*. Retrieved June 18, 2012 from <https://researchers.anu.edu.au/researchers>. pp.275-276.
- Giordano S. (2006,)Electronic Evidence and the Law, *Information Systems Frontiers Journal* 6(2): 161-174.
- Handbook of Information Security Management: Law Investigation, and Ethics. Retrieved February 16, 2014 from, [www.cccire/prg/Documents/hism/522525.html](http://www.cccire/prg/Documents/hism/522525.html)
- ITU. Retrieved June 2, 2012 from [http://www.itu.int/osg/csd/cybersecurity/gca/global\\_strategic\\_report/](http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/)
- International Association of Chiefs of Police (IACP) Newsletter Retrieved June 8, 2012 from <http://www.theiacp.org/>
- ITU (2012, October 19) The Cloud: Data Protection And Privacy Whose Cloud is it Anyway? GSR12 Discussion Paper. p.9. Retrieved July 10, 2015 from [gsr@itu.int](mailto:gsr@itu.int).
- International Telecommunication Union (ITU) (2007) Creating Trust in Critical Network Infrastructures. (Chairman's Report on Workshop Regarding the integration of developing countries in the protection of network infrastructure) Retrieved June 2, 2015 from <http://www.itu.int/osg/spu/ni/security/docs/cni.10.pdf>;
- John, W. Retrieved June 3, 2012 from <http://www.crime-research.org/news/22.07.2007>
- Jody R. (2003) International Guide to Combating Cybercrime. Retrieved June 8, 2012. From <<http://www.nctp.org>>.
- John, M, *Step Taken to End Impasse Over Cybersecurity Talks*, N.Y. TIMES, July 16, 2010, Retrieved December 13, 2014 from [http://www.nytimes.com/world/17/cyber.html?\\_r=1](http://www.nytimes.com/world/17/cyber.html?_r=1)
- Jeff Williams, (2011, 14 June ) Microsoft Malware Protection Center.( the 23rd Annual FIRST Conference, Vienna, Austria). Retrieved June 2, 2015 from [www.wired.com/beyond\\_the\\_behond/2011/03/microsoft-versus-rustock-botnet/](http://www.wired.com/beyond_the_behond/2011/03/microsoft-versus-rustock-botnet/)
- John Perry Barlow (1996, February) A declaration of the Independence of Cyberspace. Retrieved, December 18,2014 from [http://www.eff.org/pub/publications/John\\_PERRY\\_barLOW/BARLOW0296](http://www.eff.org/pub/publications/John_PERRY_barLOW/BARLOW0296).
- Johnson David, Post R, David G (1996) Law and Borders: The Rise of Law in Cyberspace, *Stanford Law Review*. 48:1367-1402.
- Johnson David, Post R, David G (1996) Law and Borders: The Rise of Law in Cyberspace, *Stanford Law Review*. 48:1367-1402.

- Kabay M [ 2001], *Studies and Surveys of Computer Crime*. Retrieved June 6, 2012  
 from<[http://www.securitystats.com/reports/Studies\\_and\\_Surveys\\_of\\_Computer\\_Crime.pdf#search='studies%20and% 20surveys%20of%20computer%20crime'](http://www.securitystats.com/reports/Studies_and_Surveys_of_Computer_Crime.pdf#search='studies%20and%20surveys%20of%20computer%20crime')>
- Kim Zetter. (2011, 13 April ) U.S. Wins Court Order to Seize Control of ‘Coreflood’ Botnet, send kill Signal. Wired Magazine Online.. Retrieved June 2, 2015 from  
 [<http://www.wired.com/threatlevel/author/kimzetter/>]
- Kew R.( 2010, March) Cyber Crime Strategy Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty, the Office of Public Sector Information, Information Policy Team, Surrey TW9 4DU or e-mail:  
[licensing@opsi.gov.uk](mailto:licensing@opsi.gov.uk). Retrieved, June 2, 2015
- Leyden J. *Love Bug Suspect Released* [2000. May], Retrieved June 10, 2012 from<[http:// www.vnunet.com/news/1101024](http://www.vnunet.com/news/1101024)>
- Lawrence A, Gordon, Martin P. Loeb, William Lucy shyn and Robert Richardson (2004 .8-10 November) CSI/FBI Computer Crime and Security Survey computer security institute publications, Retrieved June 6, 2012 from <[http://i.cmpnet.com/ gocsi/db \\_ area/pdfs/fbi/FBI2004.pdf](http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf)>
- Lange/Minster. (2011) Electronic Evidence and Discovery. (UNODC) Working Paper on the Collection of Topics- United Nations Office on Drugs and Crime. 17-21 January 2011 in Vienna at pp.1-18
- Longe O, Ngwa, Wada F, Mbarika V. & Kvasny L. (2009). Criminal Use of Information and Communication Technologies in Sub- Saharan Africa: Trends, Concerns and Perspectives. *Journal of Information Technology Impact*, Vol 9, (3). Retrieved June 22, 2015 from [www.jiti.net](http://www.jiti.net).
- Longe O & Osofisan O. (2011). On the Origins of Advance Fee Fraud Electronic Mails: A Technical Investigation Using Internet Protocol Address Tracers. *The African Journal of Information Systems: Vol. 3: Iss. 1, Article 2*. Pp.1-2. Retrieved June 22, 2015 from <http://digitalcommons.kennesaw.edu/ajis/vol3/iss>.
- McConnell International E-Lert, [2001. Feb.] *Combating Cybercrime : A Proactive Approach*. Retrieved June 12, 2012.from <[http://www.mcconnellinternational .com/pressroom/elert.cfm](http://www.mcconnellinternational.com/pressroom/elert.cfm)>
- Miles A. (2001. April 20) Bug Watch: The Fight Against Cybercrime. Retrieved June 6, 2012 from <http://www.pcw.co.uk/print/it/1120814>
- Robert H. (2012, February 22) (BSA) Global Cloud Computing Scorecard: A Blueprint for Economic Opportunity. . Retrieved, July.26,2015 from <http://portal.bsa.org/cloudscorecard>

- Rex B. Hughes, (Apr. 2009), *NATO and Cyber Defence: Mission Accomplished?*, *Atlantisch perspectief*, at p.1, Retrieved December 12, 2014 from <http://www.atlcom.nl/site/english/nieuws/wp-content/Hughes>.
- Richard Boscovich. (2012,11,October) Taking Down Botnets: Microsoft and the Rustock Botnet. Retrieved June 2, 2015 from [http://blogs.technet.com/b/microsoft\\_on\\_the\\_issues/archive/2011/02/18/taking-downbotnets-microsoft-and-the-rustock-botnet.aspx](http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/02/18/taking-downbotnets-microsoft-and-the-rustock-botnet.aspx)
- Report of Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA II). Held in Washington, DC 20006, USA. On 28, March 1999, Chapter V. [www.oas.org/en/remja/background.asp](http://www.oas.org/en/remja/background.asp). Retrieved, February 16, 2014
- Roger Clarke, Gillian Demsey & Robert F.O. Connor (1998. 16-17 Feb.) Technological Aspect of Internet Crime Prevention. A Paper Presented at the Australian Institute for criminology's Conference on "Internet Crime", Melbourne University. Retrieved June 20, 2012 from <http://www.anu.edu.au/people/Roger.Clark/II/CrimePrev.html>.
- Sir Paul Stephenson. (2010 October), *E-Crime Detectives as Vital as Bobbies on Beat*. Retrieved June 2, 2015 from [telegraph.co.uk](http://telegraph.co.uk).
- Shinder D. (2002) *Scene of the Cybercrime*. Retrieved July 9, 2012 from <http://www.store.elsevier.com>
- Shinder D. *Find Phone & Address information, medical practice...* Retrieved July 23, 2012. from [www.healthgrades.com](http://www.healthgrades.com) >..>philadelphia.
- S.Schjolberg, (2008). The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva. p.1. Retrieved June 20, 2012 from [http://www.cybercrimelaw.net/documents/cybercrime\\_history.pdf](http://www.cybercrimelaw.net/documents/cybercrime_history.pdf).
- Stein Schjøberg and Solange Ghernaoui-Hélie. (2011) A Global Treaty on Cybersecurity and Cybercrime. Second edition. p.58. Retrieved June 2, 2015 from [stein.schjolberg@cybercrimelaw.net](mailto:schjolberg@cybercrimelaw.net), [www.cybercrimelaw.net](http://www.cybercrimelaw.net), [netsgh@unil.ch](mailto:netsgh@unil.ch), [www.hec.unil.ch/sgh](http://www.hec.unil.ch/sgh).
- Schjolberg, S. (2013) Cybercrime Law. "Securing Cyberspace: A Comparative Review of Strategies Worldwide" A paper presented at the Conference on (Global organization) organized by Privacy and Cybercrime Institute of Ryerson University Canada. Held on Tuesday, March 19, 2013. Retrieved February 14, 2014 from <http://www.Cybercrimelaw.net/OECD.html>
- Smith, G. (1998) Electronic Pearl Harbor? Not likely issues in Science and Technology, 15 (3): 68-73, Retrieved June 2, 2012 from [www.nap.edu/issue/15.1/smithhtml](http://www.nap.edu/issue/15.1/smithhtml)

Scott J. Shackelford, *Estonia Two-and-a-Half Years Later: A Progress Report on Combating Cyber Attacks*, *Journal of Internet Law*. (5),37, Retrieved December 14, 2014 from <http://ssrn.com/abstract=1499849>.

Texas Penal Code. Retrieved June 9, 2012 from <<http://www.capitol.state.tx.us/statutes/docs/PE/content/word/pe.007.00.000033.00.doc> >

Tenth United Nation Congress on the Prevention of Crime and the Treatment of Offenders, (2000. April)Vienna. Retrieved June 12, 2012. From <<http://www.uncjin.org/Documents/congr10/4r3e.pdf>>

U.N. GA/DIS/3106, (9 Oct, 1998) Retrieved June 5, 2012 from,[www.un.org/ disarmament /WMD/Nuclear/](http://www.un.org/disarmament/WMD/Nuclear/).

US Department of Justice. [ 1999] *Report on Cyberstalking*. Retrieved June 12, 2012 from <<http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm>>

U.N (2001) *Commission on Crime Prevention and Criminal Justice*, 10 th session, Item 4 at 10, *Conclusion of the Study on Effective Measures to Prevent and Control High-Technology and Computer Related Crime*. Retrieved June 9, 2012.from <[http://www.unodc.org/pdf/crime/10\\_commission/4e.pdf](http://www.unodc.org/pdf/crime/10_commission/4e.pdf)>

U.N. fact sheet, setting the Record straight: The International Criminal Court, Retrieved February 16, 2014 from [http://www.un.org/plweb/cgi/idoc.pl?45+unixt\\_free\\_user\\_+www.un.org.80+un+un+webnews+webnews+++terrorism](http://www.un.org/plweb/cgi/idoc.pl?45+unixt_free_user_+www.un.org.80+un+un+webnews+webnews+++terrorism).

Vinge V. (2000) *The Digital Gaia: As Computing Power Accelerates, The Network Knows All and it's everywhere*, *Wired*, publication 8 (1), Retrieved June 22, 2015 from [www.wired.com/wired/archive/8.01/forward.html](http://www.wired.com/wired/archive/8.01/forward.html).

*Waterman*, (2007) *Who Cyber smacked Estonia*. Analysis: In United Press International. Retrieved June 2, 2015 from :[http://www.upi.com/Security\\_Terrorism/Analysis/2007/06/11/analysis\\_who\\_cyber\\_smacked\\_estonia/2683/](http://www.upi.com/Security_Terrorism/Analysis/2007/06/11/analysis_who_cyber_smacked_estonia/2683/).

Willinger/Wilson, (2004 )*Negotiating the Minefields of Electronic Discovery*. *Richmond Journal of Law and Technology*. X (5):98.

## **F. AUDIOVISUAL AND OTHER MEDIA**

James G. (Executive producer). (2012, May, 27). *Focus Africa* (television program) United Kingdom BBC, Africa Unit.

## **G. UNPUBLISHED WORKS**

Avner, L. (2013) *International Comparison of Cyber Crime*, A Paper Presented at the Conference on (Global organization) organized by Privacy and Cybercrime Institute of Ryerson University Canada. Held on Tuesday, March 19, 2013.p.9

- Alexander S. (2010) The Budapest Convention on Cybercrime as a Global Framework: Introduction to Panel Discussions. A paper presented at the Conference Organized by Council of Europe. Held in Strasbourg France from 23-25 march.2010.
- APEC, (2002) Recommendation by the APEC Telecommunications and Information Working Group (TEL) to APEC Senior Officials (SOM) for an APEC Cybersecurity Strategy, 2002/CSOM/052, Concluding Senior Officials Meeting, held in Los Cabos, B.C.S., Mexico, from 21-22 October, 2002.
- APEC,(2003) Media Release on Conference on the Strengthening International Law-enforcement Cooperation to Prosecute Cyber Criminals, Hackers, and Virus Authors. Held in Bangkok on, 25, July 2003.
- APEC, Report on 2006 Budget - Operational Account Project: TEL 04/2006 - Judge and Prosecutor Cybercrime Capacity Building Project, 2006/BMC1/012-6, Budget and Management Committee Meeting. Held at APEC Secretariat in Singapore from 29-30 March 2006
- Buheita Fujiwara (2006. November 9)Cyber Security Threats and Countermeasures. A paper presented as Chairman, Information-technology Promotion Agency (IPA), Japan in a seminar organized by Global Business Dialogue on Electronic Commerce GBDe 2006 Issue Group. Pp.34-38
- Basil, U,(2004) (NCWG Coordinator and Legal Adviser to NITDA), “Challenges of Cybercrime Enforcement in the ECOWAS Sub-Region-Case Study-Nigeria”, Abuja:
- Chan J, Brereton D, Legosz M and Doran S. (2001) E-Policing: The Impact of Information Technology on Police Practices. a paper presented to the Queensland Criminal Justice Commission in Brisbane, at p.9
- David L,(2001) International Relations of Asia: In Report of APEC Leaders Statement on Counter-terrorism, in the APEC(2001) Economic Leaders' Meeting. Held in, Shanghai on 21 October 2001.p.63
- Herbert, B; Sandro, E and Erik. P. .(2010). Trust and Security for our Digital Life. In: Report of the Committee on .National Cyber Security Research Agenda of Netherlands Published by the Netherlands home Holland, Pp.1-4
- Herman, Van R, (2005)Cybercrime: A Global Challenge, A Global Response. A paper presented at a conclusion meeting organized by Council of Europe. Held in Madrid, Spain,from 12-13 December,2005.
- Jean-Pieree Chevenement, (2000) French Minister of the Interior, (the comment made) at the G-8 Conference in Paris in 2000:

- Karpagavinayagam B, Nancy S, Festor O.( 2007 July ) “Monitoring Architecture for Lawful Interception in VoIP Networks, being a seminar paper presented at the Second International Conference on Internet Monitoring and Protection” (ICIMP) held in San Jose, from 1-5 July 2007.at p.5
- Kaspersen W.K.H.(2004) Gathering electronic evidence, A paper presented at a Conference organized by Round Table II of the 17th International Congress of Penal Law. Held at Ant.N.Sakkoulas, on Monday, 4, October,(2004)pp.80-81
- Li, X. (2007). International Actions Against Cybercrime: Networking Legal Systems in the Networked Crime Scene. *Webology*,4(3):1-45.
- Mark Clayton, (2011, April 20,) *Security Lags Cyberattack Threats in Critical Industries, Report* Christian Science Monitor, p.3
- Nagpal A. [2001 September]. *Cyberterrorism in the Context of Globalisation .A Paper presented at the National Seminar on Globalization and Human Rights) sponsored by India, UGC, held in India.*
- Nigerian National Policy for Information Technology*, (2001) Federal Ministry of Science and Technology, Abuja.
- OAS, Report. In: Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA III). Held in Washington D.C, USA, (1999) Chapter IV.
- OAS, Report In: Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA V) Held in Washington D.C. USA (2000) Appendix I.
- Piragoff K.D.(2004) International cooperation in combating cyber-crime and cyber-terrorism, A paper presented at a Conference organized by Round Table II of the 17th International Congress of Penal Law. Held at Ant.N. Sakkoulas, on Monday, 4, October, (2004), pp. 192-193.
- Sieber U. (2004) Computer crimes, cyber-terrorism, child pornography and financial crimes, A paper presented at a Conference organized by Round Table II of the 17th International Congress of Penal Law. Held at Ant.N.Sakkoulas, on Monday, 4, October, (2004) pp. 47-50
- Skol Harnsuthivarin,(2003) Cyber Security and the Safety of Electronic Commerce. A paper presented at the Workshop organized by APEC, Cyber Security Electronic Commerce Steering Group. Held in Phuket, Thailand from 15-16 August 2003. Pp43-46
- Steven, R. (2003. April) Sharing the knowledge: Government – private Sector Partnerships to Enhance Information Security. occasional paper series of the United States of

America's Air Force Institute for National Security Studies. (INSS). Presented at the US air force base, Washington DC, USA.

- Schlienger T, Teufel S. Information Security Culture : The Sociocultural Dimension in Information Security Management. In: *IFIP TC11 International Conference On Information Security*, Cairo, Egypt, 7–9 May 2002. (Report) on pp. 305-340
- Udotai B, (2004) Challenges of Cybercrime Enforcement in the ECOWAS Sub-Region-Case Study-Nigeria, a Paper presented at a seminar organized by NCWG. Held at NITDA Building Abuja in, 2004.
- Urbas G and Choo K. (2008). Resource Materials on Technology-Enabled Crime: Technical and Background Paper No.28. Canberra: Australian Institute of Criminology. p8
- United Nations Economic and Social Council,( 2004.June, 9 - 11 ) Report of Economic Commission for Africa United Nations Conference Centre Addis Ababa, Ethiopia, P.20.
- “Executive Summary”, (2001.March) *Nigerian National Policy on Information Technology (IT)*, Federal Ministry of Science and Technology: ii. Abuja.
- United Nations Economic and Social Council , Economic Commission for Africa (WSIS) Academia Research Network Brainstorming. In: Report of Workshop held in Ethiopia from, 9 – 11, June 2004. P.20.
- United Nations Economic and Social Council, Economic Commission for Africa. In: Report of a Workshop on Legal and Regulatory Framework for the Knowledge Economy. Held in Ethiopia from 28, April -1, May 2009 at p.12
- UNODC (2013) Comprehensive Study of the Problem of Cybercrime and Responses to it by Member States, the International Community and the Private Sector. Report - Expert group conduct a Comprehensive Study on Cybercrime in Vienna, 25-28 February 2013, p.8
- Victor Sabadash. (2004) Law Improvement: The legal base in fighting cyber crime. A paper presented at the conference organized by Computer Crime Research Center (CCRC). Held at Computer Crime Research Center, Eth- Zurich, on October, 27, 2004
- Viano C.E. (2004) Computer crimes and criminal law: international dilemmas and approaches, A paper presented at a Conference organized by Round Table II of the 17th International Congress of Penal Law. Held at Ant.N.Sakkoulas, on Monday, 4, October, (2004), pp. 51-52 & 67.
- Wu, K. (2012. Monday, April, 23, ) Cyber Crime: New Challenge to Mankind Society, Introduction to the Nature of Cyber Crime and its Investigation Process. A paper

presented at a course on Cyber Crime Investigation organized by Network Forensics and Law Interception Total Solution Provider ( E- Detective Solutions), held in Digital Education Institute, for Information Industry, Taiwan. at 19.

Walls D. (2002, March) Internet Related Fraud and Deceptions upon Individuals within the UK. (Final Report to the Home Office) United kingdom Home office unpublished Report-2000

Xingan Li, (2004) International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene. A paper presented at the Workshop organized by APEC Cybercrime Expert Group, on APEC Telecommunications and Information, 29th Meeting. Held in Hong Konk, China from 21-26 March 2004, p.2