CYBERCRIME IN A CYBER-DEPENDENT WORLD: ENLISTING THE DEVELOPING WORLD IN ADDRESSING THE GROWING PROBLEM OF CYBERCRIME

by

RAPULUCHUKWU ERNEST NDUKA

Submitted in accordance with the requirements for the degree

DOCTOR OF LAWS

at

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROFESSOR M BASDEO

CO-SUPERVISOR: PROFESSOR MG KARELS

2019

DECLARATION

I declare that “CYBERCRIME IN A CYBER-DEPENDENT WORLD: ENLISTING THE DEVELOPING WORLD IN ADDRESSING THE GROWING PROBLEM OF CYBERCRIME” is my own work. All sources used or quoted have been indicated and acknowledged by means of complete references.

I further declare that I submitted the thesis to originality checking software and that it falls within the accepted requirements for originality.

I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.

Signed this _____ day of _____ 2019

.....

RE NDUKA

48067938

ACKNOWLEDGMENTS

My deep appreciation goes to God Almighty who gave me the strength to surmount the various challenges that dogged my path in completing this thesis.

My gratitude goes to my promoters, Prof M Basdeo and Prof MG Karels. Without your guidance I certainly would not have completed this research. I also appreciate the assistance of Prof F Cassim. I am grateful for your comments and suggestions.

My special thanks goes to my wife, His Worship (Mrs) C.V Nduka; my Children, Rapuluchukwu Jnr, Tochukwu, Chineme and Chidalu; and my parents, Sir and Lady J.R Nduka. You have made life easier for me. I thank you all for your support and for encouraging me.

To my colleagues at the Rock Chambers, Ndukaeze law firm, I say a big thank you. May God bless you all.

SUMMARY

The internet and its attendant benefits have brought about remarkable positive transformation in every sphere of the human enterprise, adding speed and efficiency through the availability and ease in transferring information without any obstruction by jurisdiction, time and cost. The inherent advantage that the ubiquitous nature of the internet brings also emphasises the need for proper and effective regulation of this “world without borders” if the world will not experience a breakdown of order. This will involve the combined efforts of both developed and developing countries.

The reality is that developed countries are taking proactive steps to tackle cybercrime, while developing countries are apathetic and are taking few or no steps to participate in the efforts to address cybercrime. This will hamper the measures put in place by developed countries to address cybercrime because of the ubiquitous nature of the internet.

This thesis examines the steps that may be embarked upon to get developing countries involved in addressing the growing problem of cybercrime. The efforts already undertaken by developed countries in their drive to halt cybercrime are highlighted. This research will be focused on objectively evaluating the response of developing countries in the fight against cybercrime, evolving ways to pull developing countries out of their inherent apathy in the growing spate of cybercriminal activities and to get them actively involved in tackling cybercrime.

This thesis therefore looks at the prevailing legislative, regulatory and law enforcement initiatives put in place by both developed and developing countries, identifies its inadequacies and proffers solutions on how both divides can be on the same page to effectively tackle cybercrime. This research proposes the emergence of harmonised legislation, harmonised law enforcement and adjudicatory systems that will accommodate and propel the active participation of both developed and developing countries in the fight against cybercrime. The thesis further identifies the

debilitating effects of various socio-economic factors on the ability of developing countries to effectively address cybercrime, and thus proffers a number of socio-economic strategies that will cure same. The thesis also accesses the existing regulatory and internet governance schemes which discourage the participation of developing countries and suggests the emergence of an effective regulatory structure that encourages universal participation.

Any effective effort that will lead to the participation of developing countries in tackling cybercrime will encompass several strategic legal approaches and non-legal approaches which will cut through some law-making and decision-making, law enforcement and prosecution, and socio-economic strategies. It is important that both developed and developing countries start taking steps to ensure that the menace of cybercrime does not get out of hand.

KEY TERMS

Cybercrime; computer crime; developing countries; trans-border data restrictions; legislative responses; law enforcement; legislation; online global law enforcement agency; international cyber-criminal court; apathy; internet governance

LIST OF ACRONYMS AND ABBREVIATIONS

ABLJ	American Business Law Journal
ACLR	American Criminal Law Review
AEFR	Asian Economic and Financial Review
AGORA IJJS	AGORA International Journal of Juridical Sciences
AJCI	African Journal of Computer and ICT
AJCI	African Journal of Computing & ICT
AJCJS	African Journal of Criminology and Justice Studies
ALAC	At-Large Committee
ALL NLR	All Nigeria Law Report
ALR	Ankara Law Review
APEC	Asia-Pacific Economic Cooperation
ARIN	American Registry for internet Numbers
ASO	Address Supporting Organisation
ATF	Bureau of Alcohol, Tobacco and Firearms
AU	African Union
BJASS	British Journal of Arts and Social Sciences
BJIL	Berkeley Journal of International Law
CCIPS	The Computer Crime and Intellectual Property Section (CCIPS)
CCNSO	Country Code Names Supporting Organisations
CCTLD	Country-Code Top-Level Domain
CECC	Council of Europe Cybercrime Convention
CFAA	Computer Fraud and Abuse Act
CLSR	Computer Law and Security Report
CoE	Council of Europe
CSEJ	Computer Science and Engineering Journal
DoJ	Department of Justice (US)
DoJ&CD	Department of Justice and Constitutional Development
ECOWAS	Economic Community of West African States
ECPA	Electronic Communications Privacy Act

E-crime	Electronic Crime
ECT ACT	Electronic Communications and Transactions Act
ECTF	Electronic Crime Task Force
EFCC	Economic and Financial Crime Commission
EJC	European Journal of Criminology
EU	European Union
GAC	Government Advisory Committee
GAC	Governmental Advisory Committee
GARJSS	Global Advanced Research Journal of Social Science
GCA	Global Cybersecurity Agenda
GCA	Global Cyber-security Agenda
GNSO	Generic Names Supporting Organisations
HJLT	Harvard Journal of Law and Technology
HLEG	High Level Experts Group
IAB	internet Architecture Board
ICANN	internet Corporation for Assigned Names and Numbers
ICC	International Criminal Court
ICCC	International Criminal Court for Cyberspace
ICE	United States Immigration and Customs Enforcement
ICPO-INTERPOL	International Criminal Police Organization
ICT	Information and Communications Technology
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IJLIT	International Journal of Law and Information Technology
IJPSM	International Journal of Police Strategies and Management
INTERPOL	International Police
IP	Internet Protocol
IRTF	Internet Research Task Force
ISOC	Internet Society
IT	Information Technology

ITA	Information Technology Act 2000
ITAA	Information Technology Amendment Act 2008
ITU	International Telecommunication Union
ITU-T	Telecommunication Standardisation Sector
JCLA	Journal of the Computer Law Association
JHTL	Journal of High Technology Law
JIA	Journal of Interactive Advertising
JICLT	Journal of International Commercial Law and Technology
JIL	Journal of internet Law
JILT	Journal of Information Law and Technology
JLPG	Journal of Law, Policy and Globalisation
LIJ	Legal Intelligence Journal
MAG	Multistakeholder Advisory Group
NDJICL	Notre Dame Journal of International and Comparative Law
NELR	New England Law Review
NJAS	Nordic Journal of African Studies
NRO	Number Resource Organisation
NSPA	National Stolen Property Act (NSPA)
NUPI	Norwegian Institute of International Affairs
NWLR	Nigeria Weekly Law Report
OECD	Organisation for Economic Co-operation and Development
PELJ	Potchefstroom Electronic Law Journal
PJSS	Pakistan Journal of Social Sciences
PPARJ	Public Policy and Administration Research Journal
RICPCRIA	Regulation of Interception of Communications and Provision of Communication Related Information Act
RIE	Review of International Economics
RIPE-NCC	Réseaux IP Européens Network Coordination Centre
RIR	Regional Internet Registry
RJLT	Richmond Journal of Law and Technology
SAPS	South African Police Service

SFU	Special Fraud Unit
SLR	Stanford Law Review
THRHR	Tydskrifvir Hedendaagse Romeins-Hollandse Reg/Journal of Contemporary Roman-Dutch Law
TLDs	Top-level domain names
TSB	Telecommunication Standardisation Bureau
UAE	United Arab Emirates
UDRP	Uniform Domain Resolution Policy
UK	United Kingdom
UN	United Nations
UNCITRAL	United Nations Commission on International Trade Law
UNODC	United Nations Office on Drugs and Crime
UNPOL	United Nations Police
USA	United States of America
W3C	World-Wide Web Consortium

TABLE OF CONTENTS

CHAPTER 1

EXAMINING CYBERCRIME: OVERVIEW AND INTRODUCTORY REMARKS

INTRODUCTION AND THEORETICAL BACKGROUND

The emergence of the internet has brought remarkable positive transformation in every sphere of human enterprise adding speed and efficiency through the availability and ease in the transfer of information without any obstruction by jurisdiction, time and cost. The emergence of internet technology, however, has brought to the fore new types of crime which in common parlance have been coined “cybercrime”.

The evolution of the internet and, invariably, cybercrime are tied to the evolution of computers and, therefore, it is imperative to examine the evolution of both computers and the internet in order to properly appraise the impact and public law management of cybercrime.

1.1. THE ELECTRONIC EVOLUTION

Through the ages, various computing devices (which in fact were calculating devices), such as the abacus,[1] have evolved for use by merchants.[2] Further technological inventions moved the calculating devices from ordinary beads arranged on a rack to machines that could add, subtract and multiply.[3]

---

1 The abacus may be considered the first computer and emerged about 5,000 years ago in Asia Minor. See Bansal SK *Information system management* (APH Publishing New Delhi 2002) 1-10.

2 Bansal *Information system management* 2.

3 In 1642 Blaise Pascal invented a numerical wheel calculator that could add, and in 1694 Gottried Leibniz invented machines that could multiply. See Chapuis RJ and Joel AE *100 years of telephone switching* (IOS Press Amsterdam 2003) 68-118.

Charles Babbage designed the mechanical computer, but Hollerith eventually invented the mechanical computer.[4] In the course of time, Atanasoff built the first special-purpose analog computer[5] that would assist scientists to perform long and complex calculations but which, at that point, were unable to store information. The invention of transistors in 1947 made the computer faster and reliable.[6] It was only in 1951 that a team of engineers designed and sold for public consumption computers with the added programming benefit of information storage.[7]

Subsequent technological advancements led to the creation of integrated circuits, which contained thousands of transistors and chips.[8] These helped the reduction of the size of the computer from gigantic space-consuming[9] equipment to digital palm-top equipment.

Computer systems possessing the ability to store, process, analyse and retrieve data brought with them enormous benefits on which individuals and businesses have become increasingly dependent. The computer subsequently has invaded the business and personal lives of every facet of human endeavour.

The advent of the internet, however, advanced the relatively individualised computer system into a super structure within which information can be communicated without any form of inhibition by geographic precincts[10] within fractions of a second.

---

4 Sharma V, Varshney M and Sharma S *Design and implementation of operating system* (University Science Press New Delhi 2010) 1-36.

5 This was invented between 1939 and 1943. See Gay MK *Recent advances and issues in computers* (Oryx Press Phoenix 2000) 96-116.

6 LaMorte C and Lilly J "Computers: History and development" http://www.dia.eui.upm.es/asignatu/sis_op1/comp_hd/comp_hd.htm (Date of use: 2 April 2012).

7 These computers could use both numbers and alphabets and were called UNIVAC 1 (Universal Automatic Computer); http://www.osdata.com/kind/history.htm (Date of use: 2 April 2012). The two engineers were John Mauchly and J Presper Eckert. See Null L and Lobur J *The essentials of computer organization and architecture* (Jones and Bartlett Publishers Sudbury 2006) 1-37. See also http://www.ideafinder.com/history/inventions/comeniac.htm (Date of use: 2 April 2012)

8 LaMorte and Lilly http://www.dia.eui.upm.es/asignatu/sis_op1/comp_hd/comp_hd.htm (Date of use: 2 April 2012).

9 ENIAC Computer, America's first large-scale electronic computer weighing 27 tons, was the size of an entire room, consumed 150 kilowatts of power and was water-cooled. Jain VK *Basic computer programming* (Pustak Mahal Publishers New Delhi 1995) 7-25. See also http://archives.cbc.ca/science_technology/computers/clips/4182/ (Date of use: 2 April 2012).

10 Leiner BM *et al* "Brief history of the internet" https://arxiv.org/html/cs/9901011? (Date of use: 21 April 2012).

1.2. EMERGENCE OF THE INTERNET

The earliest description of a global network that will enable social interaction was envisaged in 1962 by JCR Licklider[11] in his work "On-Line Man-Computer Communication".[12] Licklider visualised a system where computers are connected globally giving every user the ability to access data and programmes from any site and from any part of the globe. Licklider later moved on to the Defence Advanced Research Projects Agency (DARPA) to head the work to develop this vision of globally-interconnected computers.[13]

In 1961 Leonard Kleinrock of MIT developed the theory of packet-switching and published his first paper on packet-switching, which was to shape the foundation of internet connections. In 1969, based on these and many other theories and research, the internet, which was known as ARPANET,[14] was launched online with four major computers[15] initially networked.[16] In June 1970, the Massachusetts Institute of Technology, Harvard, Bolt Beranek and Newman Inc, and Systems Development Corp

---

11 Licklider was a researcher with MIT who believed that the fullest potential of the computer can be achieved by improving its interaction with human beings. He wrote a series of memos describing his 'Galactic Network' which in spirit is the internet of today. Holden G *et al E-business* (John Wiley Publishers New Jersey 2009) 1-22.

12 Holden *et al E-business* 3.

13 Kent A and Hall CM *Encyclopedia of library and information science: Volume 71* (Marcel Dekker New York 2002) 146-161.

14 Advanced Research Projects Agency Network (ARPANET) was part of the United States Military programme however it was claimed by Bob Taylor of the Pentagon who was in charge of ARPANET that the creation of interconnecting computer was not a military programme but merely scientific. Saunders KM *Practical internet law for business* (Artech House Norwood 2001) 1-10. See also Peter I "The beginnings of the internet" http://www.nethistory.info/History%20of%20the%20Internet/beginnings.html (Date of use: 24 April 2012).

15 The four computers connected were at the computer research laboratories of UCLA (Honeywell DDP 516 computer); Stanford Research Institute (SDS-940 computer); UC Santa Barbara (IBM 360/75); and the University of Utah (DEC PDP-10). See Banzal S *Data and computer network communication* (Firewall Media Publishers New Delhi 2007) 633-708.

16 Howe W "A brief history of the internet" http://www.walthowe.com/navnet/history.html (Date of use: 24 April 2012).

(SDC) in Santa Monica, California, were added to the network.[17] Before the end of January 1971, Stanford University, MIT's Lincoln Labs, Carnegie-Mellon University, and Case-Western Reserve University were also connected. In a few months' time, National Aeronautics and Space Administration Ames,[18] MITRE Corporation, Burroughs Corporations,[19] RAND Research Institute[20] and the University of Illinois became connected.[21] Since then the level of interconnection has grown in leaps and bounds, and as at 2012 an estimated 9 billion devices were connected to the internet, while it is projected that by 2020 over 200 billion devices will be connected to the internet.[22]

At the early stages of the internet, it was only operable by computer experts, scientists and librarians. At that stage the internet was not user-friendly and embodied a complex system that required prior learning before its navigation was possible.[23] There has been such tremendous development over the years that even two year-olds can now navigate the internet.[24]

The internet and computers have brought untold benefits to individuals, organisations and governments, so that financial transactions, sales, education, auctions, gambling and almost every other traditional activity can now take place in this "world without borders". For instance, information on the activities of individuals, organisations and governments are made available on the internet. Traditional retail companies have their goods and services advertised and sold on the internet and the physical goods shipped to buyers' addresses.[25] Bank customers prefer online banking over traditional branch

---

17 Howe http://www.walthowe.com/navnet/history.html (Date of use: 24 April 2012).

18 This is the research centre for NASA http://www.nasa.gov/centers/ames/about/overview.html (Date of use: 24 April 2012).

19 http://www.unisys.com/unisys/about/company/history.jsp?id=209 (Date of use: 24 April 2012)

20 Ware WH "RAND contributions to the development of computing" http://www.rand.org/about/history/ware.html (Date of use: 24 April 2012).

21 Howe http://www.walthowe.com/navnet/history.html (Date of use: 24 April 2012).

22 Rayes A and Salam S *Internet of things from hype to reality: The road to digitization* (Springer Publishers Cham 2017) 1-32.

23 Howe http://www.walthowe.com/navnet/history.html (Date of use: 24 April 2012).

24 Dybwad B "2 year-old finds Ipad easy to use" http://mashable.com/2010/04/06/2-year-old-girl-uses-ipad/ (Date of use: 24 April 2012).

25 According to Consultancy Verdict Research, online sales has doubled in the United Kingdom to £26.3bn and will rise to £40bn by 2015. See Butler S "Tesco and rivals turn against huge stores as internet shopping takes over" http://www.guardian.co.uk/business/2012/mar/04/online-shopping-changes-hypermarket-strategy (Date of use: 13 August 2012).

banking for their financial transactions.[26] Traditional college and university courses are offered on the internet with options for distance learning with learning materials made available to the student on the internet, which also affords students the opportunity of reading up and writing examinations at the students' comfort and pace through the internet.[27] Communication is more dependable and quick on the internet.[28] All manners of entertainment can be accessed on the internet.[29] Communities and forums for social, professional and religious benefits are formed on the internet.[30] Business transactions are easily facilitated by means of the internet.[31]

According to the Cyberethics group, the immeasurable amount of information existing on the internet and the many users,[32] have made the internet the most valuable tool in a person's life.[33] In addition, the enormous amount of publications added on to the internet has caused cyberspace to evolve as the most powerful source of information that can be retrieved by the click of a mouse.[34] Information technology has transformed the outlook of communication with instant messaging, video conferencing, e-mail, social network mediums[35] and many other mediums of communication.[36] Voice, data and

---

26 Vaughn S "Consumers prefer online banking to traditional branch banking; Rosetta retail banking survey reveals consumer trends and insights" http://www.prweb.com/releases/2012/5/prweb9524621.htm (Date of use: 13 August 2012).

27 Mooney LA, Knox D and Schacht C *Understanding social problems* (Wadsworth Cengage 2013) 232-263.

28 Carmody B *Online promotions: Winning strategies and tactics* (Black Forest Press 2004) 47-77.

29 Carmody *Online promotions* 48.

30 Carmody *Online promotions* 48.

31 Carmody *Online promotions* 48.

32 45% of the American population uses the internet daily http://www.huffingtonpost.com/2010/06/22/internet-usage-statistics_n_620946.html (Date of use: 13 April 2012). The current population of the United States is above 300 million. See Rosenberg M "Current USA population" http://geography.about.com/od/obtainpopulationdata/a/uspopulation.htm (Date of use: 13 April 2012). Approximately 10 million Nigerians use the internet, while nine out of ten Dutch use the internet. See http://www.nationmaster.com/country/ni-nigeria/int-internet (Date of use: 13 April 2012).

33 http://www.cyberethics.info/cyethics2/page.php?pageID=70&mpath=/86/88 (Date of use: 13 April 2012).

34 http://www.cyberethics.info/cyethics2/page.php?pageID=70&mpath=/86/88 (Date of use: 13 April 2012).

35 Twitter, a social networking site, has 175 million registered users as at March 2011, while Facebook, another social networking website, has approximately 600 million users as at March 2011. See Gordon GR and McBride RB *Criminal justice internships: Theory into practice* (Anderson Publishing Waltham 2012) 11-17. See also Carlson N "How many users does Twitter

images can be transferred around the world in a matter of microseconds.[37] Anything can now be purchased on the internet, while traditional shopping malls are currently relegated in favour of cyber-shopping, which can even be done from the comfort of one's bedroom. Financial institutions rely heavily on information technology systems, shifting the "banking industry from paper and branch banks"[38] to digital networked banking services while allowing customers to transact their various businesses without visiting the bank hall.[39] Computers and the internet have positively affected every facet of human endeavour.

Unfortunately, this new technology with its accompanying enormous benefits has also provided the environment and means for the commission of various criminal activities. The ease in transmission of information and data and the absence of geographical boundaries have further aided the advent of new types of crime. This is so because traditional human activity revolves mainly around information and data. The length of time in conveying information and data from one location to another or between countries is minimised with the internet. For example, traditional distribution of child pornographic materials will entail printing the material and transporting this to various locations, which is time-consuming and capital-intensive, while it can be uploaded onto a computer system and transmitted to various locations in a matter of seconds.

---

really have" http://articles.businessinsider.com/2011-03-31/tech/30049251_1_twitter-accounts-active-twitter-user-simple-answer (Date of use: 13 April 2012).

36 Scott BA "Effects of technology and high-tech gadgets in our lives" http://ezinearticles.com/?Effects-Of-Technology-And-High-Tech-Gadgets-In-Our-Lives&id=5859939 (Date of use: 13 April 2012).

37 Ghaziri H "Information technology in the banking sector: Opportunities, threats and strategies" http://ddc.aub.edu.lb/projects/business/it-banking.html (Date of use: 13 April 2012).

38 Ghaziri http://ddc.aub.edu.lb/projects/business/it-banking.html (Date of use: 13 April 2012).

39 Ghaziri http://ddc.aub.edu.lb/projects/business/it-banking.html (Date of use: 13 April 2012).

1.3. WHAT IS CYBERCRIME?

It is important at this stage to define cybercrime because understanding the concept of cybercrime is a fundamental building block in properly analysing the various ways of getting developing countries involved in fighting the menace of cybercrime.

The concept of cybercrime was originally used to refer to criminal activities that use or target the internet. This term did not apply to stand-alone computer systems or closed computer networks.[40]

However, the concept of cybercrime has now been used interchangeably with various terms, such as e-crime; computer misuse; computer abuse; digital crime; internet crime; and computer crime, among other names.[41] The Cybercrime Convention in its explanatory report noted that reference to computer systems in the Cybercrime Convention includes "standalone" computers.[42]

It must be pointed out that, there is no clear agreement on the definition of cybercrime.[43] According to Dunn, "the vocabulary of clichés that inhabits the information-age debate, and the overall imprecision in terminology, obstruct meaningful analysis".[44]

First, the concept of cybercrime has its roots in the novel by Gibson[45] where he coined the term "cyberspace" which was a description of the mentally-created virtual environment where networked computer activity occurred.[46] Cybercrime, therefore, was

---

40 Alkaabi A *et al* "Dealing with the problem of cybercrime" in Baggili I (ed) *Digital forensics and cyber crime* (Springer Hiedelberg 2011) 1-18.

41 Ringwelski M "Effects of cybercrime" http://www.ehow.com/about_5052659_effects-cyber-crime.html (Date of use: 24 April 2012).

42 Paragraph 23 Council of Europe Convention on Cybercrime, 2001 (ETS No 185) Explanatory Report.

43 Wall D "Policing cybercrimes: Situating the public police in network of security within cyberspace" in Palmer D, Berlin MM and Das DK (eds) *Global environment of policing* (CRC Press Boca Raton 2012) 161-186.

44 Dunn M "A comparative analysis of cybersecurity initiatives worldwide" http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf (Date of use: 2 March 2012).

45 Wall DS *Cybercrime: The transformation of crime in the information age* (Polity Press 2007) 8-29. See also Gibson W *Neuromancer* (Voyager London 1995) 4.

46 Wall *Cybercrime* 10.

a description of the crimes that took place within that virtual space.[47] It is submitted that this is a good starting point in understanding the concept of cybercrime since any crime which occurs within cyberspace is covered and crimes against a stand-alone computer system need not be roped into the concept of cybercrime.

Parker, one of the earliest writers on cybercrime, referred to cybercrime as computer abuse and defined it as "any intentional act in which one or more victims suffered or could have suffered a loss, and one of the perpetrators of the crime made or could have made a profit"[48] by means of the knowledge of information systems.[49] He used the terms "computer abuse"[50] and "misuse" in describing the term "because the word abuse allows him from having to differentiate between what is a crime and what is not".[51] Kshetri[52] partly aligned himself with the position of Parker in his analysis of cybercrime by describing cybercrime and its motivation in terms of the cost benefit and economic attraction to the cybercriminal.[53]

Maat observed that the problem with the definition given by Parker was that the requirement of profit or loss as an ingredient of cybercriminal activity places a restriction on the nature of actions that should be criminalised.[54] Various malicious acts may cause harm to a computer system, yet provide no benefit to the perpetrator.[55]

According to Kowalski, the Canadian enforcement agencies, in evolving a working definition for the concept of cybercrime, has defined cybercrime as "a criminal offence

---

47 Wall *Cybercrime* 10.

48 Parker DB *Fighting computer crime – A new framework for protecting information* (Wiley Computer New York 1998) 27-55.

49 Parker *Fighting computer crime* 45.

50 Donn Parker in an earlier work had made reference to computer crime as computer abuse. See Parker D *Computer abuse perpetrators and vulnerabilities of computer systems in national computer conference* (ACM New York 1976) 65-73.

51 Freiberger P "Micro crime macro problem" *Infoworld Texas 1981* 37-38.

52 Kshetri N "The simple economics of cybercrimes" 2006 *IEEE Security and Privacy* 33-39.

53 Kshetri, however, gave a broad definition of cybercrime as broadly "as any crime that employs a computer network in any phase of the crime". Kshetri *IEEE Security and Privacy* 33.

54 Maat SM *Cyber crime: A comparative law analysis* (LLM dissertation, University of South Africa 2004) 16-17.

55 Most viruses were created to prove that a new virus is possible. See http://www.sophos.com/sophos/docs/eng/comviru/viru_ben.pdf (Date of use: 8 March 2012).

involving a computer as the object of the crime, or the tool used to commit a material component of the offence".[56] Edwards *et al* observed that this was a valuable definition as it eradicates instances where the computer plays a passive role in the commission of an offence.[57]

The Symantec Corporation[58] took a step further in an effort to proffer a broad definition of the concept of cybercrime and defined cybercrime as "any crime committed using a computer or network, or hardware device". This definition stretches the concept of cybercrime to not only revolve around crimes that target the computer systems and networks, but also to include criminal activities that take place within stand-alone hardware.[59]

However, Wall[60] argued that the term "cybercrime" will have a "greater meaning if we construct it in terms of the transformation of criminal or harmful behavior by networked technology, rather than simply the behaviour itself".[61] Several other authors define cybercrime in terms of the category of the nature of the crime committed. According to the Australian Centre for Police Research, electronic crime was defined as "offences where a computer is used as a tool in the commission of an offence, as the target of an offence, or used as a storage device in the commission of an offence".[62]

Sieber[63] argued that cybercrime should be defined in a broad sense and opined that the expression "computer crime" was defined by the OECD as "any illegal, unethical or unauthorised behaviour involving automatic data processing and/or transmission of

---

56 Kowalski M "Cyber crime: Issues, data sources, and feasibility of collecting police-reported statistics" http://publications.gc.ca/Collection/Statcan/85-558-X/85-558-XIE2002001.pdf (Date of use: 1 March 2012).

57 Totty R and Hardcastle A "Computer related crime" in Edwards C, Savage N and Walden I (eds) *Information technology and the law* (Macmillan Basingstoke 1990) 142-172.

58 http://www.pctools.com/security-news/cybercrime-international-concerns/ (Date of use: 08 March 2012).

59 Alkaabi *Dealing with the problem of cybercrime* 2.

60 Wall *Cybercrime 10*.

61 Wall *Cybercrime 10*.

62 James S and Warren I "Australian police responses to transnational crime" in Eterno JA and Das DK (eds) *Police practices in global perspective* (Rowman & Littlefield Maryland 2011)131-172.

63 Sieber U *The International emergence of criminal information law (LusInformationis)* (Heymanns Cologne 1992) 5.

data". This definition, although wide, seems to stretch the concept of cybercrime beyond the purview of criminal law because the definition also points to unethical behaviour which may not necessarily be a criminal action but merely bad conduct determined by the value system of a particular jurisdiction.[64]

Other variants of the quest to define the concept of cybercrime, attempt to take the objectives or motives[65] into account, defining cybercrime as "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks".[66] This definition appears to be more precise. However, it eliminates scenarios where the physical hardware is used to perpetrate traditional crimes, and also runs the risk of excluding crimes that are regarded as cybercrime in international treaties such as the CoE Convention on Cybercrime.[67]

In the quest for an apt definition of cybercrime, several legislative responses have come up with various descriptions of the concept of cybercrime from which the definition of cybercrime may be inferred. However, it must be borne in mind that finding a clear interpretation of the concept of cybercrime from a legislative inference will be somewhat difficult because, as clearly pointed out by Shinder,[68] legislators often do a poor job of defining terms, leaving law enforcement agencies to guess until the courts wade in to define and make ambiguous terms clear through judicial pronouncements.

---

64 "Ethics is far broader than law, which is a system of behavior enforced by the state with penalties for violations. Ethics is good conduct as determined by the values and customs of society". See Marshall J "Unethical rationalizations" http://ethicsalarms.com/rule-book/unethical-rationalizations-and-misconceptions/ (Date of use: 8 March 2012). See also Alkaabi *Dealing with the problem of cybercrime* 7.

65 http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf (Date of use: 24 April 2012).

66 According to Majid Yar, this definition was conceptualised by Thomas and Loader. See Yar M "The novelty of "cybercrime" 2005 *European Journal of Criminology* 407-427.

67 http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf (Date of use: 24 April 2012).

68 Shinder DL and Tittel E *Scene of the cybercrime* (Syngress Burlington 2002) 6.

However, although the various legislative responses cannot be said to be completely definitive on the concept of cybercrime, they provide a good springboard in determining what cybercrime depicts.[69]

For instance, the United Nations[70] defined cybercrime in two categories as

> "(a) cybercrime in a narrow sense (computer crime): any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them;
>
> (b) cybercrime in a broader sense (computer-related crime): any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network".[71]

The Council of Europe Convention on Cybercrime proposed a wider definition, describing cybercrime as involving "offences against the confidentiality, integrity and availability of computer data and systems",[72] "computer-related offences",[73] "content-related offences",[74] and "offences related to infringements of copyright and related

---

69 Chawki M "A critical look at the regulation of cybercrime" http://www.droit-tic.com/pdf/chawki4.pdf (Date of use: 24 April 2012).

70 "Tenth United Nations Congress on The Prevention of Crime and the Treatment of Offenders, Vienna, and April 2000" http://www.uncjin.org/Documents/congr10/4r3e.pdf (Date of use: 3 March 2012).

71 Mathur A "United Nations' definition of cybercrime" http://cyber-law-web.blogspot.com/2009/07/united-nations-definition-of-cybercrime.html (Date of use: 3 March 2012).

72 Chapter II Section 1 Title 1 of the Council of Europe Convention on Cybercrime, 2001 (ETS No 185). The section, articles 2-6 makes provision for the criminalisation of activities that revolve around illegal access, illegal interception, data interference, system interference, misuse of devices of computer system and network.

73 Chapter II Section 1 Title 2 of the Council of Europe Convention on Cybercrime, 2001 (ETS No 185). Articles 7-8 make provision for computer-related forgery and computer-related fraud.

74 Chapter II Section 1 Title 3 of the Council of Europe Convention on Cybercrime, 2001 (ETS No 185). Article 9 makes provision for offences related to child pornography.

rights".[75] This definition, however, does not cover offences such as identity theft, industrial espionage and some other cyber activities that are inimical to cyber users.[76]

The United Arab Emirates (UAE) Federal Law No.2 of 2006 on The Prevention of Information Technology Crimes moves a step further and states that apart from offences against computer data and systems and other computer-related offences, cybercrime also involves offences such as those that violate religious beliefs[77] or acts that threaten and violate family principles.[78] The UAE definition provides another good dimension by extending its definition of cybercrime to include the protection of family values.

Walden referred to Grabosky and noted that the issue of cybercrime was a case of "old wine in new bottles" as the offences are fundamentally common.[79] Walden agreed with the assertion by Grabosky that cybercrime involves traditional offences committed in a fresh environment as well as new offences made possible by this fresh environment.[80]

Gordon, in proffering an end to the controversy, associated himself with the definitions of cybercrime, stating that cybercrime refers to any criminal activity where a computer, network or hardware device is involved.[81]

---

75 Chapter II, Section 1, Title 4, Article 10 of the Council of Europe Convention on Cybercrime, 2001 (ETS No 185).

76 Sommer P "Malware and cyber-crime" http://www.publications.parliament.uk/pa/cm201012/cmselect/cmsctech/writev/mal/mal01.htm (Date of use: 24 April 2012).

77 Article 15 United Arab Emirates Federal Law No 2 The Prevention of Information Technology Crimes of 2006.

78 Article 16 United Arab Emirates Federal Law No 2 The Prevention of Information Technology Crimes of 2006.

79 Walden I *Computer crimes and digital investigations* (Oxford University Press New York 2007) 19.

80 Walden *Computer crimes* 19.

81 Gordon S and Ford R "On the definition and classification of cybercrime" http://profs.sci.univr.it/~giaco/download/Watermarking-Obfuscation/cybercrime%20classification.pdf (Date of use: 24 April 2012).

It is submitted that this definition is too broad and, therefore, will cover offences against stand-alone computers and offences perpetrated against and through a networked computer system.

Finally, Van der Merwe submitted that data and information contained in the computer system are the key concepts and, therefore, that information technology crime would be a better term to use than cybercrime.[82] This submission is a modern approach in the analysis of cybercrime as information technology covers every aspect of technology that is used in the retrieval, processing, storage, communication and management of information.[83] Therefore, this submission will apply to offences committed without the traditional computer (for instance with smart phones), since these hand-held devices may not fit into various people's conception of what a computer comprises of.

However, it is submitted that the use of the term "cybercrime" is wide enough to cover every facet of illegal activity performed with the aid of the computer, information technology, networks or the internet.

1.4. COMPUTERS, DATA AND NETWORK

Most of the different definitions, as mentioned above, presuppose that the perpetration of cybercrime involves computers, data and network, and it is pertinent to decipher the meaning of these concepts/technological devices.

1.4.1. COMPUTERS

The concepts of computer or computer systems were defined by the CoE as "any device or a group of interconnected or related devices, one or more of which, pursuant to a programme, performs automatic processing of data".[84] It is submitted that this definition of the term "computer" seems to be somewhat narrow, and will pose problems

---

82 Van der Merwe DP "Computer crime – Recent national and international developments" 2003 *THRHR* 31. See also http://gidsigned.com/sites/gidsigned/documents/Document_0000024.odt (Date of use: 6 April 2012).

83 http://www.wisegeek.com/what-is-information-technology.htm (Date of use: 6 April 2012).

84 Article 1(a) Council of Europe Convention on Cybercrime, 2001 (ETS No 185).

for law enforcement agencies that will need to decipher the meaning of the concept "computer" in order to carry out their duties.

A number of legislative instruments, such as the Computer Misuse Act (UK) 1990, have omitted the definition of the concept "computer" for fear that "any definition would soon become out of date due to the rapidity with which technology develops".[85] The British Court, *in DPP v Jones*, accordingly defined the computer as a "device for storing, processing and retrieving information".[86] This definition is a good effort by the Court to refrain from giving an all-encompassing definition that will soon become out of date.

The Computer Misuse Act of Singapore, a modified version of the Computer Misuse Act (UK),[87] has defined the computer as

> "an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include –
>
> (a) an automated typewriter or typesetter;
>
> (b) a portable hand-held calculator;
>
> (c) a similar device which is non-programmable or which does not contain any data storage facility; or
>
> (d) such other device as the Minister may, by notification in the Gazette, prescribe".[88]

---

85 Computer Misuse Act (UK) of 1990.

86 Per Lord Hoffman [1997] 2Cr App R, 155, HL 163. See also http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/ (Date of use: 20 March 2012).

87 Urbas G "An overview of cybercrime legislation and cases in Singapore" http://law.nus.edu.sg/asli/pdf/WPS001.pdf (Date of use: 6 March 2012).

88 Computer Misuse Act (Singapore) of 1993 http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan002107.pdf (Date of use: 20 March 2012).

This definition provides a broad understanding of the concept "computer" as it makes provision for various forms that the data processing device might take while still making provision for future scientific innovation that might change the scope of the current understanding of the concept computer. The term "computer", therefore, is used expansively to cover the software, hardware and firmware that are contained in the computer.[89]

It is submitted that, although some people might not regard hand-held devices such as the Blackberry as computers, it will rather be in line with modern dictates that any device that can perform the functions of processing, storing, communication of data and also transmission or connection into a network should be called a computer irrespective of the form that the device takes.[90]

1.4.2. DATA

Data was defined by the Council of Europe Convention on Cybercrime "as any representation of facts, information or concepts in a form suitable for processing in a computer system, including a programme suitable to cause a computer system to perform a function".[91] This definition, however, seems to restrict the application of data to computer systems since some scholars are not comfortable with referring to all forms of information technology systems as computers.[92]

The Data Protection Act of the United Kingdom, for its part, defines data as "information which is being processed by means of equipment operating automatically in response to instructions given for that purpose".[93] This is a broad definition that would accommodate every form of device that processes information and is not limited to computers.

---

89 Walden *Computer crimes* 15.

90 A mobile phone has all computing capabilities and can also be referred to as a miniature computer. See Greenspun P "Mobile phone as home computer" http://philip.greenspun.com/business/mobile-phone-as-home-computer (Date of use: 7 April 2012).

91 Council of Europe Convention on Cybercrime, 2001 ETS No 185.

92 Walden *Computer crimes* 13.

93 Section 1 Data Protection Act (UK) of 1998.

However, Wacks points out that data is only potential information and becomes information only once they are communicated, received and understood.[94] According to Bellinger *et al*, "data is raw. It simply exists and has no significance beyond its existence (in and of itself) It can exist in any form, usable or not. It does not have meaning of itself".[95]

Therefore, data may be defined in a nutshell as any representation of facts in any form that can be processed through any information technology device with the capacity to be communicated.

1.4.3. NETWORK

Walden in describing the concept "network" stated that the term refers to all forms of systems that allow the communication of data between diverse points, encompassing wireless, wireline systems, fixed and mobile access technology.[96] The Communications Act (UK) 2003, in turn, defined the concept of electronic communication "network" as:

> "(a) a transmission system for the conveyance, by the use of electrical, magnetic or electro-magnetic energy, of signals of any description; and
>
> (b) such of the following as are used, by the person providing the system and in association with it, for the conveyance of the signals –
>
> (i) apparatus comprised in the system;
>
> (ii) apparatus used for the switching or routing of the signals; and
>
> (iii) software and stored data".[97]

---

94 Wacks R *Personal information privacy and the law* (Claredon Press 1989) 25. See also Walden *Computer crimes* 13.

95 Bellinger G, Castro D and Mills A "Data, information, knowledge, and wisdom" http://www.systems-thinking.org/dikw/dikw.htm (Date of use: 28 April 2012).

96 Walden *Computer crimes* 13.

97 Section 32 Communications Act (UK) of 2003.

It is imperative to note that the word “apparatus” covers any form of computer or device that is used in processing and transmitting the data, while “signals” cover the content being conveyed by the communicating parties.[98] Thus, Walden is of the opinion that the current growth of hand-held devices, such as the smartphone, may not fit into most people’s conception of what comprises a computer, while the integration of semi-conductor chips into a wide range of household items, such as televisions, runs the risk of over-criminalisation as the unauthorised use of such items could be determined a cybercrime.[99]

However, it is submitted that any device in any form that can process data and can communicate data through an electronic network would fall under the purview of computers in which case offences committed through it would constitute a cybercrime. In the same vein, if any household equipment has an electronic chip that possesses the ability to process data and communicate same through a network, it would not be over-criminalisation if offences committed through such a device are criminalised. This is so because the computer system, data and network are basic ingredients in the commission of a cybercriminal activity and, therefore, it follows that offences perpetrated on a stand-alone computer cannot fall under the purview of cybercrime since it is not interconnected. Offences against stand-alone computers can definitely fall under computer crime of which cybercrime is a subset. However, for the purposes of this thesis, the term computer crime, information technology crime and cybercrime may be used interchangeably.

Following from the above definitions, cybercrime takes place where there is the presence of computers, data and network, and the absence of one would only amount to theft.

98 Walden *Computer crimes* 16-17.
99 Walden *Computer crimes* 17.

1.5. TAXONOMIES

In order to properly analyse the issues revolving around cybercrime, it is pertinent to examine the classification of cybercrime. As noted by Walden, the purpose of taxonomy is to provide a framework on which various types of criminal activities present in cyberspace can be effectively analysed.[100]

The classification of cybercrime is problematic with regard to which offences would fall under the purview of cybercrime and what should be left out. This difficulty is demonstrated by the divergent views various jurisdictions hold on what cybercrime entails. The following discussion will illustrate this further.

According to the UN, cybercrime is categorised into two classes:

> "a) cybercrime in a narrow sense (computer crime): any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them;
> (b) cybercrime in a broader sense (computer-related crime): any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network".[101]

Brenner[102] classified cybercrime into three classes:

(1) computer as a target of the crime;
(2) the use of the computer as the tool in committing the crime;
(3) the use of a computer as incidental to the commission of the crime where the computer plays a minor role.

---

100 Walden *Computer crimes* 24.

101 http://cyber-law-web.blogspot.com/2009/07/united-nations-definition-of-cybercrime.html (Date of use: 3 March 2012).

102 Brenner SW *Cybercrime: Criminal threats from cyberspace* (Greenwood Publishing California 2010) 39-48.

While agreeing with the classification by Brenner, the cybercrime investigation and forensics further added "crime associated with the prevalence of computers"[103] as an additional classification of cybercrime.

Several other authors classify cybercrime into two categories. For instance, according to Alkaabi,[104] the Foreign Affairs and International Trade of Canada classified cybercrime into two categories:

(1) Crimes perpetrated using computer and networks (for instance hacking and computer virus);
(2) traditional crimes that are facilitated through the use of computers (for instance child pornography).

The US Department of Justice has classified cybercrime into three categories:

"(1) the computer as a target – attacking the computers of others (spreading viruses is an example);
(2) the computer as a weapon – using a computer to commit "traditional crime" seen in the physical world (such as fraud or illegal gambling);
(3) the computer as an accessory – using a computer as a "fancy filing cabinet" to store illegal or stolen information".[105]

In contrast, other classifications consider various other factors instead of the role that computers play in the commission of a cyber-criminal activity.[106] These other factors include the following:

---

103 http://www.scribd.com/doc/15938005/Cyber-Crime-Investigation-and-Cyber-forensic (Date of use: 21 March 2012).
104 Alkaabi *Dealing with the problem of cybercrime* 7.
105 http://www.cybercitizenship.org/crime/crime.html (Date of use: 31 March 2012)
106 Alkaabi *Dealing with the problem of cybercrime* 2.

(1) *motivation* of the perpetrator rather than the nature of the crime (for instance the motivation for a hacker may be curiosity while the motivation for another hacker may be the financial reward);[107]

(2) *outcome* of the cyber-criminal activity;[108]

(3) *communication* of the crime (for instance in child pornography, communication is a more serious offence than possession);[109]

(4) *information* as the target of the crime (for instance theft of trade secrets);[110]

(5) *threats*;[111]

(6) *attackers*;[112]

(7) *attacks*;[113] and

(8) *victims*.[114]

The CoE Convention on Cybercrime[115] has classified cybercrime into four categories, as follows:

(1) "offences against confidentiality and integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference and misuse of devices)";[116]

(2) computer-related offences (forgery and fraud);

(3) content-related offences (child pornography); and

(4) "offences related to the infringement of copyright and related rights."[117]

---

107 Walden *Computer crimes* 14.

108 Walden *Computer crimes* 14.

109 Walden *Computer crimes* 14.

110 Walden *Computer crimes* 14.

111 Sukhai NB "Hacking cybercrime" in (proceedings of the 1st annual conference on information security development 17-18 September 2004 Kennesaw) 128-132.

112 Chen TM and Davis C "An overview of electronic attacks" in Kanellis P *et al* (eds) *Digital crime and forensic science in cyberspace* (Idea Publishing London 2006) 1-26; see also Alkaabi *Dealing with the problem of cybercrime* 7.

113 Chen and Davis *An overview of electronic attacks* 1-26.

114 Sabadash V "Victims of cybercrime" http://www.crime-research.org/news/04.17.2004/212/ (Date of use: 31 March 2012). See also Alkaabi *Dealing with the problem of cybercrime* 2.

115 Council of Europe Convention on Cybercrime, 2001 (ETS No 185).

116 Articles 2-6 Council of Europe Convention on Cybercrime, 2001 (ETS No 185).

117 Articles 2-6 Council of Europe Convention on Cybercrime, 2001 (ETS No 185).

The classification by the Council of Europe Convention on Cybercrime, although broad, does not address all computer-assisted threats such as identity theft.[118]

The government/industry conference on high-tech crime (G8 Summit), in a bid to cover the lacunae in the Council of Europe Convention on Cybercrime classification, posited that the best approach to classifying cybercrime (high-tech crime) should be according to the type of threat and not the type of crime.[119] The G8 Summit,[120] therefore, classified cybercrime by dividing the threats into:

(1) computer infrastructure attack - "operations to disrupt, deny, degrade or destroy the information resident in computers and computer networks, or the computers and networks themselves".[121] This would cover "malicious acts, unauthorised access, theft of service and denial of service";[122]

(2) computer-assisted threat – "malicious activities such as fraud, drug trafficking, money laundering, infringement of intellectual property rights, child pornography, hoaxes, gathering of information, illegal copy of datawhich are facilitated by the use of the computer. The computer is used as a tool in the commission of the offence/threat."[123]

Another form of classification categorises cybercrime in terms of the target of the offence and classed cybercrime into four categories:[124]

(1) cybercrime against individual (such as cyber stalking, email spoofing and spamming);

---

118 http://www.mofa.go.jp/policy/i_crime/high_tec/conf0105-6.html (Date of use: 7 April 2012).
119 http://www.mofa.go.jp/policy/i_crime/high_tec/conf0105-6.html (Date of use: 7 April 2012).
120 http://www.mofa.go.jp/policy/i_crime/high_tec/conf0105-6.html (Date of use: 7 April 2012).
121 http://www.mofa.go.jp/policy/i_crime/high_tec/conf0105-6.html (Date of use: 7 April 2012).
122 http://www.mofa.go.jp/policy/i_crime/high_tec/conf0105-6.html (Date of use: 7 April 2012).
123 http://www.mofa.go.jp/policy/i_crime/high_tec/conf0105-6.html (Date of use: 7 April 2012).
124 http://www.reportcybercrime.com/classification.php (Date of use: 24 April 2012).

(2) cybercrime against property (such as credit card fraud and intellectual property crimes);

(3) cybercrime against organisations (such as unauthorised access, denial of service and virus attack);

(4) cybercrime against society (such as cyber terrorism and forgery).

However, one consistent factor in all the classifications, irrespective of the mode of classification the various authors adopt, is the fact that the computer system either is the target of the crime or the tool used to facilitate the perpetration of the offence. It is obvious that any cyber activity that is sought to be criminalised will fall under one of these categories.

It is also apparent from the various definitions mentioned above that the term "cybercrime" is interpreted differently by different jurisdictions and authors. Therefore, as a result, what constitutes a cyber-criminal offence in one jurisdiction may be overlooked in another jurisdiction. However, one consistent factor is the presence of data, network and the computing device irrespective of its form. This, therefore, leaves out the stand-alone computer system from the purview of cybercrime, but offences against the stand-alone computer may fall within the concept of computer crime.

Therefore, the researcher will define cybercrime as any crime where the computer or network is used to aid the commission of the crime or where the computer, network or data is the target of the crime.

1.6. DEFINING THE RESEARCH PROBLEM

According to Power, "as the world moves into cyberspace and as all money flows into cyberspace, crime follows money and you're going to see it there".[125]

---

125 Power R "Deadbolting the backdoors on your network" http://www.ssg-inc.net/cyber_crime/digital_crime.html (Date of use: 9 April 2012).

The lacunae in the structure of the internet are being exploited by cyber-criminals to unleash mayhem on the internet. These challenges, which include the uncertainties of jurisdiction; the absence of regulation; varying legislations; the expertise and sophistication of cybercriminals; sophistication and adaptation of internet technology; and the volume of internet activity,[126] are further exacerbated by the apathy of developing countries to join the fight against cybercrime.

Thus, the inherent advantage that the ubiquitous nature of the internet brings and the attendant criminal activities perpetrated through this tremendous system pushes to fore the need for a proper and effective regulation of this "world without borders" since this "world" is being plagued by various criminal activities inimical to the peaceful existence and growth of this "borderless world".

According to Brokenshire, cybercrime annually costs the United Kingdom economy £27 billion.[127]

According to Symantec, cybercrime is costing the global economy more than the drug trade.[128] Symantec found out from their research that as at September 2011, cybercrime cost the global market $338 billion.[129] As at 2018, it was reported that cybercrime costs the global economy $600 billion annually.[130]

---

126 http://www.popcenter.org/problems/child_pornography/2 (Date of use: 13 April 2012).

127 Kirk J "Private industry group boosts UK cybercrime fight" http://www.computerworlduk.com/news/security/3289753/private-industry-group-boosts-uk-cybercrime-fight/ (Date of use: 9 April 2012).

128 Whittaker Z "Cybercrime costs $338bn to global economy; more lucrative than drugs trade" http://www.zdnet.com/blog/btl/cybercrime-costs-338bn-to-global-economy-more-lucrative-than-drugs-trade/57503 (Date of use: 13 April 2012).

129 Whittaker http://www.zdnet.com/blog/btl/cybercrime-costs-338bn-to-global-economy-more-lucrative-than-drugs-trade/57503 (Date of use: 13 April 2012).

130 Chalfant M "Cyber crime costs global economy $600B annually" http://thehill.com/policy/cybersecurity/374854-cybercrime-costs-global-economy-600-billion-annually-experts-estimate (Date of use: 14 September 2018).

However, not all cyber-criminal activity can be quantified in financial loss.[131] For instance, victims of child pornography suffer physical pain at the time of the abuse, psychological distress, feelings of fear, hopelessness, a distorted model of sexuality and the inability to maintain any emotional or sexual relationship.[132] Those who fall prey to cyber fraud and scams, apart from the financial loss suffered, also go through psychological distress, a lack of sense of security and self-esteem, and may never regain the money lost to the scammers.[133] The pain caused by cybercrime, although it cannot be compared to the gains, still causes enormous harm to individuals, governments and the economies of various nations and the global system.

Combating cybercrime can only be successful by the implementation of proper awareness, policy formulation, the enactment of necessary legislation and the deployment of the correct resources and technology.[134]

The ubiquitous nature of cybercrime dictates that any successful step in curbing the hazard has to take a global outlook. However, unfortunately there is a manifest disparity in the way various jurisdictions deal with this global menace. The various national responses are based on the different interpretations by each jurisdiction of what should be part of the criminal code. This mostly attributed to cultural, economic and sometimes religious influences prevalent in the relevant jurisdiction. Consequently, cyber criminals have taken advantage of these disparities and they greatly undermine global efforts to combat cybercrime. This is because where one country does not criminalise a certain action as a crime, an individual can take advantage of this to target another country that finds the same action offensive. For instance, when there was no law against a denial of service attack in Nigeria, the lacuna provided a good excuse for committing the offence

131 Whittaker Z http://www.zdnet.com/blog/btl/cybercrime-costs-338bn-to-global-economy-more-lucrative-than-drugs-trade/57503 (Date of use: 13 April 2012).

132 Their lives are literally distorted by the action of the cyber-criminal, http://www.popcenter.org/problems/child_pornography/2 (Date of use: 13 April 2012).

133 http://www.spamlaws.com/fraud-effects.html (Date of use: 9 April 2012).

134 Sembok TT "Ethics of information communication technology" http://www2.unescobkk.org/elib/publications/ethic_in_asia_pacific/239_325ETHICS.PDF (Date of use: 9 April 2012).

from Nigeria against a company in the United Kingdom since such action was not illegal in Nigeria.[135]

The efforts of developed countries such as the United States of America and European Union nations are greatly undermined by the apathy of developing countries. Therefore, the propelling factor behind this thesis is based on the assumptions that:

(i) there is an apparent apathy within developing countries in relation to addressing cybercrime and its attendant issues;
(ii) the legislative and regulatory measures put in place by many developing countries are still outdated and not in sync with the current technological realities; therefore the measures cannot effectively fight the growing threat of cybercrime;
(iii) the efforts of developed countries to nip the menace of cybercrime will not be completely effective if the support of the developing countries is not enlisted in the fight against cybercrime because of the ubiquitous nature of the internet.

This thesis demonstrates that various developed countries have taken laudable steps in nipping the menace of cybercrime in the bud. For instance, most developed countries have evolved laws to criminalise certain negative cyber activities. The European Union blazed the trail by evolving the Council of Europe Convention on Cybercrime[136] and urged member states and signatories to the Convention to domesticate and make the Convention part of their national laws. The United Kingdom has introduced a number of legislations on cybercrime such as the Computer Misuse Act (1990),[137] and updates of the Act in the Police and Justice Act (2006).[138] Australia for its part evolved the Cybercrime Act (2001),[139] while the United States has introduced various federal

135 Sec 36 Police and Justice Act (UK) 2006.
136 Council of Europe Convention on Cybercrime, 2001 (ETS No 185).
137 Computer Misuse Act (UK) 1990.
138 Secs 35-38 Police and Justice Act (UK) 2006.
139 Australian Cybercrime Act 2001.

legislations such as the Computer Fraud and Abuse Act 18 US Code § 1030,[140] and the various states[141] have statutes criminalising cybercrime.

Developed countries have also invested much in both human and technological resources in order to equip its law enforcement agencies with the requisite capacity to detect, prevent and successfully prosecute cybercriminals.[142] For instance, in 2011 the British government revealed that it would be spending £63million in fighting cybercrime.[143]

Human, material and technological resources have also been utilised substantially in creating awareness among the populace to ensure that people are alert and able to protect themselves from cybercrime. For instance, the British government created a special cybercrime unit in the police with the necessary training, skills and experience to effectively tackle cybercrime.[144]

Private and public organisations have put the necessary technological measures in place to prevent the intrusion of cybercriminals into the network of these organisations.[145] For instance, companies invest in technologies that prevent illegal access to the companies' networks, such as the use of data encryption, hardware and software firewalls, to protect these companies from cybercriminals.[146]

---

140 18 USC 1030 – Crimes and criminal procedure – Fraud and related activity in connection with computers.

141 For example, Texas has its updated Penal Code providing for computer crimes. See Title 7 Chapter 33 Texas Penal Code.

142 The UK government creates a new cybercrime unit of 'cyber-specialists' that gives the police forces across the country the requisite skills and experience to tackle cyber crimes. See Ragan S "UK unveils new cyber security strategy, will create new cybercrime unit". http://www.securityweek.com/uk-unveils-new-cyber-security-strategy-will-create-new-cybercrime-unit (Date of use: 13 April 2012).

143 http://www.which.co.uk/news/2011/02/government-allocates-63m-to-fight-cybercrime-245078/ (Date of use: 13 April 2012).

144 Nguyen A "Government creates new cyber crime unit" http://www.csoonline.com/article/695079/government-creates-new-cyber-crime-unit (Date of use: 24 April 2012).

145 http://us.norton.com/cybercrime/prevention.jsp (Date of use: 24 April 2012).

146 Girard F "What can companies do to prevent cyber crime?" http://www.ehow.com/info_8152903_can-do-prevent-cyber-crime.html (Date of use: 16 August 2012).

Unfortunately, with the various impressive steps taken by developed countries[147] in order to curb cybercrime, developing countries exhibit an alarming level of apathy towards taking any steps to fighting cybercrime or to join the fight against cybercrime. For instance, Nigeria recently enacted cybercrime legislation in Nigeria while this research was proceeding.[148] Most banks in Nigeria, however, do little to protect their customers from cybercrime and would rather blame their customers for cybercriminal activities against the customer in order to exonerate themselves from blame.[149] The police or cybercrime investigating units of most developing countries lack the capacity and funding to efficiently investigate and prosecute cybercrime.[150]

Chapter two of this thesis will deal mainly with the various steps already taken by developed countries and the steps taken by developing countries[151] with a view to finding the reason behind the apathy of developing countries and proffering solutions to the apathy of developing countries in fighting cybercrime.

---

147 For instance, developed countries have enacted statutes that will tackle cybercrime, such as the Computer Misuse Act (UK) 1990 and CoE Convention on Cybercrime. They also embark on awareness campaigns to educate the public about the ills of and how to prevent cybercrime. Most developed countries, such as the United Kingdom, have set up specially-trained cybercrime units in the police that may attempt to prevent, investigate and prosecute cybercriminals.

148 Onyekwere J "Cybercrimes Act 2015 and the need for further amendments" *The Guardian* 24 August 2015. However, one also finds snippets of laws that prohibit certain activities in the internet, scattered in various legislations. For instance, child pornography is criminalised by the Child Rights Act 2003.

149 In Nigeria, the government rolled out the cash-less initiative and banks, as a result of the initiative, compel their customers to sign up to internet banking and to use the automatic teller machines. However, in the event of the customer falling victim to any form of cybercriminal activity, the action is mostly blamed on the carelessness of the customer. See http://www.punchng.com/business/technology/cyber-laws-necessary-to-protect-cash-less-system-fico-boss/ (Date of use: 24 April 2012).

150 The donors to the Kenya Cybercrime Police Unit threatened to withdraw their funds as capacity was not being built and most senior police officers were frustrating efforts to build and increase capacity of the police in fighting cybercrime in Kenya; http://allafrica.com/stories/201204170035.html (Date of use: 24 April 2012).

151 Determining whether a country is a developed or a developing country depends on the gross domestic product (GDP) per capita; life expectancy; the extent of industrialisation; health care; child welfare; the standard of living; transportation; and the infrastructural and technological advancement of the countries. A country with high levels of these elements usually are termed developed countries, while countries that are yet to attain a high level of these criteria are termed developing countries. See Surbhi S "Difference between developed countries and developing countries" http://keydifferences.com/difference-between-developed-countries-and-developing-countries.html (Date of use: 4 November 2017).

Unfortunately, cybercrime is a global phenomenon and efforts by developed countries will yield very little or no fruit if the gap created by the apathy of developing countries is not taken care of. Therefore, the appropriate legal and legislative measures, technical and procedural measures, capacity, organisational structures and international cooperation must be set in place by developing countries with the help of developed countries if the fight against cybercrime is to gain momentum.[152]

The objective of this thesis, therefore, is to examine the extent to which the various national and international approaches to cybercrime have fared and to formulate ways of getting developing countries involved in the global effort to fight cybercrime.

The thesis will compare the approaches of various jurisdictions in developed countries in order to understand the effectiveness of their approach, and examine the factors that influenced these approaches with a view of replicating them in developing countries and also on to the global terrain.

To this end, the legal approaches by the following developed countries and one region will be evaluated: the United Kingdom; the United States of America;[153] and the European Union in general.[154] On the other hand, the position of the following developing countries will also be analysed: Nigeria, South Africa and India.[155] It must be

---

152 https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf (Date of use: 28 April 2012).

153 From the United Nations classification of developed countries, the United Kingdom, the United States of America, Australia and most nations within the European Union fall in the class of developed countries; https://web.archive.org/web/20050511011954/http://unstats.un.org/unsd/mi/developed_new.htm (Date of use: 4 November 2017).

154 The European Union is the leading regional body with proactive steps towards tackling cybercrime. The enactment of the Council of Europe Convention on Cybercrime with countries from other continents as signatories makes them the foremost regional body to tackle cybercrime. See Council of Europe Convention on Cybercrime, 2001 ETS No 185. On the other hand, the European Union is home to most developed countries of the world. See Martin W "The 25 richest, wealthiest, happiest and most advanced countries in the world" http://www.independent.co.uk/travel/the-25-richest-healthiest-happiest-and-most-advanced-countries-in-the-world-a7396051.html (Date of use: 4 November 2017).

155 From the United Nations classification of countries, Nigeria, South Africa and India fall in the category of developing countries. See http://www.ssr.org/DevelopingCountries (Date of use: 4

pointed out that some other countries have been classified as least-developed countries.[156] In this thesis however, the term developing countries will be used to also encompass countries classified as least-developed countries, since their level of development is worse than the recognised countries designated as "developing countries".

The thesis observes that, although most developed countries have formulated cybercrime legislation and are taking more steps to further update these legislations, most developing countries have either adopted the legislations of developed countries or simply rely on antiquated legislation and allow the courts to stretch the law to accommodate these new types of crime.[157]

The thesis, therefore, will analyse and review the current legislative responses of both the developed countries and the developing countries with a view to making out a case for the introduction of global uniform cybercrime legislation.

The thesis also observes that the apathy of developing countries towards fighting cybercrime is largely connected with various socio-economic factors, such as poverty, corruption and insecurity that affect the general development of the country, causing cybercrime to be the lowest on the scale of preference of these developing countries.

The thesis will also focus on identifying those factors that exacerbate the apathy of developing countries in fighting cybercrime. The thesis will proffer various socio-

---

November 2017). According to the United Nations a developing country is a "country with a underdeveloped industrial base and a low Human development index (HDI) relative to other countries". See Malek A, Carbone F and Alder J "Community engagement, rural institutions and rural tourism business in developing countries" in Oriade A and Robinson P (eds) *Rural tourism and enterprise: Management, marketing and sustainability* (Cabi Wallingford 2017) 145-157.

156 According to the United Nations, these are developing countries that "exhibit the lowest indicators of socioeconomic development, with the lowest Human Development Index ratings of all countries in the world". These include countries like Mozambique, Senegal, Malawi, Madagascar and a host of other countries. See Wang B "Poverty statistics and estimates and definitions" https://www.nextbigfuture.com/2011/02/poverty-statistics-and-estimates-and.html (Date of use: 12 October 2018). See also, https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/publication/ldc_list.pdf (Date of use: 12 October 2018).

157 Until 2015 Nigeria had no cybercrime legislation.

economic solutions that will rekindle the interest of developing countries in joining the fight against cybercrime.

The statistics on the menace of cybercrime portend that cybercriminal activities are on the increase and that there is an urgent need for efficient decisive action. For instance, CNBC news reports that Norton in a survey estimated that cybercrime cost the global economy over $450 billion in 2016[158] and is projected to progress to $2 trillion by 2019.[159] The *Telegraph* newspaper reports that in the United Kingdom, cybercrime accounts for almost half of the crimes committed in the country and more than 5,5million cyber offences are committed every year.[160] The FBI reports that online phishing increased by 2,370 per cent between January 2015 and December 2016, and this annually costs American businesses $500 million.[161] The number of viruses and malicious codes in circulation are countless. Thousands of social media accounts are hacked daily.[162]

The efforts by developed countries in fighting cybercrime seem to be not enough since there is a steady increase in the menace of cybercrime, and it seems that cyber-criminals are winning the war. The support of developing countries must be solicited if a meaningful dimension must be taken to win this war against cybercrime.

In summary, the thesis intends to examine the steps that may be embarked upon in order to get developing countries involved in addressing the growing problem of

158 Graham L "Cybercrime costs the global economy $450 billion: CEO" https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html (Date of use: 4 November 2017).

159 Morgan S "Cyber crime cost projected to reach $2 Trillion by 2019" https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#620937163a91 (Date of use: 4 November 2017).

160 Evans M "Fraud and cyber crime are now the country's most common offences" http://www.telegraph.co.uk/news/2017/01/19/fraud-cyber-crime-now-countrys-common-offences/ (Date of use: 4 November 2017).

161 Mathews L "Phishing scams cost American businesses half a billion Dollars a year" https://www.forbes.com/sites/leemathews/2017/05/05/phishing-scams-cost-american-businesses-half-a-billion-dollars-a-year/#783faf393fa1 (Date of use: 4 November 2017).

162 Ochman BL "Facebook silent as my account and 45 000 others are hacked. 600 000 Facebook logins are compromised daily. What to do if your Facebook account is hacked" http://www.whatsnextblog.com/2012/01/facebook-silent-as-my-account-and-45000-others-are-hacked-600000-facebook-logins-are-compromised-daily/ (Date of use: 24 April 2012).

cybercrime. The efforts already taken by developed countries in their drive to nip cybercrime in the bud will be analysed. The thesis will objectively evaluate the response of developing countries in their fight against cybercrime, and will make recommendations on steps that should be taken to pull developing countries out of their apathy to tackle cybercrime. It must be pointed out that this research spanned several years – from 2012 to 2018 when it was finally completed. Thus some statistics were figures obtainable within the period that specific portion of the research was put together.

1.7. DIRECTION AND FOCUS OF THE THESIS

This thesis acknowledges the fact that the menace of cybercrime is growing in leaps and bounds and will undoubtably negatively affect economic, private and government activities. In addition, most developed countries are taking various steps in addressing the menace of cybercrime. The thesis will attempt to show how developed countries have risen to the challenge of cybercrime.

This fight cannot reach its zenith without the involvement of developing countries because domestic solutions by developed countries alone are inadequate since cyberspace is global and has no geographic and political boundaries.[163]

However, it is evident that developing countries have taken few or no steps to participate in the efforts to address the growing menace of cybercrime. For instance, like most developing countries Mozambique has no cybercrime legislation and has not put in place any organisational structure, capacity building, technical and procedural measures to tackle cybercrime.[164]

---

163 Cassim F "Formulating specialised legislation to address the growing spectre of cybercrime: A comparative study" 2009 *Potchefstroom Electronic Law Journal* 36-79.

164 https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx (Date of use: 16 August 2019).

This unfortunate apathy by developing countries undoubtably will hamper the measures put in place by developed countries to address cybercrime because of the ubiquitous nature of the internet. For instance, most financial fraud that involves advance fee fraud is committed in Nigeria while the target of the swindle is in a developed country.[165]

The apathy of developing countries is exacerbated by various factors such as regulatory, cultural and social factors.[166] The impact of these factors and possible solutions to them will be discussed in the body of the thesis.

In finding answers to the apathy of developing countries in fighting cybercrime, the thesis intends to ask some salient questions and to provide some reasonable answers to the following research questions:

(i) What is the extent of the involvement of developing countries in tackling the menace posed by cybercrime?
(ii) What are the factors that impede the active participation of developing countries in taking decisive steps in joining the fight against cybercrime?
(iii) What effective strategies will ensure the participation of various stakeholders in developing countries in the fight against cybercrime?
(iv) Would a harmonised cybercrime convention or legislation provide the much-needed regulatory framework in addressing cybercrime, on the one hand, and propel developing countries to get involved in the fight against cybercrime, on the other?
(v) In answering (i) above, what is the level of the participation of developing countries in the control of cyberspace and/or policy making that affects the cyberspace?

In finding answers to the above questions, the thesis is divided into nine chapters.

---

165 http://www.419eater.com/html/419faq.htm (Date of use: 24 April 2012)
166 Shalhoub ZK and Al Qasimi SL *Cyber law and cyber security in developing and emerging economies* (Edward Elgar Cheltenham 2010) 1-29.

Introducing the thesis, chapter 1 addresses the origins of computers and the internet while highlighting the menace of cybercrime. This chapter defines cybercrime while looking at the varying views on the definition of cybercrime and the confusion associated with the evolution of a common taxonomy, in order to properly establish a good foundation for the analysis of the thesis.

Chapter 2 examines the legal measures put in place by developed countries in cybercrime prevention. In doing this, the legal measures taken by various developed countries such as the United Kingdom, the United States of America and the European Union in curbing the menace of cybercrime will be examined. To this end, the various legislative responses by these developed countries will be examined. This chapter will then discuss the various steps already taken by developing countries in curbing cybercrime and the existing apathy thereto. This chapter highlights the dearth of technical and policy capacity in the various cybercrime-fighting institutions of several developing countries. This chapter will also identify the factors that aid in curbing the apathy of developing countries. A case study of Nigeria, South Africa and India will be undertaken.

Chapter 3 reveals the differences in cybercrime taxonomies and legislations between nations and identifies the inherent disadvantages these differences pose in forming a unified front by various nations in the fight against cybercrime. The chapter also focuses on the disparities and the similarities between legislations in developed countries such as the USA and the United Kingdom, with the Council of Europe Convention on cybercrime and also highlights the necessary improvements that should be made. This chapter proposes a unified legislation born out of a unified cybercrime taxonomy.

Chapter 4 identifies the procedural hurdles in the investigation, prosecution and prevention of cybercrime. The chapter also analyses the threat posed by jurisdiction in effectively fighting cybercrime. The chapter makes out a case for a uniformed law enforcement agency and the emergence of an international judicial body on cybercrime

with an appellate jurisdiction that will ensure compliance with the regulatory mechanisms.

Chapter 5 examines various socio-economic steps that should be embarked upon to enlist the support of developing countries in fighting cybercrime. This chapter identifies that a major glitch that compounds the apathy of developing countries in fighting cybercrime are various socio-economic factors. The chapter will proffer steps that should be taken by developed countries to help deal with these socio-economic factors and the steps that should be taken by developing countries alike. This chapter will also examine the possibility of persuading developing countries to join the cybercrime fight through the provision of financial aid, trans-border data restrictions[167] and other strategies that will propel the private sector into lobbying its governments to comply with the fight against cybercrime, such as the restriction of trans-border data to the private sector.

Chapter 6 analyses the presence and activities of various policy-making bodies that affect cyberspace. This chapter analyses the organisational structure of the internet in relation to developing countries. The chapter identifies the need for the emergence of a regulatory body that will ensure compliance with cybercrime legislation. The chapter also identifies the absence of developing countries in participating in these various internet governing groups as a factor in the apathy of developing countries towards fighting cybercrime. To this end, the chapter poses the major question as to who governs the internet and what the place of developing countries is in such governance. The chapter will attempt to make suggestions that will see the involvement of developing countries in this regulatory body.

Chapter 7 will attempt to unveil the various factors that hamper international cooperation and, therefore, highlight the disadvantage of this disunity in effectively fighting

---

167 For example, India has been under intense pressure to increase their data protection and cybercrime regulation in exchange for more outsourcing. See Sainty K and Ailwood A "Managing compliance in the global space – Transborder data flow" http://www.aar.com.au/pubs/pdf/priv/pap30nov04.pdf (Date of use: 24 April 2012).

cybercrime. The chapter will formulate solutions that will strengthen international cooperation leading to the effective curbing of the menace of cybercrime.

Chapter 8 highlights the need for proper capacity building and examines the need for the establishment of formidable cybercrime-enforcing institutions versed with the knowledge and expertise in delivering progressive strategies as a step in fighting the menace of cybercrime. This chapter concludes the thesis with a summary of the research findings and conclusions. Recommendations that will bolster and position developing countries to properly address cybercrime are also made.

CONCLUSION

This chapter provides an overview of the concept of cybercrime, the purpose of this research and the steps that should be taken to find reasonable answers to the questions raised. It is evident that

(i) the menace of cybercrime grows in leaps and bounds and the efforts of developing countries in fighting the menace is not helping the fight;
(ii) the support of developing countries must be obtained since cybercrime is a global phenomenon;
(iii) the enactment of an efficient legal structure and legislation holds a key in the involvement of developing countries in the fight against cybercrime;
(iv) an understanding and identification of the socio-economic and political culture of the developing countries holds another key in resolving the apathy of developing countries;
(v) developing countries have been left behind in the scheme of things with regard to internet governance and the various regulatory processes that govern the internet; there is a veritable need for an efficient regulatory structure to be formulated and developing countries to be made part of the process;

(vi) enlisting the support of developing countries in fighting the menace of cybercrime transcends the formulation of cybercrime legislation and includes socio-economic strategies that will compel the involvement of developing countries in fighting cybercrime.

Therefore, the subsequent chapters will seek to find solutions on how to get the developing world involved in the fight against cybercrime. In the next chapter - chapter 2, the researcher examines the response of select developed and developing countries in addressing cybercrime. It analyses the legislative and law enforcement initiatives put in place by developed and developing countries using some countries as examples. The researcher in the next chapter will highlight the dearth of technical capacity to address cybercrime in developing countries and also decipher the factors behind the apathy of developing countries in taking adequate steps in addressing cybercrime. It will proffer some solutions that will address such apathy.

CHAPTER 2

THE RESPONSE OF DEVELOPING COUNTRIES IN CYBERCRIME PREVENTION AND THE APATHY OF DEVELOPING NATIONS IN RESPONSE

INTRODUCTION

The menace of cybercrime has become a significant source of concern to individuals, private organisations, national, regional and international governments. Because of the ubiquitous nature of the internet, various countries have taken measures to combat cybercrime. The menace of cybercrime has propelled various governments and organisations into evaluating their legal systems, taking essential socio-economic steps and putting in place the necessary technological measures to address cybercrime.

Several countries have overhauled their legal, socio-economic and technological responses to cybercrime and are still working assiduously towards evolving better ways to combat cybercrime, while other countries have done little or nothing to address this. It is evident that developed countries have made good efforts to tackle e-crime, and some developing countries are emulating their steps. Unfortunately, many developing countries are doing little or nothing to combat cybercrime. As pointed out by Cobb,[168] cybercrime cannot be tackled by one country but requires an international response. In

168 Cobb M "International computer crime requires an international response" http://www.computerweekly.com/tip/International-computer-crime-requires-an-international-response (Date of use: 4 November 2012).

the same vein, Putnam and Elliot observe that the challenge is how to regulate a technology that enhances rapid transactions and flow of information across continents while placing reliance on legal and investigative instruments that are made to apply to specific national jurisdictions.[169] Understanding the problems created by these procedural lacunae emphasises the fact that it would be desirable for nations to come to an international arrangement regarding the creation of an effective common front in tackling cybercrime.[170]

However, acknowledging the fact that coming to an international arrangement is not simple. It is pertinent that nations in the meantime make adequate efforts to tackle cybercrime.

The pertinent questions to be asked therefore are the following:

(i) What is the extent of the involvement of developing countries in tackling the menace posed by cybercrime?
(ii) What are the factors that impede the active participation of developing nations in taking decisive steps in joining the fight against cybercrime?

The purpose of this chapter is to examine the responses of developed countries in the fight against cybercrime while trying to decipher the reasons behind the apathy of most developing nations in taking adequate steps to combat cybercrime. The chapter will take a comparative look into the measures put in place by developed countries in their fight against cybercrime in order to point out the areas where various developing countries are not taking adequate steps to address the menace.

169 Putnam TL and Elliot DD "International responses to cyber crime" in Sofaer AD and Goodman SE (eds) *The transnational dimension of cyber crime* (Hoover Stanford 2001) 35-67.
170 Putnam and Elliott *International responses* 41.

The UN Office on Drugs and Cybercrime Study identified some effective responses that will address the threat of cybercrime.[171] Chief among the responses are adequate legislative responses; proper law enforcement; prosecution and capacity prevention (public-private partnerships and awareness creation); effective international cooperation; and observance of the principles of human rights and the rule of law.[172]

This chapter will analyse the legislative responses and the law enforcement initiatives put in place to tackle electronic crime.[173] In doing so, the chapter will examine the current trend in some developed countries in line with the above-mentioned responses to cybercrime and compare same with the position of some developing countries in order to ascertain the adequacy of the measures put in place by developing countries in fighting cybercrime.

The chapter will furthermore examine the various responses to cybercrime adopted by the United States of America and the United Kingdom in order to ascertain the adequacy of their various approaches. The measures taken by these developed countries will be compared to the position or measures prevalent in South Africa, India and Nigeria.

2.1. LEGISLATIVE RESPONSES OF DEVELOPED NATIONS

The prerequisite for an effective response and action against cybercrime is the enactment of an adequate legislative framework.[174] Cybercriminals cannot be convicted for a crime unless the offence is defined and criminalised with some form of punishment attached to it.[175] Various jurisdictions in response to the menace of cybercrime have

171 https://www.unodc.org/documents/southeastasiaandpacific/2012/05/cyber-crime/Bangkok_intro_presentation.pdf (Date of use: 4 November 2012).

172 https://www.unodc.org/documents/southeastasiaandpacific/2012/05/cyber-crime/Bangkok_intro_presentation.pdf (Date of use: 4 November 2012).

173 It should be noted that other effective responses to cybercrime will be also be addressed in chs 3-7 of this thesis.

174 Goodman MD and Brenner SW "The emerging consensus on criminal conduct in cyberspace" (2002) 6 *International Journal of Law and Information Technology* 139-223.

175 For example, sec 36(12) of the Constitution of the Federal Republic of Nigeria of 1999 provides that "[a] person shall not be convicted of a criminal offence unless that offence is defined and the

taken some legislative steps to address the issue. Developed countries have taken the lead in proscribing various cyberactivities and some developing countries have followed suit, while most developing countries have done little or nothing to proscribe even the major cybercrime threat.

This sub-section is poised to examine the legislative responses of some developing countries. In doing that, this sub-section will first examine the legislative responses of some developed countries that have taken the lead in proffering legislative solutions to cybercrime, in order to establish whether the current trend and apathy in the legislative responses of some developing countries are acceptable. To this end, the United States of America and the United Kingdom will be examined as examples of developed countries, while South Africa, India and Nigeria will be examined as examples of developing countries. This sub-section will not examine all the legislations in these countries but will examine the major relevant legislations.[176] Some inadequacies found in each country's legislation will be highlighted.

2.1.1. UNITED STATES OF AMERICA

The peculiar nature of the federal structure of the United States allows various states that make up the United States of America to enact their own legislation under the specified principle of federalism.[177] Therefore, various states have enacted cybercrime

---

penalty therefore is prescribed in a written law". This principle was further established in the case of Aoko v. Fagbemi (1961) 1 All NLR 400. See also the case of FRN v. Ifegwu (2003) 15 NWLR pt. 842 pg. 113; where it was held that "it is sacrosanct that no person shall be liable to be tried or punished in any court of this land except under the clear and unambiguous provisions of a written law".

176 To illustrate this in the United States of America jurisdiction, some state legislation will be examined because of the peculiar nature of the United States federal system of government.

177 Art 1 sec 8 of the United States of America Constitution stipulates certain areas the United States Federal Congress can make laws to regulate, while art 1 para 9 stipulates areas that the states" legislatures cannot make laws to regulate. See the United States of America Constitution http://www.usconstitution.net/const.html (Date of use: 6 November 2012). Also, by virtue of the Tenth Amendment, the state can make laws regulating areas not specifically listed in the Constitution. See Longley R "Federalism: Whose power is this?" http://usgovinfo.about.com/od/rightsandfreedoms/a/whatisfederalism.htm (Date of use: 6 November 2012).

laws in order to combat cybercrime.[178] However, as pointed out by Chik,[179] where the problem the law intended to solve has a national outlook and the involvement of the federal government and its agencies is essential, the federal legislature or congress can make a uniform and consistent law that is common to all states to address the problem. Where conflicts exist between a federal law and a state law, the federal law takes precedence.[180] However, subject to the federal legislation pre-empting state laws where they conflict, every state can enact its distinctive criminal legislation because there is no legal requirement compelling each state to adopt a uniform or already-existing national legislation.[181] There are several optional legal machineries[182] put in place to persuade states to adopt laws that are similar to the federal legislation or other state legislations in order to achieve uniformity and consistency.[183]

This sub-section will examine some state laws and the relevant federal legislations that address cybercrime.

2.1.1.1. STATE LEGISLATION

According to Brenner, various states in exercising their powers to enact criminal legislations have criminalised a wide range of activities that revolve around computers and their networks.[184] According to her, "computer intrusions and damage caused by

---

178 Longley R "Federalism: Whose power is this?" http://usgovinfo.about.com/od/rightsandfreedoms/a/whatisfederalism.htm (Date of use: 6 November 2012).

179 Chik W "Challenges to criminal law making in the new global information society: A critical comparative study of the adequacies of computer-related criminal legislation in the United States, the United Kingdom and Singapore" www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc (Date of use: 6 November 2012).

180 Drahozal CH *The supremacy clause: A reference guide to the United States Constitution* (Greenwood California 2004) 89-94.

181 Maxeiner JR "Uniform law and its impact on national laws limits and possibilities" in *United States of America national report* papers delivered at the Intermediary congress of the International academy of comparative law, 13-15 November 2009, Mexico City 1-46.

182 For example, the Uniform Acts or Laws which are "laws that are designed to be adopted generally by all the states so that the law in one jurisdiction is the same as in another jurisdiction". See http://legal-dictionary.thefreedictionary.com/Uniform+Acts (Date of use: 11 November 2012).

183 Chik www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc (Date of use: 6 November 2012).

184 Brenner S "State cybercrime legislation in the United States of America: A survey" 2001 *Richmond Journal of Law and Technology* 28-36.

computer intrusions" are the greatest concern of the majority of state cybercrime statutes in the United States.[185] Under the offence of intrusion, states provide for two main categories of criminal activities, which are trespassing or hacking[186] and vandalism or cracking[187] of the computer or a computer network.[188] The offender must also possess the requisite mental state to be convicted of the cybercriminal activity.[189] Most states have also criminalised the "causing and/or denial, disruption, degradation or interruption of the use of computer services or gaining access to a computer system or network".[190]

A considerable number of states, such as Georgia,[191] have criminalised "computer invasion of privacy" which refers to a situation where the offender gains access to an individual's personal data such as the individual's financial and medical history, employment, salary, credit and other personal records or information.[192]

According to Brenner,[193] some states have criminalised the "misuse of computer information" which proscribes activities that copy, receive or use data obtained through hacking or cracking of a computer or computer network.[194] A substantial number of

185 *Brenner 2001 Richmond JLT* 34.

186 Trespassing or hacking refers to a situation where an offender wilfully accesses a computer or computer network without authorisation. See for example art 5 sec 13A-8-102(a) Computer Crime Act of Alabama State http://www.internetlibrary.com/statuteitem.cfm?Num=10 (Date of use: 11 November 2012).

187 Vandalism or cracking refers to a situation where the offender wilfully accesses a computer without authorisation and modifies, destroys or upsets the operation of the computer and/or the data it contains. For example, see art 5 sec 13A-8-103 Computer Crime Act of Alabama State http://www.internetlibrary.com/statuteitem.cfm?Num=10 (Date of use: 11 November 2012).

188 *Brenner 2001 Richmond JLT* 34.

189 Virtually all the states provide for mental capacity before a person can be liable for the offence under cybercrime legislation. See http://www.encyclopedia.com/topic/Computer_Crime.aspx#2 (Date of use: 11 November 2012).

190 Sec 76-6-703 Criminal Code of Utah State http://le.utah.gov/code/TITLE76/htm/76_06_070300.htm (Date of use: 11 November 2012). See *Brenner 2001 Richmond JLT* 34.

191 Sec 16-9-93c Computer Systems Protection Act of Georgia State, 1991 http://www.gaicac.us/Statutes_Georgia.htm#ComputerCrime (Date of use: 11 November 2012)

192 *Brenner 2001 Richmond JLT* 34.

193 *Brenner 2001 Richmond JLT* 34.

194 The states of Kentucky, Connecticut and Delaware have criminalised the misuse of computer information. See http://www.encyclopedia.com/topic/Computer_Crime.aspx#2 (Date of use: 11 November 2012). See also sec 935 Criminal code of Delaware State,

states prohibit the "intentional modification or destruction, without consent, of computer equipment or supplies used or intended to be used in a computer, computer system or computer network" which is referred to as an "offence against computer equipment or supplies".[195]

Many states, such as Alabama,[196] have criminalised the "use of computers to devise or execute fraud,[197] theft and embezzlement".[198] Many other states have criminalised "computer theft"[199] (which covers a number of other offences, such as information theft),[200] computer hardware theft[201] and software theft.[202] A significant number of states have also criminalised theft of computer services[203] and the use of a computer to commit theft in the conventional sense.[204] On the other hand, a few states[205] have proscribed the "unlawful possession of computer data and/or computer software".[206] Only a few states prohibit the "forgery or falsification"[207] of data in computers or computer systems.

---

http://delcode.delaware.gov/title11/c005/sc03/index.shtml#P1781_140437 (Date of use: 11 November 2012).

195 See sec 97-45-7 of the Criminal Code of Mississippi, 1972 (as amended) http://www.mscode.com/free/statutes/97/045/0007.htm (Date of use: 18 November 2012). See also *Brenner 2001 Richmond JLT* 34-35.

196 http://www.encyclopedia.com/topic/Computer_Crime.aspx#2 (Date of use: 11 November 2012).

197 This refers to the use of a computer or its system or network to devise any scheme for the purposes of defrauding or for the purposes of obtaining property, services or monetary gain through fraudulent representations. See art 5 sec 13A-8-102 (2) Alabama Computer Crime Act of 1985. See also sec 1 of the Penal Code of California State 502(c) https://mandreptla.org/CalifPenalCode502.htm (Date of use: 11 November 2012).

198 *Brenner 2001 Richmond JLT* 35.

199 Sec 11-52-1 General Laws of Rhode Island, 2000.

200 Sec 11-52-1 General Laws of Rhode Island, 2000.

201 See for example sec 2C: 20-25 Code of Criminal Justice of New Jersey, 1995 http://law.onecle.com/new-jersey/2c-the-new-jersey-code-of-criminal-justice/20-25.html (Date of use: 11 November 2012).

202 See for example sec 11-52-4 General Laws of Rhode Island, 2000.

203 See for example sec 935 Criminal Code of Delaware State http://delcode.delaware.gov/title11/c005/sc03/index.shtml#P1781_140437 (Date of use: 11 November 2012).

204 *Brenner 2001 Richmond JLT* 35.

205 See for example sec 61-3C-6 Computer Crime and Abuse Act of West Virginia http://www.legis.state.wv.us/wvcode/code.cfm?chap=61&art=3C (Date of use: 12 November 2012).

206 *Brenner 2001 Richmond JLT* 35.

207 For example, see sec 16-9-93(d) Computer Systems Protection Act of Georgia, 1991.

A few states have enacted statutes that prohibit the creation and spread of viruses and other malicious programmes that can harm the computer or its system and network,[208] while a few states have proscribed the introduction of false information into a computer system with the intent of "damaging or enhancing an individual's credit rating".[209] A small number of states have enacted legislation prohibiting the "interruption or denial of essential services" which are necessary for public health, welfare and safety, including emergency services, healthcare services, public or private utility, communication services, government services or transportation.[210]

A notable aspect of the various state legislations on cybercrime is the prohibition of offences against the person aided by the use of the computer system or network. A few states outlaw the use of the computer or its network to cause physical injury to a person.[211] A few states also prohibit the tampering or breaking into a computer system, thereby causing the death of an individual or creating a threat resulting in the death of an individual.[212] However, as pointed out by Brenner, no state has enacted a "cyber-homicide" offence.[213]

Among other prohibited computer-aided activities against a person are the prohibition of cyber-stalking, harassment and bullying.[214] A reasonable number of states have proscribed same.[215] For the offence to be committed, the offender must have frightened

---

208 See for example sec 502(c)(8) Penal Code of California https://mandreptla.org/CalifPenalCode502.htm (Date of use: 12 November 2012). See also *Brenner 2001 Richmond JLT* 34.

209 See for example sec 61-3C-14 West Virginia Code http://www.legis.state.wv.us/wvcode/code.cfm?chap=61&art=3C (Date of use: 12 November 2012).

210 For example, see Title 14 sec 73.7(b) Revised Statutes of Louisiana, 2011. See also *Brenner 2001 Richmond JLT* 36.

211 See sec 18.2-152.7 Virginia Code http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.7 (Date of use: 27 November 2012).

212 See sec 609.891(2) Minnesota Statutes 2012 https://www.revisor.mn.gov/statutes/?id=609.891 (Date of use: 27 November 2012).

213 *Brenner 2001 Richmond JLT* 30.

214 *Brenner 2001 Richmond JLT* 30.

215 See sec 11.41.270 Alaska Statute http://www.legis.state.ak.us/basis/folioproxy.asp?url=http://wwwjnu01.legis.state.ak.us/cgi-bin/folioisa.dll/stattx99/query=*/doc/{t3744}/pageitems={body} (Date of use: 27 November 2012).

or threatened to injure an individual or the family and must have transmitted this intent to the individual.[216]

According to Putnam and Elliot, these various state legislations have made a difference from the international custom by making a concerted effort in proscribing sexual crimes that involve the use of computers and their networks.[217] Sexual crimes constitute the second-largest body of offences prohibited by state cybercrime legislations in the United States, after computer intrusion and damage offences.[218] However, in criminalising sexual crimes a majority of states have only proscribed the use of computers to solicit sex or to lure a minor into sex by an adult.[219]

It is understandable that the majority of sexual offences revolve around luring a minor into a sexual act since sex between consenting adults ordinarily is not a crime in the United States, and the law seeks to protect the vulnerable minor who may not be in the right frame of mind to make an informed lawful decision. Several states in a bid to prohibit child pornography have criminalised the creation, storage or distribution of child pornography.[220] In addition, most states prohibit the compiling of information about a child in order to facilitate, offer, encourage or solicit an unlawful sexual act from the child.[221] While many states prohibit the use of computers to send obscene images to a

---

216 See also sec 947.0125(2) Wisconsin Statute http://docs.legis.wisconsin.gov/statutes/statutes/947/0125/1 (Date of use: 27 November 2012).

217 Putnam TL and Elliot DD "International responses to cyber crime" in Sofaer AD and Goodman SE (eds) *The transnational dimension of cyber crime* (Hoover 2001) 35-67.

218 Putnam and Elliott *International responses* 41.

219 See for example Title 11, sec 1112A Criminal code of Delaware http://delcode.delaware.gov/title11/c005/sc05/index.shtml (Date of use: 1 December 2012). See also Tennessee Code Annotated Section 39-13-528 http://www.state.tn.us/tccy/tnchild/39/39-13-528.htm (Date of use: 1 December 2012).

220 See for example sec 21-1040.13a Oklahoma Statutes http://oklegal.onenet.net/oklegal-cgi/ifetch?Oklahoma_Statutes.99+845214534629+F (Date of use: 1 December 2012).

221 Sec 21-1040.13a Oklahoma Statutes http://oklegal.onenet.net/oklegal-cgi/ifetch?Oklahoma_Statutes.99+845214534629+F (Date of use: 01 December 2012)See also Section 847.0135 Florida Statutes http://law.justia.com/codes/florida/2004/TitleXLVI/chapter847/847_0135.html (Date of use: 1 December 2012).

child,[222] the state of Pennsylvania proscribes communicating with a minor with the aid of the computer with the intent of luring the minor into prostitution.[223]

2.1.1.2. FEDERAL LEGISLATION

The United States have enacted a number of federal statutes that address the issue of cybercrime. The United States has approximately 40 federal legislations that address the issue of cybercrime.[224] However, the prominent federal legislative responses will be highlighted. The foremost federal statute on cybercrime is the Computer Fraud and Abuse Act (CFAA) of 1984 (as amended).[225]

There are also other legislations that prohibit cybercrime. According to Doyle, the CFAA deals with the computer or computer system as victims, while other federal statutes on cybercrime deal with the computer or computer system as the arena or repositories of evidence of crime.[226]

The CFAA prohibits gaining access into a computer to commit espionage with the intent to disclose information obtained therein to someone not authorised to receive that information.[227] The CFAA also prohibits computer trespassing that grants the perpetrator access to the financial records of a financial institution, governmental agency information, information from a protected computer[228] and also computer

---

222 See for example sec 13A-6-111 of the Criminal Code of Alabama.

223 See Title 18 Pennsylvania Statutes sec 6318.

224 Chik www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc (Date of use: 2 December 2012).

225 Computer Fraud and Abuse Act 18 United States Code sec 1030 (amended in 1986, 1988, 1989, 1990, 1994 and 1996) http://www.panix.com/~eck/computer-fraud-act.html (Date of use: 2 December 2012).

226 Doyle C "Cybercrime: An overview of 18 USC 1030 and Related Federal Criminal Laws" http://www.fas.org/sgp/crs/misc/97-1025.pdf (Date of use: 2 December 2012).

227 18 United States Code sec 1030 (a)(1) http://www.panix.com/~eck/computer-fraud-act.html (Date of use: 2 December 2012). See also Doyle http://www.fas.org/sgp/crs/misc/97-1025.pdf (Date of use: 2 December 2012).

228 18 United States Code sec 1030(a)(2) http://energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf (Date of use: 2 December 2012). See also Doyle http://www.fas.org/sgp/crs/misc/97-1025.pdf (Date of use: 2 December 2012).

trespassing into a government computer.[229] The CFAA also prohibits gaining unauthorised access into a protected[230] computer with the intent to commit fraud and the commission of the fraud.[231] It also prohibits the destruction of a protected computer with malicious programmes or codes.[232]

The CFAA further prohibits trafficking in passwords that will affect interstate or foreign commerce and computers used by the United States government.[233] It also prohibits the transmission of any threat to cause damage to a bank computer, government computer or any computer employed in foreign and/or interstate trade, with the intention of extorting money or other valuables from the legal entity.[234]

Another United States federal legislation that seeks to address the issue of cybercrime is Title 18 Section 1028 of the United States Code which prohibits identity theft by criminalising the production, transfer and/or possession of any device intended to be used to falsify personal or financial identifying documents.[235] The United States also has the Electronic Communications Privacy Act (ECPA), which proscribes the unlawful interception of a computer system and/or network and any other form of wire communication.[236] This law, therefore, protects illegal access to computer communications, whether in transit or stored on a computer system.[237] The Wire Fraud

---

229 18 United States Code sec 1030 (a)(3) http://energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf (Date of use: 2 December 2012).

230 A protected computer refers to any computer used by the financial institution or by the government of the United States or any computer including one located outside the United States used in interstate or foreign commerce or communication or that can affect interstate or foreign commerce or communication of the United States; http://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_%28CFAA%29 (Date of use: 2 December 2012).

231 Title 18 United States Code sec 1030(a)(4) See also Doyle http://www.fas.org/sgp/crs/misc/97-1025.pdf (Date of use: 2 December 2012) .

232 Title 18 United States Code sec 1030(a)(5) See also Doyle http://www.fas.org/sgp/crs/misc/97-1025.pdf (Date of use: 2 December 2012).

233 Title 18 United States Code sec 1030(a)(6)

234 Title 18 United States Code sec 1030(a)(7) See also Doyle http://www.fas.org/sgp/crs/misc/97-1025.pdf (Date of use: 2 December 2012).

235 Title 18 United States Code sec 1028.

236 Title 18 United States Code secs 2510-2522.

237 http://www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html (Date of use: 8 December 2012).

Act prohibits computer-aided fraud used to obtain money or property.[238] The National Stolen Property Act (NSPA) prohibits computer-aided transmission or transfer of funds which the transferor knows is stolen, converted or obtained by fraud.[239]

Title 18 Section 1462 of the United States Code prohibits the use of a computer or its system to import obscene materials into the United States.[240] The following section, Title 18 Section 1463, proscribes the transportation of obscene materials.[241] However, it does not mention the use of the computer as a means for the transportation. However, it can be inferred that since the computer can be used to import, store and transport obscene materials, this section can cover the use of computers in transporting obscene materials.

Section 2251 of Title 18 of the United States Code prohibits the sexual exploitation of minors by employing or inducing the minor into participating in the production of a visual depiction of sexually-explicit conduct or the transmission of such explicit conduct.[242] Section 2252 of Title 18 of the United States Code prohibits the transportation of child pornography by the aid of computer.[243] Finally, Title 18 Section 2319 of the United States Code prohibits the infringement of copyright.[244]

According to Brenner, United States federal legislations prohibit various traditional crimes and, therefore, cover traditional activities and conduct committed with the aid of the computer.[245]

238 Title 18 United States Code sec 1343.
239 Title 18 United States Code sec 2314.
240 Title 18 United States Code sec 1462.
241 Title 18 United States Code sec 1463.
242 Title 18 United States Code sec 2251.
243 Title 18 United States Code sec 2252.
244 Title 18 United States Code sec 2319.
245 *Brenner 2001 Richmond JLT* 35.

2.1.1.3. IDENTIFIED INADEQUACIES OF THE UNITED STATES LEGISLATIVE RESPONSE

The various legislative bodies in the United States have proactively enacted laws within their various sphere of control in order to address cybercrime. The United States evidently is taking the lead in addressing the issue of cybercrime.[246] However, Chik was quick to point out that a major flaw in the legislative response of the United States shows that the laws on cybercrime were introduced piecemeal, as the crime emerged.[247] These legislations, although proactive and wide enough to cover various offensive activities committed in cyberspace, have other flaws which will be enumerated.

For the state legislative responses, it is submitted that the various states with cybercrime laws in the United States have done a good job in criminalising various cyber activities, and most academics are of the opinion that the state laws are currently adequate to handle cybercrime in the United States and that further federal legislative measures are not necessary.[248] However, one great impediment to the efficacy of the state legislative response is that since cybercrime is not bound by state jurisdictions and boundaries, state legislation are impaired and can only operate within their territorial sphere of control. State courts will also be ineffective in fighting cybercrime.[249] As observed by Brenner, "there is a great deal of variation – both in terms of coverage and in terms of approaches – in the cybercrime legislation adopted by the various states" [250] and the contrasting laws among the various states pose a great threat to tackling cybercrime since cybercriminal activities can be interstate.[251] Unfortunately, as pointed out by Chik, the United States will continue to enact state-centric legislations that

246 Cassim F "Formulating specialised legislation to address the growing spectre of cybercrime: A comparative study" 2009 *Potchefstroom ELJ* 46.

247 Chik www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc (Date of use: 8 November 2012).

248 Dierks MP "Computer network abuse" 1993 *Harvard Journal of Law and Technology* 307-342.

249 Sloan J "Fighting computer crime by combining Federal and State law" http://www.uplink.com.au/lawlibrary/Documents/Docs/Doc121.html (Date of use: 2 December 2012).

250 *Brenner 2001 Richmond JLT* 39.

251 *Brenner 2001 Richmond JLT* 39.

address cybercrime in the way that states enact other criminal laws. Therefore, the ubiquitous nature of cyberspace suggests that the principles of jurisdiction which properly govern the application and enforcement of other criminal laws will not properly apply to cyberspace.[252] In addition, on the other hand, the absence of a uniform procedural system has contributed to making adjudication and enforcement of the varying states laws difficult.[253]

It is submitted that having a uniform federal legislation that addresses the issue of cybercrime in the United States will be a better approach to tackle the menace of cybercrime instead of relying on the varying state legislations that create some difficulty in the deterrence and punishment of offenders.

As far as the inadequacies of the United States federal legislations on cybercrime are concerned, it should be noted that the federal legislations on cybercrime are not as comprehensive and practical as the legislations enacted by the various states in fighting cybercrime with their other traditional statutes.[254] According to Sloan, the Computer Fraud and Abuse Act of 1984, the chief federal legislation on cybercrime, is hardly ever used and has received little consideration by United States federal prosecutors.[255] The limitation in the Computer Fraud and Abuse Act of 1984, which is the resultant effect of streamlining the statute to cover only fraud and abuse against the United States federal government, has prompted United States federal prosecutors to instead rely on the Wire Fraud Statute[256] in its prosecution of fraud-related cybercriminal activities.[257] Unfortunately, the Wire Fraud Statute may also not be applicable when the illegally-

252 Chik www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc (Date of use: 10 November 2012).
253 Chik www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc (Date of use: 10 November 2012).
254 Sloan http://www.uplink.com.au/lawlibrary/Documents/Docs/Doc121.html (Date of use: 10 December 2012).
255 Sloan http://www.uplink.com.au/lawlibrary/Documents/Docs/Doc121.html (Date of use: 10 December 2012).
256 Title 18 United States Code sec 1343 http://www.law.cornell.edu/uscode/text/18/1343 (Date of use: 14 December 2012).
257 Sloan http://www.uplink.com.au/lawlibrary/Documents/Docs/Doc121.html (Date of use: 2 December 2012).

acquired property or data will bestow no economic gain on the cybercriminal or inflict some loss to the victim.[258]

However, the ubiquitous nature of cybercrime suggests that the best approach to addressing the menace of cybercrime in the United States should be the main reserve of the federal legislative bodies and enforcement agencies while the states play a supportive role. However, the peculiar jurisprudence of the United States leaves the states playing the primary role in criminal law and enforcement.[259] The United States jurisprudence allocates more power to the states in its enforcement of each state's criminal statute but fails to grasp the extent of the astronomical increase in private interstate cyber-criminal activities.[260]

It is submitted that although the United States has a peculiar criminal jurisprudence, cybercrime should not be lumped into and classified as another genre of criminal activity that must be made subject to this peculiar criminal jurisprudence. Cybercrime legislation and enforcement should be the exclusive preserve of the United States federal authorities. Federal legislation must address all possible cybercriminal activity, relieving the states of the burden of jurisdictional uncertainty, legislation, and enforcement, extradition of a cybercriminal and prosecution of cybercrime.[261] As Chik opined, "seeking a consistent solution at the national level is preferable to sub-national efforts with varying degrees of effectiveness, particularly if the objectives of eliminating or at least reducing computer-related crimes, through deterrence and punishment of offenders, are to be met".[262]

---

258 See *United States v Riggs* 739 F. Supp 414 (ND Ill. 1990) See also *United States v. Schreier* 908 F.2d 645 (10th Cir 1990). See also Sloan http://www.uplink.com.au/lawlibrary/Documents/Docs/Doc121.html (Date of use: 2 December 2012).

259 Chik www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc (Date of use: 10 November 2012).

260 Sloan http://www.uplink.com.au/lawlibrary/Documents/Docs/Doc121.html (Date of use: 10 December 2012).

261 Sloan http://www.uplink.com.au/lawlibrary/Documents/Docs/Doc121.html (Date of use: 10 December 2012).

262 Chik www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc (Date of use: 10 December 2012).

However, it is evident that when the state legislation on cybercrime and federal legislation on cybercrime are put together, the United States of America blazes the trail in enacting relevant laws to address the issue of cybercrime. In addition, the ratification of the Council of Europe Cybercrime Convention and the advent of the Bill to enact the International Cybercrime Reporting Cooperation Act[263] signify the desire and drive to update obsolete cybercrime laws in the United States in line with emerging cybercrime trends.[264]

2.1.2. UNITED KINGDOM

The discovery by United Kingdom courts that the country's existing legislation could not accommodate emerging technological trends led to the enactment of the Computer Misuse Act of 1990.[265] The Act proscribed the "unauthorised access to computer material, unauthorised access with intent to commit or facilitate commission of further offences and unauthorised impairment of computer material".[266] In a bid to keep up with the pace of the technological advancement and to ensure the effectiveness of legislations on cybercrime, the Computer Misuse Act has seen some amendments and some other laws enacted to make modifications to the existing Act.

The UK government, in proposing more expansion and stiffer penalties to the legislation, enacted the Police and Justice Act of 2006.[267] The Act revolves more around police reforms and also made some amendments to the Computer Misuse Act of 1990 by criminalising the denial of service attacks,[268] and the making, obtaining, supplying or

---

263 The Act will ensure that the capacity of foreign countries to combat cybercrime and develop action plans to improve the capacity is reported. See Senate Bill sec 1469 "International Cybercrime Reporting and Cooperation Act" http://beta.congress.gov/bill/112th-congress/senate-bill/1469/text (Date of use: 13 April 2013).

264 Cassim 2009 *Potchefstroom ELJ* 67.

265 In *R v Gold* [1988] 2 WLR 984 the defendant could not be convicted because the existing traditional criminal code did not criminalise the unlawful access to a computer.

266 Computer Misuse Act of the United Kingdom, 1990.

267 Emm D "Cybercrime and the law: A review of UK computer crime legislation" http://www.securelist.com/en/analysis/204792064/Cybercrime_and_the_law_a_review_of_UK_computer_crime_legislation (Date of use: 21 December 2012).

268 Secs 36(1)-(6) Police and Justice Act of United Kingdom, 2006.

offer of the software or materials that could be used to commit a computer crime.[269] The Act further raised the maximum penalty for unauthorised access[270] to a computer from a six months' to two years' prison sentence.[271] Some amendments to the Police and Justice Act were also made in the Serious Crime Act of 2007.[272] The United Kingdom also has the Data Protection Act of 1998,[273] which regulates the procurement, use, disclosure and disposal of private data.[274]

In a bid to strengthen the legislations on cybercrime and curb the use of the internet to perpetrate crime, the Regulation of Investigatory Powers Act (RIPA) was enacted to enable public authorities use covert means where it is necessary, proportionate and compatible with human rights, to obtain private information.[275] This piece of legislation, however, has been criticised as the government's attempt to repressively regulate the internet.[276]

There are a number of other existing legislations that are employed to address various computer-enabled traditional offences.[277] These legislations have had some amendments to bring them up to the present technological advancements.[278]

Computer-enabled fraud is partly regulated by the Theft Act of 1968[279] which has been amended by the Fraud Act of 2006, and it proscribes the offence of fraud by false representation, a failure to disclose information and the abuse of position.[280]

---

269 Secs 37(1)-(5) Police and Justice Act of United Kingdom, 2006.

270 This is the least serious of the offences as provided for under the Computer Misuse Act of United Kingdom, 2006 and also had the least punishment under the said Computer Misuse Act.

271 Secs 35(3)(a)-(c) Police and Justice Act of United Kingdom, 2006.

272 Sec 61 Serious Crime Act of United Kingdom, 2007.

273 The first Data Protection Act was enacted in 1984.

274 Data Protection Act C.29 of United Kingdom, 1998.

275 Regulation of Investigatory Powers Act C.23 of United Kingdom, 2000.

276 Mobbs P "The law on the misuse of computers and networks" http://www.internetrights.org.uk/index.shtml?AA_SL_Session=8fa795873994ed10dd54938b98227a99&x=605 (Date of use: 1 January 2013).

277 Chik www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc (Date of use: 1 January 2013).

278 Chik www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc (Date of use: 1 January 2013).

279 Sec 15 Theft Act C.60 of United Kingdom, 1968.

280 Fraud Act C.35 of United Kingdom, 2006.

Computer-enabled forgeries are also partly regulated by Forgery and Counterfeiting Act of 1981.[281] Computer-based obscenity and pornography are regulated by section 127 of Communications Act of 2003[282] which proscribes the sending of offensive messages and obscene and indecent materials over public electronic communications networks. The Protection of Children Act of 1978[283] proscribes the making, distribution, possession or advertisement of indecent pictures of a child.[284]

Hate messages are prohibited by the Public Order Act[285] which proscribes the use, publication, public performance, distribution or broadcasting of words, behaviour, or written material intended to incite racial hatred. Copyright infringements are prohibited by the Copyright, Designs and Patent of 1988.[286]

2.1.2.1. IDENTIFIED INADEQUACIES OF THE CYBERCRIME LEGISLATION IN THE UNITED KINGDOM

The legislation in the United Kingdom and its amendments illustrate that the UK also is one of the leading countries that ensure that their laws are updated in line with technological advancements.

The Computer Misuse Act, in addressing the pertinent issue of jurisdiction, provides that the UK courts have the jurisdiction to adjudicate, once the offence committed has a significant link with the UK and either the offender or the target computer was in the UK.[287] In further addressing the issue of jurisdiction, the courts held in *R v Smith*

---

281 Forgery and Counterfeiting Act C.45 of United Kingdom, 1981.

282 Sec 127 Communications Act C.21 of United Kingdom, 2003.

283 Sec 1 Protection of Children Act C.37 of United Kingdom, 1978.

284 There have been some amendments to the Protection of Children Act by the Criminal Justice Act C.33 of United Kingdom, 1994.

285 Part III secs 17-28 Public Order Act C.64 of United Kingdom, 1986.

286 Sec 107 Copyright, Designs and Patent Act of United Kingdom, 1988 (as amended by the Copyright and Related Rights Regulations 2003).

287 See secs 4-5 Computer Misuse Act of United Kingdom, 1990. The courts therefore held in *R v Waddon* 6 April 2000 (unreported): "The Court of Appeal held that the content of American websites could come under British jurisdiction when downloaded in the United Kingdom." See http://www.cps.gov.uk/legal/l_to_o/obscene_publications/ (Date of use: 1 January 2013).

(Wallace Duncan) that the offence must have a substantial connection with the UK for the courts to have jurisdiction.[288]

However, various academics believe that the existing legislation addressing cybercrime in the UK is not adequate, and have called for more comprehensive legislation to be enacted.[289] For example, in *R v Bedworth*[290] the jury acquitted the accused because he argued that he had developed an addiction to computer use and, therefore, did not run contrary to the element of intent as prescribed by section 2 of the Computer Misuse Act, since he did not have the requisite intent to commit the offence. Also, in *DPP v Bignell*[291] two officers who used the police national computer to obtain information for their personal use were acquitted on the grounds that their actions did not strictly contravene the element of "unauthorised access" as provided for by section 1 of the Computer Misuse Act, since the information had been obtained by another person under the mistaken belief that the information was for official police business. As observed by Mobbs, the Computer Misuse Act was drafted widely in order to ensure that the law would not become outdated as technology advances, which implies that the Act can sometimes become a "blunt instrument" in the fight against cybercrime.[292]

However, with amendments to some legislations, such as the enactment of the Police and Justice Act which criminalised the denial of service attacks and raised the punishment for unauthorised access from two months to six years, and the amendment of the Theft Act of 1968 by the Fraud Act of 2006, the UK demonstrates that it is tackling the menace of cybercrime squarely.[293]

---

288 *R v Smith (Wallace Duncan)* (No 4) [2004] 3 WLR 229 per Lord Chief Justice Woolf.

289 Pearson C "Problems with the Computer Misuse Act" http://www.ehow.co.uk/list_7373521_problems-computer-misuse-act.html (Date of use: 3 January 2013).

290 *R v Bedworth* (1991); see also Clayton R "UK law and the internet" http://www.cl.cam.ac.uk/~rnc1/notes/EL09_UKLaw.pdf (Date of use: 3 January 2013).

291 *DPP v Bignell* [1998] 1 Cr App R8; see also Computer Misuse Act of United Kingdom, 1990.

292 Mobbs http://www.internetrights.org.uk/index.shtml?AA_SL_Session=8fa795873994ed10dd54938b98227a99&x=605 (Date of use: 3 January 2013).

293 Cassim 2009 *Potchefstroom ELJ* 67.

It is submitted that with concerted efforts by law enforcement bodies, private and public organisations, cybercrime can to a large extent be addressed within the jurisdiction of the UK using the existing legislations, except in cases where other jurisdictions are involved in terms of the object or the subject of the offence.

2.2. LEGISLATIVE RESPONSES OF DEVELOPING NATIONS

2.2.1. NIGERIA

After years of clamour for a comprehensive cybercrime law in Nigeria, a cybercrime Act was eventually enacted in 2015, to provide the legislative framework that will enable the country to tackle cybercrime. The Nigerian Cybercrime Act was enacted after years of drafting, debating and jettisoning other laws meant to prevent cybercrime in and emanating from Nigeria.[294] For example, several Bills, such as the Cyber Security and Data Protection Agency (Establishment) Bill 2008, the Electronic Fraud Prohibition Bill 2008, the Nigeria Computer Security and Protection Agency Bill 2009, the Computer Misuse Bill 2009 and the Economic and Financial Crimes Commission Act (Amendment) Bill 2010 at some point were drafted to address cybercrime but eventually were never passed into law.

The Nigerian Cybercrime Act 2015 criminalised four major aspects of cybercriminal activities, by providing for classes of offences against the state, offences against the confidentiality and integrity of computer systems and data, offences against the person, and also provides for cyber fraud and its related offences. The Act empowers the office of the National Security Adviser to coordinate the enforcement of the provisions of the Act.[295]

---

294 The journey to the final enactment of the Cybercrime Act 2015 started in 2004. See Onalaja G "12 Ways the Nigeria's Cyber crime Act is messed up" http://techcabal.com/2015/10/21/12-ways-nigerias-cyber-crime-act-is-messed-up/ (Date of use: 9 April 2018).

295 Sec 24(1) Cybercrime Act 2015.

In providing for such offences which are against the state, the Act empowered the President of the country under section 3 of the Act to designate some computer systems and networks that are vital to the economy, national security and wellbeing of Nigerian citizens as critical national information infrastructure. The Act criminalised the commission of any offence against the said critical national information infrastructure.[296] The Act under this class of offences in section 17 also proscribed cyber-terrorism. [297]

In protecting the integrity and confidentiality of computer systems and data, the Act criminalised illegal access to computers;[298] the illegal interception of communications;[299] unauthorised modification of computer data or programmes;[300] system interference;[301] and misuse of devices.[302]

The Act further takes steps to protect the person by criminalising identity theft;[303] child pornography;[304] cyber-stalking;[305] racist, gender and xenophobic activities;[306] and cyber-squatting.[307] In criminalising identity theft, section 13 of the Act proscribes

296 Sec 5 Cybercrime Act 2015.

297 The Act prohibits the use of computer systems or network for the purposes of terrorism.

298 Sec 6 Cybercrime Act 2015. Sec 6(1) provides: "Any person, who without authorisation or in excess of authorisation, intentionally accesses in whole or in part, a computer system or network, commits an offence ..."

299 Sec 7 Cybercrime Act 2015. It provides: "Any person, who intentionally and without authorisation or in excess of authority, intercepts by technical means, transmissions of non-public computer data, content data or traffic data, including electromagnetic emissions or signals from a computer, computer system or network carrying or emitting signals, to or from a computer, computer system or connected system or network; commits an offence ...".

300 Sec 8 Cybercrime Act 2015. Sec 8(1) provides: "Any person who directly or indirectly does an act without authority and with intent to cause an unauthorised modification of any data held in any computer system or network, commits an offence ..." Sec 8(2) provides: "Any person who engages in damaging, deletion, deteriorating, alteration, restriction or suppression of data within computer systems or networks, including data transfer from a computer system by any person without authority or in excess of authority, commits an offence ...".

301 Sec 9 Cybercrime Act 2015. It provides that "any person who without authority or in excess of authority, intentionally does an act which causes directly or indirectly the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference in the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose, commits an offence ...".

302 Sec 10 Cybercrime Act, 2015.

303 Sec 13 Cybercrime Act, 2015.

304 Sec 14 Cybercrime Act, 2015.

305 Sec 15 Cybercrime Act, 2015.

306 Sec 18 Cybercrime Act, 2015.

307 Sec 16 Cybercrime Act, 2015.

fraudulently obtaining another person's identity or impersonating another in order to deceive, defraud, gain advantage, obtain property or interest, cause disadvantage to the person being impersonated, avoid arrest or prosecution and obstruct or pervert justice. In criminalising child pornography, section 14(1) of the Cybercrime Act 2015 proscribes the production for distribution, making available or offering, distribution or transmission, procuring for oneself or for another person, possession in a computer or storage medium; of child pornography.[308] Section 14(2) further attempts to protect children by proscribing the use of the information technology system to facilitate the meeting of a child for sexual activities, and recruiting or causing a child to participate in pornographic performances. In criminalising cyber-stalking, section 15(1) of the Cybercrime Act proscribes the use of communication networks to send offensive, indecent or menacing messages which are false and intended to cause annoyance, irritation or anxiety to the recipient. Section 15(2) goes on to proscribe the transmission of messages that induce fear of death or injury, threats to kidnap or demand for ransom, and threats to damage the property or reputation of another. In criminalising racist, gender and xenophobic activities, the Act proscribes the use of a computer network to distribute racist and xenophobic materials publicly, publicly threaten or insult persons for belonging to a group identified by race, descent, colour, religious, national or ethnic origin.[309] Section 18(1)(d) of the Cybercrime Act further criminalises the distribution of materials that deny, approve or justify acts of genocide or crimes against humanity. In prohibiting cyber-squatting, the Act proscribes the unlawful use of the name, trademark, business name, domain name, registered words or phrases owned by corporate bodies, individuals or the government in a manner that interferes with the use by the owner.[310]

Another category of offences the Nigerian Cybercrime Act 2015 seeks to protect against are cyber fraud and related offences. The Act thus criminalises computer-related fraud and computer-related forgery. The Act thus proscribes the unauthorised alteration, deletion or suppression of data with the intention that the altered data be acted upon as

---

308 Under Nigerian laws, a child or minor is anyone below the age of 18 years. See section 14(4) of the Cybercrime Act 2015.

309 Secs 14(1)(a)-(c) Cybercrime Act 2015.

310 Sec 16(1) Cybercrime Act 2015.

genuine, whether the data is intelligible or not.[311] In criminalising cyber fraud, the Nigerian Cybercrime Act prohibits the alteration, erasing, inputting, suppression of computer-held data or the sending of messages that misrepresents facts with the intent to defraud, regardless of whether or not the act confers any economic benefit on the perpetrator.[312]

There are also other relevant laws dealing with some aspects of cybercrime in Nigeria. These laws include the Economic and Financial Crimes Commission (Establishment) Act of 2004; the Nigerian Criminal Code Act of 1916; and the Advance Fee Fraud and Other Related Offences Act of 2006.

The Economic and Financial Crimes Commission (Establishment) Act of 2004 empowers the Economic and Financial Crimes Commission (EFCC) to investigate, prohibit, and prosecute all forms of economic and financial crimes in Nigeria. The Act refers to financial crime as

> "the non-violent criminal and illicit activity committed with the objectives of earning wealth illegally either individually or in a group or organised manner thereby violating existing legislation governing the economic activities of government and its administration and includes any form of fraud, narcotic drug trafficking, money laundering, embezzlement, bribery, looting and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking and child labour, illegal oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and piracy, open market abuse, dumping of toxic wastes and prohibited goods, etc".[313]

The Act thus empowers the Commission to investigate and prosecute financial malpractices; financial crimes relating to terrorism; the retention of proceeds of a

311 Sec 11 Cybercrime Act 2015.
312 Secs 12(1) and (2) Cybercrime Act 2015.
313 Sec 46 Economic and Financial Crimes Commission (Establishment) Act of Nigeria, 2004.

criminal conduct; offences that relate to false information and that relate to economic and financial crimes; and further criminalises these offences.[314] In addition, the Act empowers the Commission to investigate offences that are provided for under other existing laws but within the ambit of economic and financial crimes, for example, offences under the Advance Fee Fraud and Other Related Offences Act of 2006 and Money Laundering Act of 2004.[315] The Act does not criminalise or make direct reference to any form of cybercrime. However, since certain financial activities (such as advance fee fraud) criminalised by the Act can be perpetrated through the internet, it could be argued that the Act addresses certain aspects of cybercrime activities.[316]

The other relevant legislation that seeks to address cybercrime in Nigeria is the Advance Fee Fraud and Other Related Offences Act of 2006 which is an offshoot of section 419 of the Nigerian Criminal Code Act of 1916. The Act makes direct reference to the internet and cybercrime. The Act criminalises fraud by making it an offence to obtain property or a benefit, whether in Nigeria or outside Nigeria, by false pretences and with the intent to defraud.[317] In a bid to further protect foreigners from fraudulent representations originating from Nigeria and sent to recipients outside the shores of Nigeria, section 4 of the Act prohibits inviting any person to Nigeria by inducement with the intent to defraud the person or any other person through false pretences.

In order to address the issue of cybercrime, the Act goes a step further by providing for the regulation of internet service providers and internet cafes, and requires such providers to register with the Economic and Financial Crime Commission.[318] The law, therefore, vests the duty of surveillance not only on the government or the Economic and Financial Crime Commission, but also on industry players to ensure that their facilities are not used to commit internet fraud.[319] This will compel internet cafes and internet service providers to keep a record of transactions of users and to monitor the

314 Secs 14-18 Economic and Financial Crimes Commission (Establishment) Act of Nigeria, 2004.
315 Sec 7 Economic and Financial Crimes Commission (Establishment) Act of Nigeria, 2004.
316 Oriola TA "Advance fee fraud on the internet: Nigeria's regulatory response" 2005 *Computer Law and Security Report* 237-248.
317 Sec 1 Advance Fee Fraud and Other Fraud Related Offences Act of Nigeria, 2006.
318 Sec 13(1) Advance Fee Fraud and Other Fraud Related Offences Act of Nigeria, 2006.
319 Sec 13(3) Advance Fee Fraud and Other Fraud Related Offences Act of Nigeria, 2006.

use of their systems against illegal transactions.[320] However, it is submitted that this amounts to a breach of privacy. Although this Act addresses an aspect of cybercrime, it does not address the broad range of cybercriminal activities.[321]

Another relevant legislation on cybercrime is the Criminal Code Act which does not make any reference to cybercrime but is used as a traditional legislation to combat a modern form of crime. The enactment of the Criminal Code Act predates the internet era and, therefore, does not make direct reference to any form of cybercrime or even internet scam.[322] The Act prohibits any type of theft of funds and property in any form and manner.[323] Section 419 of the Criminal Code prohibits advance fee fraud, which is a major feature on the Nigerian cybercrime scene, consisting of the sending of bogus e-mails and messages to victims under the false pretence that the victim will acquire some non-existent benefit. Section 419 of the Act provides 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 person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years".[324] The Advance Fee Fraud and Other Related Offences Act of 2006 is an enlarged adaptation of section 419 of the Nigerian Criminal Code.

2.2.1.1. IDENTIFIED INADEQUACIES OF THE NIGERIAN LEGISLATIVE RESPONSE

The Nigerian legislature has followed the example of most developed nations to enact the Nigerian Cybercrime Act of 2015 which addresses a wide range of cyber-criminal activities. It is agreed that the Act is highly punitive which is well suited for the Nigerian environment considering the growing menace of cybercrime emanating from the

320 Chawki M "Nigeria tackles advance fee fraud" (2009) *Journal Information Law and Technology* 1-20.

321 Ewelukwa N "Non-passage of cybercrime bill decried" http://www.thisdaylive.com/articles/non-passage-of- cyber-crime-bill-decried/88750/ (Date of use: 8 January 2013).

322 The Nigerian Criminal Code was first enacted in 1916.

323 Wada F and Odulaja GO "Assessing cybercrime and its impact on e-banking in Nigeria using social theories" (2012) *African Journal of Computer and ICT* 69-82.

324 Sec 419 Nigerian Criminal Code Act of Nigeria (Laws of the Federation) 1990.

country.[325] The Act, however, has been identified as "structurally deficient".[326] For example, the Act empowers the National Security Adviser to superintend over the Act through an advisory council and, yet, the National Security Adviser is not a member of the said advisory council.[327] The Act proceeded to make extraneous provisions that have no bearing on the main spirit behind the legislative intervention. For example, the Act places a levy of 0.005 percent of all electronic transactions by GSM, telecommunication and internet service providers, insurance companies, banks and other financial institutions, and the Nigerian stock exchange.[328] This creates extra costs for these businesses and the burden of this levy will eventually be transferred to the final consumers by these businesses/institutions. The Act further makes it mandatory for cybercafe operators to register their businesses with the Computer Professionals Registration Council of Nigeria (CPN), yet it provides no sanction for a refusal to register.[329] The irrelevance of this provision is further exacerbated by the fact that cybercafes are being phased out and most internet users in Nigeria rely on their internet-enabled devices.[330]

Pundits also criticised the Act as being incomprehensive, drafted without the input of most telecommunication companies/stakeholders and that its enforcement mechanisms are set in such a manner as to show a conspiracy that ensures that Nigeria does not enforce cybercrime.[331] On the other hand, the National Security Adviser (throughout Nigerian history having been appointed from the military)[332] is saddled with

---

325 Ilori T "The Nigerian Cybercrimes Act 2015: Is it uhuru yet?" http://www.lawyard.ng/the-nigerian-cybercrimes-act-2015-is-it-uhuru-yet-by-tomiwa-ilori/ (Date of use: 17 May 2018) For example, the punishment for misuse of device, forgery and fraud is three years' imprisonment or an option of a fine of seven million Naira or both.

326 Ogunseinde T "Analysis: Nigeria Cybercrimes Act 2015: What are the issues?" http://technologytimes.ng/analysis-nigeria-cybercrimes-act-2015-issues/ (Date of use: 16 May 2018).

327 Ogunseinde http://technologytimes.ng/analysis-nigeria-cybercrimes-act-2015-issues/ (Date of use: 16 May 2018).

328 Sec 44(2)(a) and the second schedule to the Cybercrime Act.

329 Sec 7 of the Nigerian Cybercrime Act.

330 Ndiomewese I "A tribute to cybercafes and their undeniable role in Nigeria's internet revolution" https://techpoint.ng/2015/12/16/cybercafes-in-nigeria-memoirs/ (Date of use: 17 May 2018).

331 Ogunseinde http://technologytimes.ng/analysis-nigeria-cybercrimes-act-2015-issues/ (Date of use: 16 May 2018).

332 Alex R "List of national security advisers since 1999" https://www.nigerianbulletin.com/threads/list-of-national-security-advisers-since-1999.149490/ (Date of use: 19 May 2018).

coordinating the enforcement of the Act.[333] A coordinating authority should rather be one versed in policing and investigation and not military combat, and in the peculiar case of cybercrime, be versed in same. The Act, however, does not give the responsibility of the enforcement of the Act to any law enforcement agency.[334]

A major lacuna in the Criminal Code Act and the Advance Fee Fraud and Other Related Offences Act is the prohibition of the offence of obtaining by false pretence.[335] The Act makes reference to tangible property being obtained and deprived by the victim of the scam,[336] but intangible property such as information may also be the target of the offender. However, it is submitted that the courts may interpret the current section 1 of the Advance Fee Fraud and Other Related Offences Act as covering every form of benefit, whether intangible or not.

The Criminal Code Act, for its part, provides that the person committing the offence cannot be arrested without a warrant unless he was found committing the offence.[337] As pointed out by Chawki, this does not reflect the understanding that the crime is perpetrated in cyberspace, and an offender will rarely be caught in the act until the act has been completed.[338] Chawki also points out that since most advance fee fraud representations made to the victim entail that the victim participates in an illegal act in order to receive the benefit, the victim may find it difficult to recover his money since the victim had wanted to participate in an illegal venture, and the court cannot enforce illegality.[339]

---

333 Sec 41(1) Cybercrime Act 2015.

334 Sec 47 Cybercrime Act 2015.

335 Obtaining by false pretence refers to the acquisition of property from another by intentionally misrepresenting an existing or past fact. See LaMance K "What is the crime of false pretenses?" http://www.legalmatch.com/law-library/article/false-pretenses.html (Date of use: 19 October 2014).

336 Ani L "Cyber crime and national security: The role of the penal and procedural law" in Azinge E and Bello F *Law and security in Nigeria* (NIALS Press 2011) 197-234.

337 Sec 419 Nigerian Criminal Code Act.

338 Chawki *Journal ILT* 8.

339 Chawki *Journal ILT* 8.

2.2.2. INDIA

The relevant legislation on cybercrime in India is the Information Technology Act 2000 (as amended in 2008). The Act covers a wide range of issues that would help to address the dangers of cybercrime in India. The essential aim of the Act is to validate and legalise electronic and on-line transactions and create an enabling environment for its use, and then to criminalise activities that will affect the effective operation of these electronic transactions.[340] The Act provides for the creation of the Cyber Appellate Tribunal, which demonstrates the government's intention to address cybercrime by prioritising and speedily dispensing with cybercrime cases.[341]

The Act provides for the legal recognition of electronic documents; the legal recognition of digital signatures; cybercrime offences and punishments; investigation; and the adjudication and justice dispensation system.[342] The Act criminalises the unlawful alteration of computer source codes or programmes, hacking or the unlawful alteration of information in a computer system and the publication or transmission of obscene or pornographic materials.[343] The Act also empowers the controller to issue directives to guarantee that the provisions of the Act are complied with, and it is an offence not to comply with the directive.[344] The Act also makes it an offence to refuse to assist a government agency in intercepting information that will enable the government to protect state sovereignty and security.[345] Furthermore, the Act criminalises any unlawful access or attempt to access any protected system.[346]

In a bid to have updated legislation on cybercrime as a result of some apparent lacuna in the Information Technology Act of 2000, the government in 2008 brought about an

340 Shah S "The Information Technology Act 2000: A legal framework for e-governance" http://www.sudhirlaw.com/cyberlaw-itact.htm (Date of use: 11 January 2013).
341 Secs 48-56 Information Technology Act of India, 2000.
342 Information Technology Act of India, 2000.
343 Secs 65-67 Information Technology Act of India, 2000.
344 Sec 68 Information Technology Act of India, 2000.
345 Sec 69 Information Technology Act of India, 2000.
346 Protected systems refers to any computer, computer system or computer network declared by the government to be a protected system. See sec 70 of the Information Technology Act of India, 2000.

amendment to the Act. The 2008 amendment to the Information Technology Act expanded and modified section 66 of the 2000 Act which deals with hacking and, thus, criminalised the transmission of offensive, threatening or annoying messages with the aid of the computer system.[347] The amendment also prohibits the receipt of stolen computer resources or electronic devices by an offender who is aware of the fact that the device has been stolen; identity theft; cheating by impersonation with the aid of the computer system; and the unlawful recording, publication or transmission of an individual's nudity.[348] The amendment further proscribes cyber-terrorism.[349]

Section 67 of the 2000 Act deals with the publication of obscene materials and, in a bid to stamp out online pornography, further prohibits the publication and transmission of pornographic materials and child pornographic materials.[350]

2.2.2.1. IDENTIFIED INADEQUACIES OF THE INDIAN LEGISLATIVE RESPONSE

The Information Technology Act 2000 and its amendments reveal that the Indian government is taking decisive steps in addressing the perils of cybercrime through its legislative initiative. A few lacunae in the existing legislation are highlighted.

Section 66(a), which address the transmission of offensive messages, has been criticised as an infringement of the fundamental right to free speech.[351] It has also been criticised as being too broad, and that the mere fact that a false message causes "annoyance" or "inconvenience" is not sufficient to infringe upon an individual's freedom of speech unless such false message directly impinges on decency, morality, public

347 Sec 32 Information Technology Amendment Act of India, 2008.
348 Sec 32 Information Technology Amendment Act of India, 2008.
349 Sec 66F Information Technology Amendment Act of India, 2008.
350 Sec 66F Information Technology Amendment Act of India, 2008.
351 A high court has been asked to declare sec 66(a) *ultra vires* and a violation of the constitutional right to freedom of expression. See http://www.thehindu.com/news/states/tamil-nadu/validity-of-section-66a-of-it-act-challenged/article4116598.ece (Date of use: 12 January 2013).

order or defamation.[352] According to Cushing, "loosely-worded laws, ostensibly designed to "protect" citizens, usually devolve into tools of censorship".[353]

In addition, section 69 of the ITAA has been criticised as an infringement of an individual's right to privacy and personal liberty since the law allows government agencies to decrypt and intercept private messages. The 2008 amendment further widens the scope by allowing the monitoring of personal information and computer systems without a warrant from a magistrate or judge.[354]

2.2.3. SOUTH AFRICA

The common law of South Africa deals with traditional crimes. Its provisions could be widened to accommodate and address certain aspects of emerging cyber-criminal activities.[355] For example, in *Nissan v Marnitz NO & Others*[356] the Court held that money transferred electronically and received by an individual who is aware that he is not entitled to the money and yet uses the money has committed theft. Therefore, traditional crimes that are recognised by common law statutes can be used to address the issues of cyber-defamation, indecency, child pornography, cyber-smearing and cyber-fraud.[357] For example, sections 27 and 28 of the Films and Publications Act of 1996 prohibit the creation, production, importation or possession of child pornographic materials.[358] Nevertheless, when dealing with the cybercriminal activities relating to phishing, spamming, treason, murder, assault, theft and extortion, the common law statutes become limited and ineffective.[359]

---

352 Prakash P "Short note on IT Amendment Act, 2008" http://cis-india.org/internet-governance/publications/it-act/short-note-on-amendment-act-2008 (Date of use: 12 January 2013).

353 Cushing T "Abuse of India's Information Technology Act results in India's first arrested Twitter user" http://www.techdirt.com/articles/20121106/16174720954/abuse-indias-information-technology-act-results-indias-first-arrested-twitter-user.shtml (Date of use: 14 March 2013).

354 http://www.sacw.net/article606.html (Date of use: 12 January 2013).

355 Snail S "Cyber crime in South Africa – Hacking, cracking, and other unlawful online activities" (2009) *Journal of Information Law and Technology* 1-13.

356 *Nissan v Marnitz NO & Others* 2005 (1) SA 441 (SCA).

357 Snail *Cyber crime* 2009 *Journal ILT* 2.

358 Films and Publications Act, Act. No. 65 of South Africa, 1996.

359 Snail *Cyber crime* 2009 *Journal ILT 3*.

However, the application of the common law to modern cyber-criminal activities is regarded by the courts as an academic exercise, which has caused much uncertainty in the outcome of criminal prosecutions.[360] The courts and criminal prosecutors, therefore, were wary of embarking on such uncertain prosecutions, and this has led to much criticism of the adequacy of the existing laws to address cybercrime.[361] The decision in *S v Mashiyi*[362] reinforced the decision in *Narlis v South African Bank of Athens*,[363] and held that a computer-generated document was inadmissible. This case of *S v Mashiyi* illustrated that the existing traditional laws were not adequate in addressing emerging modern crimes.

As a result of the uncertainties that accompany the common law in addressing cybercrime, the Electronic Communications and Transactions Act 25 of 2002 (ECT Act) was enacted to comprehensively deal with cybercrime.[364] The ECT Act seeks to "enable and facilitate electronic communications and transactions in the public interest".[365] The ECT Act does not exclude any common law or statutory provision relating to electronic transactions from being applied.[366] Chapter XIII of the ECT Act criminalises several cybercrime offences. The Act prohibits the unauthorised access to or interception of data.[367] It also criminalises the unlawful modification or destruction of data.[368] Section 86(3) of the Act introduces a new form of crime known as the "anti-cracking and hacking law".[369] The section prohibits the production, sale, designing or distribution of any computer programme or any security circumventing device,[370] while section 86(4)

360 Snail *Cyber crime* 2009 *Journal ILT* 3.
361 Snail *Cyber crime* 2009 *Journal ILT* 3.
362 *S v Mashiyi* 2002 (2) SACR 387. However, in *S v Harper* 1981 (1) SA 88 it was held that if the computer merely stored or recorded the information, the documents will be admissible. See also Snail *Cyber crime* 2009 *Journal ILT* 2.
363 *Narlis v South African Bank of Athens* 1976 (2) SA 573. The Court reasoned that the computer was not a person and could not make a statement, therefore a computer print-out was inadmissible in civil proceedings. See also Snail *JILT* 2.
364 Snail *Cyber crime* 2009 *Journal ILT* 2.
365 Sec 2 Electronic Communications and Transactions Act of South Africa, 2002.
366 Sec 3 ECT Act.
367 Sec 86(1) ECT Act.
368 Sec 86(2) ECT Act.
369 http://www.hg.org/article.asp?id=5351 (Date of use: 20 January 2013).
370 http://www.hg.org/article.asp?id=5351 (Date of use: 20 January 2013).

prohibits the use of such device. The ECT Act also criminalises denial of service attacks in section 86(5). It further criminalises computer-related extortion, forgery and fraud.[371] Spamming is prohibited in section 45 of the Act by criminalising the sending of unsolicited commercial communication to consumers.

In order to facilitate the enforcement of the provisions of the ECT Act and to enable the investigation of incidents of cyber-criminal activities, the ECT Act provides for cyber-inspectors who, authorised by a warrant, are empowered to access and inspect a computer system suspected of being used in the commission of an offence.[372]

The ECT Act also addresses the issue of jurisdiction. Section 90 of the Act prescribes circumstances where South African courts can assume jurisdiction over a cyber-criminal activity. The circumstances include instances where the offence itself was perpetrated in South Africa; where a component of the offence or preparation for the offence was perpetrated in South Africa or the outcome of the offence has an effect in South Africa; where the criminal act was perpetrated by a South African citizen, permanent resident or an individual carrying on business in South Africa; or where the offence was perpetrated on board a ship or aircraft registered in South Africa or a voyage or flight departing South Africa at the time the offence was perpetrated.[373] It is submitted that the provisions of section 90 of the ECT Act are wide enough to cover most situations where the cyber-criminal activity will affect South Africa or its residents and also protect foreign nationals from cyber-criminal activities emanating from South Africa.

As a result of the provision by section 3 of the ECT Act, which allows other statutory or common law to be relied upon in addressing cybercrime, cybercrime is not limited to the Electronic Communications and Transactions Act 2002. Such other legislations which seek to address certain aspects of cybercrime include the Prevention of Organised Crime Act 1998, which deals with various forms of organised crime, criminal gang activities and money laundering that are computer-enabled or committed in cyber

371 Sec 87 Electronic Communications and Transactions Act, of South Africa, 2002.
372 Secs 80-83 ECT Act.
373 Sec 90 Electronic Communications and Transactions Act, of South Africa 2002.

space.[374] The Financial Intelligence Centre Act 2001 (FICA) was also enacted to provide for the establishment and regulation of a financial intelligence centre to assist in addressing money laundering and identifying the proceeds of unlawful activities.[375] The FICA also prohibits the proceeds of unlawful activities and money-laundering activities in line with the Prevention of Organised Crime Act.[376]

Unlicensed gambling, which includes unlicensed online gambling, is criminalised by the National Gambling Act,[377] and unlicensed lottery is made unlawful by the Lotteries Act 1997[378] which can also be computer-enabled. Computer-related copyright infringement can be dealt with by section 27 of the Copyright Act 1978 which prohibits the unauthorised copying, sale or distribution of copyrighted materials.[379]

The Regulation of Interception of Communications and Provision of Communication Related Information Act (RICPCRIA) of 2002 prohibits the unlawful interception of any communication in the course of its transmission or occurrence.[380] The Interception and Monitoring Prohibition Act of 1992 also prohibits such interception of communication which will include computer communications.[381] Again, the Criminal Law (Sexual Offences and Related Matters) Amendment Act prohibits various forms of child pornography and the possession and distribution of child pornography.[382]

In order to facilitate the admissibility of information in electronic format, the ECT Act provides that the rules of evidence must not be employed to deny due evidential weight or render inadmissible electronic data messages on the grounds that the message is a

374 Prevention of Organised Crime Act of South Africa, 1998.
375 Sec 3 Financial Intelligence Centre Act of South Africa, 2001.
376 https://www.fic.gov.za/SiteContent/ContentPage.aspx?id=1 (Date of use: 20 January 2013).
377 Sec 89 National Gambling Act of South Africa, 2004.
378 Secs 57-59 Lotteries Act of South Africa, 1997.
379 Copyright Act of South Africa, 1978.
380 This would include interception of e-mails and computer messages. See sec 2 Regulation of Interception of Communications and Provision of Communication Related Information Act (RICPCRIA) of South Africa, 2002.
381 Sec 2 Interception and Monitoring Prohibition Act 127 of South Africa, 1992.
382 Secs 17-20 Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of South Africa, 2007 (as amended by the Judicial Matters Amendment Act 66 of 2008).

data message or that it is not in its original form.[383] This provision lays to rest the traditional requirement of the Evidence Act that for documentary evidence to be admissible, amongst other requirements of law, the original documents must be what will be tendered in evidence.[384] According to Cassim,[385] the provisions of section 15 of the ECT Act form a rebuttable presumption of law that data messages and computer print-outs are admissible in law.

Regardless of the existing South African legislative responses on cybercrime, the South African parliament is taking steps to enact a South African Cybercrime Act to consolidate the existing cybercrime offences and create new offences to further strengthen the legislative response to cybercrime by closing up the lacunae prevalent in the existing legislative responses.[386] The Cybercrime Bill which was introduced in 2015 has gone through various legislative processes and is expected to be passed into law by the end of the year 2019. The Cybercrime Bill when passed into law is intended to repeal the relevant sections of the ECT Act that deal with cybercriminal offences.[387]

According to the long title, the Bill intends to "create offences which have a bearing on cybercrime; to criminalise the distribution of data messages which are harmful and to provide for interim protection orders; to further regulate jurisdiction in respect of cybercrimes; to further regulate the powers to investigate cybercrimes; to further regulate aspects relating to mutual assistance in respect of the investigation of cybercrime; to provide for the establishment of a designated Point of Contact; to further provide for the proof of certain facts by affidavit; to impose obligations to report cybercrimes; to provide for capacity building; to provide that the Executive may enter into agreements with foreign States to promote measures aimed at the detection,

383 Sec 15 Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of South Africa 2007.

384 The other requirements of law are that the evidence has to be relevant and admissible; its authenticity has to be proved; and the original document must be produced. See Cassim 2009 *Potchefstroom ELJ* 118-123.

385 Cassim 2009 *Potchefstroom ELJ* 119.

386 Ameer-Mia F and Pienaar C "South Africa: Cybersecurity 2019" https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/south-africa (Date of use: 18 September 2019).

387 Ameer-Mia and Pienaar https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/south-africa (Date of use: 18 September 2019).

prevention, mitigation and investigation of cybercrimes; to delete and amend provisions of certain laws; and to provide for matters connected therewith."[388]

Part I of the said Bill (sections 2-11) seeks to protect the confidentiality and integrity of computer systems and data, and also prohibit cyber fraud and its related offences. Thus the Bill intends to prohibit unlawful intentional access to computer systems, data and programs.[389] It also intends to criminalise the unauthorised interception of data.[390] Section 4 of the Bill seeks to proscribe the unauthorised possession or use of any software or hardware tools in perpetrating the offences criminalised under the Bill.[391] The Bill also outlaws the unauthorised interference with data or computer program but dwells on the deletion, alteration, modification, denial of access to data.[392] Again, the Bill prohibits unauthorised intentional interference of computer storage medium through the alteration, interruption or impairment of the functioning, confidentiality, integrity or availability of the computer storage system.[393] Section 7 of the Bill seeks to prohibit unauthorised procurement, possession, provision, receipt or use of password, access code while section 8 proscribes cyber fraud. Section 8 also proscribes cyber forgery and further creates the offence of cyber uttering which criminalises the passing off of false data or computer program with the intent to defraud, which prejudices or can prejudice another individual.

Part II of the Bill seeks to prohibit various forms of malicious communications. The Bill thus seeks to prohibit the communication of data messages which incites violence or damage to property and/or which threatens individuals with violence or damage to property.[394] This section of the Bill also proscribes the broadcast or distribution of an individual's intimate image without the individual's consent.[395]

---

388 See the long title of the South African Cybercrime Bill.
389 Sec 2 of the South African Cybercrime Bill.
390 Sec 3 of the South African Cybercrime Bill.
391 The tools will be for the purposes of unlawful access and intereference with data, computer, computer systems and computer programs. See Sec 4(2) of the South African Cybercrime Bill.
392 Sec 5 of the South African Cybercrime Bill.
393 Sec 6 of the South African Cybercrime Bill.
394 Secs 14 and 15 of the South African Cybercrime Bill.
395 Sec 16 of the South African Cybercrime Bill. The said image may be real or simulated.

The South African Cybercrime Bill when passed into law, through its section 20, seeks to protect a complainant by granting powers to a magistrate to restrain persons who have embarked on activities contemplated under sections 14-16[396] of the Bill, from further doing so pending the completion of the investigation of such complaints by the South African Police Service (SAPS).[397]

The South African Cybercrime Bill which is intended to repeal relevant sections of the ECT Act also seeks to address the issue of jurisdiction. Section 24 of the Bill in providing for the circumstances where a Court in South Africa can assume jurisdiction, further broadens and increases the circumstances created by section 90 of the ECT Act. It prescribes that the South African courts can assume jurisdiction over a cyber-criminal activity, where the offence itself was perpetrated in South Africa or aboard a vessel, aircraft, ship, off-shore installation or fixed platform that is registered or required to be registered in South Africa.[398] The Court will also have jurisdiction where the offence was committed against a company, citizen or ordinary resident of South Africa.[399] The Bill seeks to protect South Africans from the failure of countries that are complacent about updating their cybercrime legislations by giving the South African court jurisdiction in circumstances were the offending activity is committed outside South Africa but the offender is a citizen or resident of South Africa or was arrested within South Africa or is a company registered in South Africa.[400] The South African court can assume jurisdiction whether or not the offending activity is a crime where it was committed.[401]

---

396 Sec 14-16 of the South Afrcian Cybercrime Bill relates to malicious communication of data messages that incite or threatens violence or damage to property, and also broadcast or distribution of an individual's intimate image with the individual's consent.

397 Sec 20 of the South African Cybercrime Bill provides that "A complainant who lays a charge with the South African Police Service that an offence contemplated in section 14, 15 or 16 has allegedly been committed against him or her, may on an ex parte basis in the prescribed form and manner, apply to a magistrate's court for an order pending the finalisation of the criminal proceedings to— (a) prohibit any person from further making available, broadcasting or distributing the data message contemplated in section 14, 15 or 16 which relates to the charge; or (b) order an electronic communications service provider or person in control of a computer system to remove or disable access to the data message in question".

398 Sec 24 (1) (a) of the South African Cybercrime Bill.

399 Sec 24 (1) (b) of the South African Cybercrime Bill.

400 Sec 24 (2) of the South African Cybercrime Bill.

401 Sec 24 (2) of the South African Cybercrime Bill.

In facilitating the enforcement of the provisions of the intended Cybercrime Act, the Bill intends to empower the South African Police Service and authorised investigators[402] to investigate, search, access, and seize computers, data, data storage mediums, network, printout, program, suspected of being used in the commission of an offence, provided that they are armed with a search warrant.[403] The Bill however, will allow a Police officer to search, access or seize without a search warrant where the person with the lawful authority over the article consents to the search or seizure, or where the Police officer reasonably believes that a search warrant will be issued if same is applied for and that delay in procuring the search warrant will defeat the purpose of the search or seizure.[404] The Bill stipulates several steps that enables the provision of an effective mutual assistance to foreign authorities over cybercriminal activities emanating from South Africa,[405] and further mandates the National commissioner to establish a designated point of contact within the South African Police Service (SAPS) that will ensure the immediate provision of assistance in the investigations of offences proscribed by the Bill.[406]

2.2.3.1. IDENTIFIED INADEQUACIES OF THE SOUTH AFRICAN LEGISLATIVE RESPONSE

The ECT Act has brought about remarkable positive changes in the legislative approach to addressing cybercrime in South Africa. However, the sanctions attached to the offences have been criticised as being inadequate,[407] and therefore may not generate the desired effect of deterring cyber-criminals from their nefarious activities. For example, the penalty for computer-related fraud is imprisonment of a maximum of five

---

402 An investigator is a non-member of the South African Police Service (SAPS), who is authorised by a search warrant or requested by a police officer to assist in the search, access or seizure of an article used in committing an offence proscribed by the Act. See Sec 25 of the South African Cybercrime Bill.

403 Secs 25-30 of the South African Cybercrime Bill.

404 Secs 31 and 32 of the South African Cybercrime Bill.

405 Secs 46 – 51 of the South African Cybercrime Bill.

406 Sec 52 of the South African Cybercrime Bill.

407 Cassim 2009 *Potchefstroom ELJ* 119.

years or the payment of fine,[408] while in the United Kingdom the penalty is 10 years' imprisonment or the payment of fine or both.[409] The South African Cybercrime Bill which seeks to repeal relevant sections of the ECT Act has not solved the issue since the punishment which will be attached to a number of the offences are still inadequate or even without a definite penalty leaving the duration or gravity of the punishment for the courts to decide. For example under the ECT Act, cyber-fraud has a penalty of five years imprisonment or payment of fine but the South African Cybercrime Bill does not stipulate a definite penalty but allows the court to impose a penalty within the court's jurisdiction that the court considers appropriate in line with Section 276 of the South African Criminal Procedure Act.[410] Malicious communication that incites violence, threaten to damage property and distribute intimate images only elicit a fine or maximum of three years imprisonment which is inadequate.[411]

The search and seizure authority given to cyber inspectors under the ECT Act, has been criticised as opening the door to a breach of an individual's inalienable right to privacy and property.[412] However, it is submitted that since the enactment of the Constitution, which provides for the right to privacy and property and also provides for circumstances in which the right can lawfully be infringed upon, the activities of cyber inspectors, once they are performed within the ambits of the law, would no longer amount to a derogation of an individual's fundamental rights.[413]

The Cybercrime Bill which seeks to repeal relevant sections of the ECT Act, provides a detailed expression of the offences which it seeks to criminalise, in order to take care of all manner of circumstances that may arise. For example, the Bill broadly defines hacking[414] and elaborately dedicates sections 3 – 6 of the Bill in proscribing unauthorised interference and/or interception of data, computer, computer program, and

---

408 Sec 89 ECT Act.
409 Sec 1(3)(b) Fraud Act C.35 of United Kingdom, 2006.
410 Sec 19 (4) of the South African Cybercrime Bill.
411 Sec 19 (7) of the South African Cybercrime Bill
412 Cassim 2009 *Potchefstroom ELJ* 119.
413 See sec 36 Constitution of the Republic of South Africa, 1996.
414 Sec 2 of the South African Cybercrime Bill.

computer storage medium.[415] The Bill also creates some new offences like adding cyber uttering to the already existing offence of cyber forgery.[416] Unfortunately, the makers of the South African Cybercrime Bill did not consolidate all known cyber-criminal activities into this single legislation. For example, computer-related copyright infringement was not dealt with by the Bill, and while section 16 of the Bill which deals with intimate pictures can be relied upon in prosecuting child pornography, it would have been more desirable that a section of the Bill is dedicated to child pornography with more stringent penalty attached to its violation.[417] This is so because, section 16 of the Bill revolves around the distribution of the intimate pictures of an individual without the individual's consent, meanwhile consent should not be a consideration when a child is involved. Also, most sections of the Bill that criminalised certain cyber activities were so elaborate and repetitive. According to Emma-Iwuoha the Bill is "trying to catch everything but not doing it in a correct and informed way".[418]

It must however be pointed out, that the main forms of cybercriminal activities were dealt with by the said South African Cybercrime Bill. Emma-Iwuoha pointed out that the use of broad definitions employed in criminalising the offences leaves innocent persons susceptible to falling foul of the provisions of the Bill.[419] For example, the mere possession of devices or tools that can be used to gain access or interfere with a computer system or network, comes with a penalty.[420] Thus penetration testers or ethical hackers who test computer systems to detect the vulnerability of the computer system, would run afoul of section 7 of the Bill even though the tools are used in

---

415 These sections will take care of the offences criminalised by the Regulation of Interception of Communications and Provision of Communication Related Information Act (RICPCRIA) of 2002 and the Interception and Monitoring Prohibition Act of 1992, which had proscribed the unlawful interception of any communication in the course of its transmission or occurrence.

416 Cyber uttering by sec 9 of the Bill relates to the passing off of computer program or data with the intent to defraud another.

417 Sec 16 (1) of the Bill provides thus "Any person (''A'') who unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message of an intimate image of a person (''B'') without the consent of B, is guilty of an offence".

418 Chapman C "South Africa welcomes new cybercrime legislation" https://portswigger.net/daily-swig/south-africa-welcomes-new-cybercrime-legislation (Date of use: 5 October 2019).

419 Chapman https://portswigger.net/daily-swig/south-africa-welcomes-new-cybercrime-legislation (Date of use: 5 October 2019).

420 Sec 7 of the South African Cybercrime Bill.

performing their lawful jobs, and then the onus of proving their innocence will shift to the accused.[421]

The Norwegian Institute of International Affairs (NUPI) stated that the emergence of the South African Cybercrime Act will empower the South African Police Services (SAPS) to effectively fight cybercrime while cybercrime specialists will be authorised to effectively track prohibited cyber activities, since the existing ECT Act and RICA have left South Africa vulnerable to cyber-attacks.[422] They however, pointed out that given the absence of adequate cybercrime skills development training, the capability of the South African Police Service is in doubt.[423]

2.3. LAW ENFORCEMENT INITIATIVES IN RESPONSE TO CYBERCRIME IN DEVELOPED NATIONS

The second strategy/element, as pointed out earlier, which is essential in effectively addressing the issue of cybercrime, is the capacity of law enforcement bodies to prevent, investigate and prosecute cyber-criminals. This refers to the law enforcement mechanisms put in place by the law enforcement bodies of the various nations.

The training of law enforcement and judicial bodies that deal with cyber-criminal activities must be adequate and frequently updated to keep up with the pace of technological advancement. As the rate of cybercrime increases, the need to hire and train new personnel also increases in order to keep up with the exponential increase in cyber-criminal activities. For example, according to the Indian Crime Investigation Department, an increase in cybercriminal cases was registered in Andhra Pradesh from

---

421 Chapman https://portswigger.net/daily-swig/south-africa-welcomes-new-cybercrime-legislation (Date of use: 5 October 2019).

422 Van Der Westhuizen H “New Bill offers robust game plan against cybercrime in South Africa” https://saiia.org.za/research/new-bill-offers-robust-game-plan-against-cybercrime-in-south-africa/ (Date of use: 4 October 2019).

423 Van Der Westhuizen https://saiia.org.za/research/new-bill-offers-robust-game-plan-against-cybercrime-in-south-africa/ (Date of use: 4 October 2019).

380 cases in 2011 to approximately 500 cases in 2012, while only about 197 cases were reported in 2010.[424]

Another essential aspect of capacity building for law enforcement agencies is the adequate funding of these bodies so as to properly equip them with the right training and equipment in order to properly investigate, prosecute and prevent the cybercrime.

Gonzalez points out that the two main roles of law enforcement agencies/police in combating cybercrime are the prevention of cybercrime activities before they occur or limiting the scope of their operation through the dissemination of warnings about threats in order for individuals to protect themselves, and responding to a crime that has taken place through proper investigation and identification of the perpetrators.[425]

In order to properly analyse the law enforcement initiatives, it is pertinent to also examine certain factors that will enhance the effectiveness of these bodies. These will include the staff strength, technological resources, funding and training/education of the personnel involved in the combat.

However, it should be pointed out that some of the law enforcement initiatives are not government-established but may be forums established to assist the government-established law enforcement bodies to properly execute their functions. This portion of the thesis, in highlighting the efforts of various law enforcement bodies to combat electronic crime, will analyse only the leading law enforcement bodies of the countries being compared, using the information in the public realm to perform the analysis.

The essence of this section of the research is not to go into a detailed analysis of the *modus operandi* of each law enforcement body, but to show the level of commitment and extent to which some countries have gone and are prepared to go in the bid to

---

424 http://www.ndtv.com/article/south/hands-on-training-to-andhra-pradesh-police-officers-to-probe-cyber-crimes-318057 (Date of use: 5 February 2013).

425 http://www.gpo.gov/fdsys/pkg/CHRG-106shrg69335/html/CHRG-106shrg69335.htm (Date of use: 5 February 2013).

combat cybercrime, and to compare same with countries that are lagging behind in the fight against cybercrime. It must be noted that normally there is limited information on current strategies, the amount of funding and the number of law enforcement agents employed by various governments in tackling crime in order not to equip the criminals with privileged information that will help them elude law enforcement agents. This part of the research will focus on the leading law enforcement bodies of the countries being examined.

2.3.1 UNITED KINGDOM

The UK Parliamentary Office of Science and Technology highlighted that there are several bodies saddled with combating cybercrime and enforcing cyber-laws in the UK.[426] There are also other forums established to assist the government-established bodies. These law enforcement initiatives are discussed below.

i. LOCAL POLICE FORCES

According to the report of the UK Parliamentary Office of Science and Technology,[427] every UK police force has some level of computer crime forensic and investigation capabilities. Therefore, the UK Home Office has advised people to contact their local police when there are incidents of cybercrime or when they are victims of cybercrime.[428] The UK police have set up the Police Central E-Crime Unit, which is the police unit that coordinates online law enforcement and leads investigations into online offences.[429] The unit collaborates with other agencies that also assist in ensuring that the rule of law is adhered to in UK cyberspace.

426 http://www.parliament.uk/documents/post/postpn271.pdf (Date of use: 5 February 2013).
427 http://www.parliament.uk/documents/post/postpn271.pdf (Date of use: 5 February 2013).
428 http://www.parliament.uk/documents/post/postpn271.pdf (Date of use: 5 February 2013).
429 Yar M *Cybercrime and society* (Sage Publications London 2013) 142-155.

ii. SERIOUS AND ORGANISED CRIME AGENCY

The Serious and Organised Crime Agency (SOCA) has an electronic crime unit which oversees the policing of computer crime in the UK.[430] The enactment of the Serious and Organised Crime Act of 2005 brought about a fusion of the National High Tech Crime Unit (NHTCU), which used to investigate serious and organised crime committed over the internet, with SOCA.[431] The main aim of SOCA is to reduce the harm caused by organised crime through the cyberspace.[432] In a bid to create a stronger body to tackle organised crime, including cybercrime, the UK government has proposed the emergence of the National Crime Agency (NCA) that was supposed to come into being in 2013.[433] The NCA will fuse with SOCA and will emerge as a stronger crime-fighting body. This indicates a stronger resolve to combat online crime in the United Kingdom.

iii. CHILD EXPLOITATION AND ONLINE PROTECTION CENTRE

The Child Exploitation and Online Protection Centre (CEOP) aims at eradicating child sex abuse.[434] The agency is a part of the UK policing system that tracks and brings child sex offenders to justice.[435] It also operates a website and an offline instruction campaign to advise minors and their parents about online safety.[436]

iv. COMMUNICATION ELECTRONICS SECURITY GROUP

The Communication Electronics Security Group (CESG) is the UK government's national technical authority for information assurance which aims at protecting and promoting the essential interests of the country by providing the requisite advice and

---

430 http://www.parliament.uk/documents/post/postpn271.pdf (Date of use: 5 February 2013).

431 See sec 1(3) Serious and Organised Crime Act of United Kingdom, 2005. See also Goodwin B "Hightech is put on trial" http://www.computerweekly.com/feature/High-tech-crime-is-put-on-trial (Date of use: 5 February 2013).

432 http://www.parliament.uk/documents/post/postpn271.pdf (Date of use: 5 February 2013).

433 http://www.homeoffice.gov.uk/crime/nca/ (Date of use: 5 February 2013).

434 http://ceop.police.uk/About-Us/ (Date of use: 5 February 2013).

435 Yar *cybercrime* 145.

436 http://www.parliament.uk/documents/post/postpn271.pdf (Date of use: 5 February 2013).

support on the security of communication and electronic data systems.[437] It ensures that communication and information technology systems are secured and reliable for the private and public sectors.

v. NATIONAL INFRASTRUCTURE SECURITY COORDINATION CENTRE

The National Infrastructure Security Coordination Centre (NISCC) is made up of various departments with the aim of protecting the country's Critical National Infrastructure (CNI) from electronic attack.[438] The body collaborates with Telecommunications, energy, and water agencies to make available threat evaluations and warnings relating to information and communication technology (ICT) incidents.[439]

vi. CYBER SECURITY OPERATIONS CENTRE

The Cyber Security Operations Centre (CSOC) was set up in 2010 to monitor the internet for threats to UK infrastructure. The agency aims to counter such threats when necessary.[440]

vii. UK COMPUTER EMERGENCY RESPONSE TEAM

The UK Computer Emergency Response Team (UKCERT) an informal forum that comprises of UK computer security incident response teams (CSIRT) in collaboration with other government, academic, corporate and commercial computer emergency response teams.[441] This forum provides practical information and advice in relation to information technology security issues.[442]

---

437 http://www.parliament.uk/documents/post/postpn271.pdf (Date of use: 5 February 2013).
438 http://www.parliament.uk/documents/post/postpn271.pdf (Date of use: 5 February 2013).
439 http://www.parliament.uk/documents/post/postpn271.pdf (Date of use: 5 February 2013).
440 https://www.infosecurity-magazine.com/news/uk-government-cyber-security-operations-centre/ (Date of use: 5 February 2013).
441 https://joinup.ec.europa.eu/sites/default/files/document/2014-12/United%20Kingdom%20Country%20Report.pdf (Date of use: 5 February 2013).
442 https://joinup.ec.europa.eu/sites/default/files/document/2014-12/United%20Kingdom%20Country%20Report.pdf (Date of use: 5 February 2013).

viii. INTERNET WATCH FOUNDATION

The Internet Watch Foundation (IWF) operates a reporting system where individuals can report criminal online content that will assist the police, various law enforcement bodies and internet service providers (ISPs) to investigate child pornography hosted anywhere in the world and criminally obscene adult content hosted in the United Kingdom.[443]

2.3.1.1. STAFF RESOURCES

As at the year 2007, the computer crime unit of the Serious and Organised Crime Authority (SOCA) has 80 staff members. During 2009, McMurdie, the Metropolitan Police Superintendent, pointed out that the Police Central E-Crime Unit (PceU) had 30 staff members.[444] However, according to Tom Brewester, following the fusion of the E-Crime Unit and the Serious and Organised Crime Authority (SOCA) and the Police Central E-Crime Unit (PceU) with the proposed National Cybercrime Unit (NCCU) of the National Crime Agency (NCA), an additional 70 workers will be added to this number.[445] This does not put into account the trained police detectives across the various police stations across the country.

2.3.1.2. TECHNOLOGICAL RESOURCES

The technological resources available to law enforcement agencies to a large extent determine their capacity to investigate cyber-criminal activities. This is achieved through cyber-forensics. An essential part of the use of forensics and other technological resources in the fight against cybercrime is to safeguard and salvage evidential

443 Wall D "Maintaining order and law in the internet" in *Crime and the internet* (Routledge New York 2001) 167-183.

444 Wattanajantra A "Cybercrime: The challenges of the police central e-crime unit" http://www.itpro.co.uk/609968/cybercrime-the-challenges-of-the-police-central-e-crime-unit (Date of use: 17 April 2013.

445 Brewster T "The rush to fix Britain's cyber police" http://www.techweekeurope.co.uk/news/fixing-cyber-police-security-pceu-soca-national-crime-agency-106466 (Date of use: 17 April 2013).

materials from computers and other ICT equipment and to translate such evidence into a structure that will be admissible in court.[446]

The London Metropolitan Police Force uses the EnCase forensic edition as its main tool in computer crime investigations.[447] The EnCase forensic edition has also been confirmed to aid Scotland Yard's computer crime unit to solve cases relating to child pornography, viruses, denial of service attacks and to preserve, analyse and document vital digital evidence.[448] The EnCase forensic edition has been classed by Sheldon as the latest forensic technology.[449]

Apart from the EnCase forensic tool, the police also rely on several "FastBloc write-blocking hardware devices" in order to guarantee that all retrieved evidence meets forensic standards and to ensure that the digital evidence is reliable and admissible in court.[450] There are several other forensic tools that assist forensic investigators in investigating cybercrime, some of which include Forensic Toolkit (computer forensic software), mobile phone examiners, digital decryption tools and many other tools that assist and educate the investigators in their effort to combat cybercrime in the UK.[451]

2.3.1.3. FUNDING

An important aspect that will boost the ability of the prevalent law enforcement bodies to fight cybercrime is the funding received by these bodies. This will enable the correct personnel to be engaged to give proper training to these personnel, get up-to-date

446 http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf (Date of use: 7 February 2013).

447 Zintel M "Scotland Yard selects guidance software's EnCase to combat UK's computer crime" http://www.crime-research.org/news/2003/01/Mess1003.htm (Date of use: 7 February 2013).

448 Zintel http://www.crime-research.org/news/2003/01/Mess1003.htm (Date of use: 7 February 2013).

449 Zintel http://www.crime-research.org/news/2003/01/Mess1003.htm (Date of use: 7 February 2013).

450 Zintel http://www.crime-research.org/news/2003/01/Mess1003.htm (Date of use: 7 February 2013).

451 http://www.accessdata.com/products/digital-forensics (Date of use: 7 February 2013).

equipment to prevent and investigate the crime, and enable these bodies to run their various activities without any hindrance.

In 2010 the UK government spent £650 million on its National Cyber Security Programme in order to effectively tackle cybercrime.[452] During 2011/2012 the government spent £63 million.[453] The UK police forces spent £1.3 Million on cybercrime training between 2015 and 2017[454] while the UK government in 2016 announced that it will increase its cyber security spending to £1.9 Billion.[455] These funds do not include private sector participation in the fight against cybercrime. In addition, in 2012 the UK government sent £100,000 to the Council of Europe global project to help fund the project.[456] This funding to a large extent demonstrates the commitment and willingness of the UK government to combat cybercrime within and outside its borders.

2.3.1.4. TRAINING AND EDUCATION

The UK police forces require their staff to undergo training courses to enhance their knowledge of cybercrime and to equip them with the basic knowledge to combat the menace. To this end, the College of Policing[457] was formed upon the emergence of the Serious Organised Crime Agency; to train members of the police force in courses that will give them the knowledge to investigate and combat cybercrime.[458] The government

---

452 http://www.infosecurity-magazine.com/view/13346/uk-to-spend-650m-on-new-national-cyber-security-programme/ (Date of use: 7 February 2013).

453 http://www.homeoffice.gov.uk/about-us/freedom-of-information/released-information1/foi-archive-crime/21981-cyber-crime-funding/ (Date of use: 7 February 2013).

454 http://www.governmenttechnology.co.uk/news/20032018/police-spend-%C2%A313-million-cyber-crime-training (Date of use: 16 September 2018).

455 Flinders K "UK government re-announces £1.9bn cyber security spend" https://www.computerweekly.com/news/450402098/UK-government-re-announces-19bn-cyber-security-spend (Date of use: 16 September 2018).

456 http://www.publicservice.co.uk/news_story.asp?id=19047 (Date of use: 7 February 2013).

457 This used to be the duty of the National Police Improvement Agency until the enactment of the Crime and Courts Act which provided for the emergence of Serious Organised Crime Agency. See http://www.npia.police.uk/en/16761.htm (Date of use: 7 February 2013).

458 http://www.college.police.uk/cps/rde/xchg/cop/root.xsl/16732.htm. (Date of use: 7 February 2013) Note that upon the subsequent emergence of the National Crime Agency (NCA), some of the functions of the College of Policing will be transferred to the National Crime Agency (NCA) and the Police ICT Company. See http://www.npia.police.uk/en/16761.htm (Date of use: 7 February 2013).

also collaborates with other participants in the sector to increase the skills of the law enforcement bodies. For example, Sheldon points out that in 2003, more than 550 UK computer crime investigators had undertaken courses organised by Guidance Software's forensics.[459] Between 2015 and 2017, 39,438 police officers were given cybercrime training.[460]

Sheldon further observed that for an individual to be suitable for training for the role of a computer crime forensic investigator, the individual should possess some minimum skills, which include:

(i) intermediate understanding of computer architecture;
(ii) intermediate appreciation as regards the use and methodology of computer related devices;
(iii) intermediate appreciation of the application and methodology of software with specific reference to internet and email clients, word processing, file sharing, and database applications;
(iv) intermediate understanding of relevant legislation;
(v) good communication skills;
(vi) ability to manage workload and prioritise tasks; and
(vii) ability to work effectively as part of a team.[461]

2.3.2. UNITED STATES OF AMERICA

According to the United States Department of Justice, the United States has several law enforcement initiatives/bodies saddled with the duty of combating cybercrime and

459 Zintel http://www.crime-research.org/news/2003/01/Mess1003.htm (Date of use: 7 February 2013).
460 http://parliamentstreet.org/wp-content/uploads/2018/03/Parliament-Street-Policing-and-Cybercrime.pdf (Date of use: 16 September 2018).
461 http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf (Date of use: 7 February 2013).

enforcing cyber-laws in the US.[462] The primary law enforcement bodies are discussed below.

i. THE FEDERAL BUREAU OF INVESTIGATIONS

The Federal Bureau of Investigations (FBI**)** leads the US government's effort to combat cybercrime through its Cyber Division.[463] The agency aims at preventing and investigating cybercrime, educating the public, training FBI personnel and assisting in the prosecution of cyber-criminal activities.[464]

ii. THE DEPARTMENT OF JUSTICE

The Department of Justice is a major key law enforcement body in the investigation and prosecution of cybercrime. The Department of Justice has a number of bodies under its jurisdiction, with various functions enhancing its ability to investigate cybercrime. The Computer Crime and Intellectual Property Section (CCIPS) is the agency's unit saddled with the duty of executing the Department's national strategies in combating computer crime within and outside the borders of the US.[465] The CCIPS collaborates with other government agencies and attorneys in the prevention, investigation and prosecution of computer crimes.[466] The National Institute of Justice, a subsidiary of the Department of Justice, engages in research, the sponsoring of research, evaluation and development of strategies in combating cybercrime.[467]

Another branch of the Department of Justice that deals with aspects of cybercrime is the Bureau of Alcohol, Tobacco and Firearms (ATF). The ATF prevents, investigates and

---

462 http://www.justice.gov/criminal/cybercrime/reporting.html (Date of use: 8 February 2013).

463 Lubic P "FBI has lead in addressing cybercrime for US" http://paulsinternetsecurityblog.wordpress.com/2013/01/31/fbi-has-lead-in-addressing-cybercrime-for-us/ (Date of use: 8 February 2013).

464 Hamilton J *Defending the nation: The FBI* (Abdo Publishing Edina 2007) 12-17.

465 Brenner SW *Cybercrime: Criminal threats from cyberspace* (Greenwood Publishing California 2010) 149-163.

466 Brenner *Cybercrime: Criminal threats from cyberspace* 155.

467 Dempsey J and Forst L *An introduction to policing* (Delmar New York 2010) 1-108. See also http://www.nij.gov/topics/crime/internet-electronic/welcome.htm (Date of use: 8 February 2013).

prosecutes internet bomb threats and trafficking in explosives or incendiary devices or firearms over the internet in collaboration with other government agencies.[468]

iii. THE UNITED STATES SECRET SERVICE

The US Secret Service combats cybercrime through its Electronic Crime Task Force (ECTF).[469] The government introduced the ECTF to bring together a network of prosecutors, private industry, academia and law enforcement agencies from federal, state and local agencies.[470] The unit aims at preventing, detecting, mitigating and investigating attacks on the country's financial and critical infrastructures.[471]

iv. UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT

The United States Immigration and Customs Enforcement (ICE) agency is the investigative arm of the US Department of Homeland Security. The ICE has a cybercrime centre that combats criminal activities perpetrated through the internet.[472] The ICE cybercrimes centre is made up the Cyber Crimes Unit, Computer Forensics Unit and the Child Exploitation Investigations Unit. This centre was set up to provide support for investigations into cross-border crimes and the provision of training to international, federal, state and local law enforcement agencies.[473] The Centre aims at providing investigative support and training on cyber-related criminal activities connected to money laundering, financial fraud, internet gambling, identity and benefit document fraud, counter-proliferation, narcotics trafficking and illegal exports.[474]

---

468 Castro D "US federal cybersecurity policy" in Andreasson KJ *Cybersecurity: Public sector threats and responses* (CRC Press 2012) 127-156. See also http://www.atf.gov/about/mission/# (Date of use: 8 February 2013).

469 Govern K and Winn J "Data integrity preservation and identity theft prevention: Operational and strategic imperatives to enhance shareholder and consumer value" in Jalivand A and Malliaris T *Risk management and corporate governance* (Routledge New York 2012) 300-318.

470 http://www.secretservice.gov/ectf.shtml (Date of use: 08 February 2013).

471 http://www.secretservice.gov/ectf.shtml (Date of use: 08 February 2013).

472 http://www.ice.gov/cyber-crimes/# (Date of use: 8 February 2013).

473 http://www.ice.gov/cyber-crimes/# (Date of use: 8 February 2013).

474 http://www.ice.gov/cyber-crimes/# (Date of use: 8 February 2013).

v. UNITED STATES POSTAL INSPECTION SERVICE

The US Postal Inspection Service (USPIS) is the law enforcement unit of the US postal service saddled with the responsibility of investigating and enforcing criminal laws in order to protect the use of the country's mail system.[475] The cybercrime unit of the USPIS investigates criminal activities in conjunction with other government agencies, child exploitation and internet fraud with a mail nexus.[476]

vi. VARIOUS STATE POLICE COMPUTER CRIMES UNIT

The peculiar nature of the US legal system gives autonomy to states to enable them to enact criminal statutes under the principles of federalism although there are federal legislations on the same issue. Thus, the various states also have their cybercrime units which usually is a unit of the state police that prevents, investigates and prosecutes cyber-criminal activities within that state as provided by the state legislation. For example, the Michigan state police has a Computer Crimes Unit (CCU) which provides investigative support to law enforcement agencies around the state.[477]

According to the Department of Justice, each of the federal government-established law enforcement bodies has an office located in each state of the country.[478] In order to effectively combat cybercrime, the various law enforcement bodies and their cybercrime units share information and greatly collaborate with one another so as to present a common front in combating cybercrime.[479] The FBI in 2012 came up with the Next Generation Cyber Initiative, which is made up of specially-selected and highly-trained computer scientists who respond to cybercrime issues at any time of the day, and

475 https://postalinspectors.uspis.gov/aboutus/lab.aspx (Date of use: 8 February 2013).
476 http://www.justice.gov/criminal/cybercrime/reporting.html (Date of use: 8 February 2013).
477 http://www.michigan.gov/msp/0,1607,7-123-1589_3493_4602-143714--,00.html (Date of use: 8 February 2013).
478 http://www.justice.gov/criminal/cybercrime/reporting.html (Date of use: 8 February 2013).
479 http://www.justice.gov/criminal/cybercrime/reporting.html (Date of use: 8 February 2013).

immediately send their findings to the FBI cyber division for it to review the findings and send same to other law enforcement agencies.[480]

2.3.2.1. STAFF RESOURCES

According to FBI director,Mueller, the FBI has approximately 70 cyber squads across the FBI's field offices in 56 locations across the country.[481] The FBI also has more than 1,000 specially trained agents and forensic specialists on cybercrime.[482] According to Mueller, the FBI also has special agents that are attached to police departments in Romania, Estonia, Ukraine and The Netherlands.[483] The FBI also has legal attaché offices that constitute 63 offices covering every other country of the world.[484] The FBI also has a National Cyber Investigative Joint Force which brings together 20 law enforcement, intelligence and military agencies to investigate cyber-attacks and to predict future cyber-attacks on the nation and its infrastructure.[485] The United States Service Electronic Crimes Special Agent programme has approximately 1,400 secret service special agents that combat cybercrime.[486]

---

480 Friedman IN "National cyber security: FBI unveils next generation cyber initiative" http://www.examiner.com/article/national-cyber-security-fbi-unveils-next-generation-cyber-initiative (Date of use: 8 February 2013).

481 http://www.fbi.gov/news/testimony/oversight-of-the-federal-bureau-of-investigation-4 (Date of use: 10 February 2013).

482 Prior to the 11 September 2001 attack and the constant growth in cyber criminal activities in the United States, the FBI had previously been criticised as not having competent staff to tackle cybercrime and the few existing staff complained of being overwhelmed by the volume of work they were saddled with. See http://ecommerce.hostip.info/pages/240/Computer-Crime-ENFORCEMENT-AGENCIES.html (Date of use: 10 February 2013).

483 http://ecommerce.hostip.info/pages/240/Computer-Crime-ENFORCEMENT-AGENCIES.html (Date of use: 10 February 2013).

484 http://ecommerce.hostip.info/pages/240/Computer-Crime-ENFORCEMENT-AGENCIES.html (Date of use: 10 February 2013).

485 http://ecommerce.hostip.info/pages/240/Computer-Crime-ENFORCEMENT-AGENCIES.html (Date of use: 10 February 2013).

486 Martinez PA "Testimony of Pablo A Martinez, Deputy Special Agent in Charge, Criminal Investigative Division, US Secret Service, before the Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism" http://www.dhs.gov/news/2011/04/11/testimony-pablo-martinez-deputy-special-agent-charge-criminal-investigative-division (Date of use: 11 February 2013).

2.3.2.2. TECHNOLOGICAL RESOURCES

The various law enforcement bodies in the United States make use of a variety of computer forensic investigation tools in analysing, investigating and producing admissible evidence for the prosecution of offenders. The FBI[487] uses the Guidance software's Encase[488] multi-purpose forensic tool to analyse and investigate digital evidence.[489] Other law enforcement bodies with cybercrime units, such as the Department of Justice, the Drug Enforcement Agency (DEA), the Department of Treasury and the Department of Defence, also rely on this investigative tool. According to Andrei Belenko, the Elcomsoft Password Recovery Bundle, which is used for password recovery and decryption, is used by the FBI, the CIA, the US army, the Department of Defence and other law enforcement bodies in its investigation and analysis of computer crimes.[490] The FBI also relies on a software tool called the Cyber Crimes Task Force (CCTF) application which reduces the time and manpower in investigating a case by providing the ability to track and report budgetary and operational information in real time.[491] This software also enables names, figures, staffing and other statistical information to be entered or retrieved from a central database and this provides accuracy and efficiency during cybercrime investigations.[492]

As observed by the National Institute of Justice report, the capability of a cybercrime investigation unit to recognise domain names**,** decipher internet Protocol (IP)

---

487 The FBI has 14 regional computer forensics laboratoriums. See DeBruin L "FBI, police go high-tech to fight crime" http://usatoday30.usatoday.com/news/nation/2011-07-30-police-fbi-digital-detectives_n.htm (Date of use: 11 February 2013).

488 The EnCase forensic tool was used to investigate and produce the evidence used in convicting the BTK killer, Denis Radder who was convicted largely on digital evidence. See Taub EA "Deleting may be easy, but your hard drive still tells all" http://www.nytimes.com/2006/04/05/technology/techspecial4/05forensic.html?pagewanted=print&_r=0 (Date of use: 11 February 2013).

489 http://investors.guidancesoftware.com/releasedetail.cfm?releaseid=560712 (Date of use: 11 February 2013).

490 Belenko A "Breakthrough in password recovery: Thunder tables and GPUs" http://www.elcomsoft.com/presentations/elcomsoft_company_product_presentation_2009.pdf (Date of use: 11 February 2013).

491 http://www.fbi.gov/about-us/itb/news-features/cyber-one-stop-shopping-and-real-time-tracking (Date of use: 11 February 2013).

492 http://www.fbi.gov/about-us/itb/news-features/cyber-one-stop-shopping-and-real-time-tracking (Date of use: 11 February 2013).

addresses, and discover the owners of the IP addresses and domain names used in committing crimes is a vital part of conducting cybercrime investigations.[493] In addition, the ability to determine how data is routed is also essential in uncovering useful information in cybercrime investigations.[494]

Therefore, the FBI and other cybercrime law enforcement bodies employ some tools in detecting the domain names, data route and internet protocols.[495] The FBI employs internet tools such as "NSLookup" to find the IP address of a subject from a domain name; "Traceroute" to determine the networks location of a subject's computer; "Whois" to obtain a subject's IP address; and "Ping" to obtain an IP address for a domain name or to establish whether another computer is currently connected to a particular network.[496] These tools, however, are not adequate.

.

2.3.2.3. FUNDING

According to the FBI budget for 2012, $18,6 million was requested to enable the FBI to protect critical technological networks from cyber attacks, and to investigate and combat cybercrime.[497] In 2011 the FBI set aside $5 million for the training of its agents involved in cases of national cyber intrusions.[498] It was also reported that the US spends $66 billion to enhance its cyber-security.[499] In 2012 the US Department of State, in an effort to tackle cybercrime worldwide and to provide law enforcement training to East African countries, released $250 000 to the United Nations Office on Drugs and Crime Global Programme on Cybercrime in Africa.[500]

---

493 Hagy DW "Investigative uses of technology: devices, tools and techniques" https://www.ncjrs.gov/pdffiles1/nij/213030.pdf (Date of use: 11 February 2013).

494 Hagy https://www.ncjrs.gov/pdffiles1/nij/213030.pdf (Date of use: 11 February 2013).

495 Hagy https://www.ncjrs.gov/pdffiles1/nij/213030.pdf (Date of use: 11 February 2013).

496 Hagy https://www.ncjrs.gov/pdffiles1/nij/213030.pdf (Date of use: 11 February 2013).

497 Mueller RS "FBI budget for fiscal year 2012" http://www.fbi.gov/news/testimony/fbi-budget-for-fiscal-year-2012 (Date of use: 12 February 2013).

498 Schwartz MJ "FBI to get more cyber crime agents" http://www.informationweek.com/security/government/fbi-to-get-more-cyber-crime-agents/232300860 (Date of use: 12 February 2013).

499 https://www.statista.com/statistics/615450/cybersecurity-spending-in-the-us/ (Date of use: 16 September 2018).

500 http://www.state.gov/r/pa/prs/ps/2012/12/201786.htm (Date of use: 18 April 2013).

On the state level, various states have been making meaningful financial contributions to equip law enforcement agencies in fighting cybercrime; and funds are also being released to states to fund their fight against cybercrime. For example, in 2012 the US Department of State released $234,000 to the state of Alabama to aid its fight against cybercrime.[501] Private organisations have also contributed financially to the fight against cybercrime. For example, Facebook donated $250,000 to aid the fight against cybercrime.[502]

2.3.2.4. TRAINING AND EDUCATION

The United States Manual on the prevention and control of computer-related crime expects that cybercrime law enforcement bodies should be trained in obtaining and conserving computer evidence, international and jurisdictional issues, differences between criminal and civil laws, and the rights and privileges of the accused and also the victim of the crime.[503]

The FBI has a training academy to equip law enforcement agents to combat cybercrime.[504] The FBI academy provides training on the basics of computers and also on advanced investigative courses or techniques to prepare the trainees for intricate computer crime incidents.[505] The National Cyber-Forensics and Training Alliance (NCFTA) assists in training local, state and federal law enforcement bodies, academics and other private bodies on cybercrime prevention and investigation.[506] The Federal

---

501 http://www.wsfa.com/story/16555968/ala-gets-funding-to-fight-cyber-crime (Date of use: 18 April 2013).

502 Cluley G "Facebook donates $250 000 to help fight cybercrime (using money acquired from spammers)" http://nakedsecurity.sophos.com/2012/10/23/facebook-fight-cybercrime/ (Date of use: 18 April 2013).

503 Sen ON *Criminal justice responses to emerging computer crime problems* (MSc dissertation, University of North Texas 2001) 50.

504 The FBI training academy is based at Quantico, Virginia. See http://www.net-security.org/article.php?id=34&p=1 (Date of use: 12 February 2013).

505 http://www.net-security.org/article.php?id=34 (Date of use: 28 April 2013).

506 Protalinski E "Internet fraud alert: One-stop service to report stolen data" http://arstechnica.com/tech-policy/2010/06/internet-fraud-alert-one-stop-service-to-report-stolen-data/ (Date of use: 12 February 2013).

Law Enforcement Training Center (FLETC) also trains law enforcement bodies and shares technology with them.[507]

The United States Secret Service has a training programme for its Electronic Crimes Special Agent Program (ECSAP). The training programme has three levels of training, comprising the basic investigation of computers and electronic crimes, network intrusion responder, and computer forensics respectively.[508]

Local law enforcement agencies also provide adequate training for their law enforcement agencies. For example, the California District Attorneys' Office created the High Technology Crime Division which trains the police and other state law enforcement and prosecution bodies in combating cybercrime throughout the state of California.[509] Local cybercrime investigators, prosecutors and police are trained by the various agencies such as the National White Collar Crime Centre (NW3C) or the National Cybercrime Training Partnership (NCTP).[510]

2.4. LAW ENFORCEMENT INITIATIVES IN RESPONSE TO CYBERCRIME IN DEVELOPING NATIONS

2.4.1. NIGERIA

In analysing the law enforcement initiatives in Nigeria, it should be pointed out that the major extant law on cybercrime – the Cybercrime Act of 2015 – does not place the

507 http://www.fletc.gov/about-fletc (Date of use: 12 February 2013).

508 Martinez PA "Testimony of Pablo A Martinez, Deputy Special Agent in Charge, Criminal Investigative Division, US Secret Service, before the Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism" http://www.dhs.gov/news/2011/04/11/testimony-pablo-martinez-deputy-special-agent-charge-criminal-investigative-division (Date of use: 12 February 2013).

509 http://da.co.la.ca.us/htcu.htm (Date of use: 12 February 2013).

510 Sen ON *Criminal justice responses to emerging computer crime problems* (MSc dissertation, University of North Texas 2001) 50.

responsibility of its enforcement on a particular law enforcement agency.[511] It is customary for the Nigerian legislative and judicial system, at the time of criminalising certain actions, to make provision for the law enforcement body that will tackle the offences.[512] For example, the Economic and Financial Crime Commission Act[513] established the Economic and Financial Crime Commission as the law enforcement body that will enforce the provisions of the Act.[514] In the case of the Nigerian Cybercrime Act, the Act empowers all appropriate law enforcement agencies to enforce the Act.[515] The implication of allowing all relevant law enforcement agencies to enforce the Act is that infact there is no law enforcement body for this all-important legislation.[516] For example, the National Security Adviser, saddled with the responsibility of coordinating the law enforcement bodies, took a year before it could inaugurate the Cybercrime Advisory Council (the policy-making body created by the Act).[517] This defect weighs heavily on any meaningful fight against cybercrime in Nigeria.

Therefore, two major law enforcement agencies have been identified as the prevalent cybercrime law enforcement agencies in Nigeria.[518] The primary law enforcement bodies are now discussed.

---

511 Agbamuche-Mbu M, Igbanoi J and Soniyi T "Cybercrime Act does not create an enforcement agency" https://www.thisdaylive.com/index.php/2016/05/24/cybercrime-act-does-not-create-an-enforcement-agency/ (Date of use: 20 May 2018).

512 Agbamuche-Mbu, Igbanoi and Soniyi https://www.thisdaylive.com/index.php/2016/05/24/cybercrime-act-does-not-create-an-enforcement-agency/ (Date of use: 20 May 2018).

513 The Economic and Financial Commission Act is another law that addresses cybercrime in Nigeria.

514 Sec 5(1) Economic and Financial Commission Act, 2002.

515 Section 41(1)(a) Nigerian Cybercrime Act 2015.

516 Agbamuche-Mbu, Igbanoi and Soniyi https://www.thisdaylive.com/index.php/2016/05/24/cybercrime-act-does-not-create-an-enforcement-agency/ (Date of use: 20 May 2018).

517 Agbamuche-Mbu, Igbanoi and Soniyi https://www.thisdaylive.com/index.php/2016/05/24/cybercrime-act-does-not-create-an-enforcement-agency/ (Date of use: 20 May 2018).

518 Quarshie HO and Martin-Odoom AM "Fighting cybercrime in Africa" (2012) *Computer Science and Engineering Journal* 98-100.

i. THE ECONOMIC AND FINANCIAL CRIME COMMISSION

The Economic and Financial Crime Commission (EFCC) leads the Nigerian effort in combating cybercrime through its operations department which is the hub of all investigations in the agency.[519] The enabling Act that brought the EFCC into being empowers the agency to combat financial crimes which include those perpetrated through the internet. The agency's attention therefore revolves around financial crimes and not other forms of cybercriminal activities.[520] Thus, the agency aims at preventing and investigating computer-enabled financial crimes, especially advance fee fraud (popularly called 419);[521] educating the public; and training EFCC personnel and prosecuting offenders through its legal unit.[522] However, with the enactment of the Cybercrime Act of 2015, the EFCC is also allowed to investigate the offences criminalised by the Cybercrime Act, 2015 since the EFCC is a "relevant" law enforcement agency.[523] Thus, the EFCC can investigate the varying genres of cybercrime.

ii. THE NIGERIAN POLICE

This agency is the major law enforcement agency in the country and is involved in the prevention, investigation and prosecution of cybercrime through its Criminal Investigation Department.[524] The arm of the Criminal Investigation Department that deals with cybercrime is the Special Fraud Unit of the police.[525] The investigative jurisdiction of the Special Fraud Unit revolves around high-profile fraud, IT fraud and

---

519 http://www.efccnigeria.org/efcc/index.php/about-efcc/operations (Date of use: 21 February 2013).

520 Wada F and Odulaja GO "Assessing cyber crime and its impact on e-banking in Nigeria using social theories" (2012) *African Journal of Computer and ICT* 69-82.

521 The term '419' is adapted from sec 419 of the Nigerian Criminal Code which criminalises all forms of advance fee fraud. Advance fee fraud refers to the situation "when fraudsters target victims to make advance or upfront payments for goods, services and/or financial gains that do not materialise". See http://www.actionfraud.police.uk/fraud-az-advance-fee-fraud (Date of use: 9 October 2014).

522 http://www.efccnigeria.org/efcc/index.php/about-efcc (Date of use: 21 February 2013).

523 Sec 41(1)(a) Nigerian Cybercrime Act 2015.

524 http://www.npf.gov.ng/departments/d-department/crime-investigation (Date of use: 22 February 2013).

525 http://www.npf.gov.ng/departments/d-department/crime-investigation (Date of use: 22 February 2013).

cybercrime with a particular emphasis on just advance fee fraud.[526] The Special Fraud Unit, however, investigates fraud cases where there are multiple victims, where the loss is above two million Naira (₦2,000,000), and the transaction being investigated is of huge legal and financial intricacies beyond the capability of other law enforcement bodies.[527] The local Nigerian police command also sometimes meddles into combating advance fee fraud, but in reality lacks the requisite capacity to tackle it.[528] With the enactment of the Cybercrime Act 2015, which empowers all relevant law enforcement bodies, the various formations of the Nigerian police can also investigate and enforce the provisions of the Cybercrime Act 2015.[529]

2.4.1.1. STAFF RESOURCES

Nigeria, as most developing countries, rarely acquires or keeps accurate records or statistics of its various agencies. Thus, statistics on law enforcement agencies and its agents are mostly non-existent. For example, the Police Service Commission[530] admitted that the Commission does not have information on the exact number of police officers in Nigeria.[531]

2.4.1.2. TECHNOLOGICAL RESOURCES

The EFCC has a forensics laboratory that caters for the forensics investigation and digital evidence preparation of the agency.[532] The Special Fraud Unit of the Nigerian Police Criminal Investigation Department also has a forensic laboratory for the

526 http://www.npf.gov.ng/departments/d-department/crime-investigation (Date of use: 22 February 2013).

527 http://specialfraudunit.org.ng/fraud.html (Date of use: 22 February 2013).

528 The local police mostly pretend that they are investigating advance fee fraud and end up extorting individuals and businesses under the guise that they are fighting advance fee fraud. See http://www.balancingact-africa.com/news/en/issue-no-177/internet/nigerian-police-exto/en (Date of use: 9 October 2014).

529 Section 41(1)(a) Nigerian Cybercrime Act 2015.

530 This agency oversees the welfare, conditions of service, salaries, and promotion of members of the Nigerian police.

531 http://www.nigerianpilot.com/we-dont-know-exact-number-of-police-in-nigeria-psc/ (Date of use: 20 April 2013).

532 http://newsdiaryonline.com/house_speak.htm (Date of use: 22 February 2013).

investigation of fraud crimes which includes advance fee fraud perpetrated through the internet.[533] The foundation of a modern forensic laboratory for the Special Fraud Unit was set up in early 2013.[534]

The EFCC's effort to tackle the genre of cybercrime that they are empowered to fight led to the development of the Eagle Claw software which is used to sniff out fraudulent e-mails from computer systems.[535] The software, which was developed with the help of Microsoft, will also provide the EFCC with the alternative of either monitoring or closing down fraudulent e-mail addresses.[536]

The Nigerian police[537] and sometimes the EFCC also rely on traditional methods of investigation which entails going to internet cafes as regular customers, covertly spying on internet users and then swooping on those users whose activities on the internet look suspicious.[538] The arrested persons will be forced to open all the websites they visit, and if any person is found to be sending fraudulent e-mails, that person is transported to the police station where the person makes a confessional statement which sometimes is elicited after some physical torture.

---

533 http://specialfraudunit.org.ng/about.html (Date of use: 22 February 2013).

534 Odita S "For police, a forensic laboratory to fight financial crimes" http://www.ngrguardiannews.com/index.php?option=com_content&view=article&id=112349:for-police-a-forensic-laboratory-to-fight-financial-crimes&catid=3:metro&Itemid=558 (Date of use: 22 February 2013).

535 Oates J "Operation Eagle Claw nets 18 Nigerian spammers" http://www.theregister.co.uk/2009/10/23/nigeria_police_success/ (Date of use: 23 February 2013).

536 Oates http://www.theregister.co.uk/2009/10/23/nigeria_police_success/ (Date of use: 23 February 2013).

537 Ladapo observed that the Nigerian police lack the capacity to investigate and, therefore, when it wants to elicit a confessional statement from an accused person, they can indulge in the torture of the individual to force the person to give a confessional statement that will be used by the prosecution. See Ladapo OA "Effective investigations, a pivot to efficient criminal justice administration: Challenges in Nigeria" (2011) *African Journal of Criminology and Justice Studies* 79-94.

538 The EFCC employed the same style to arrest some advance fee fraudsters in some parts of Nigeria. See http://www.fraudwatchers.org/forums/showthread.php?t=15076 (Date of use: 23 February 2013).

2.4.1.3. FUNDING

Law enforcement agencies in Nigeria that combat cybercrime are funded mainly by the Nigerian government and also by foreign government donors. For example, in 2004 the Nigerian government funded the EFCC with US $2 million.[539] The European Union between 2005 and 2009 also gave a grant of approximately $32 million to the EFCC.[540]

The UN Office on Drugs and Crime (UNODC) reports that the European Union has released €25 million to enable the EFCC to upgrade its operational capacity through the acquisition of up-to-date equipment and personnel training.[541]

Unfortunately, in December 2012 *Vanguard* newspaper reported that the Nigerian government was not providing the much-needed funds to combat cybercrime by stating that the "EFCC is not properly positioned budget-wise to perform its tedious task" because there was no allocation by the federal government to take care of the agency's legal department, forensic laboratory and the information technology portions of the Commission for the year 2012.[542]

2.4.1.4. TRAINING AND EDUCATION

The EFCC has an academy that trains members of the agency and other law enforcement agencies on how to investigate and combat fraud and advance fee fraud (cybercrime).[543]

---

539 Ogwezzy MC "Cyber crime and the proliferation of yahoo addicts in Nigeria" (2012) *AGORA International Journal of Juridical Sciences* 86-102.

540 Ogwezzy *Cyber crime* 2012 *AGORA IJJS* 94.

541 http://www.unodc.org/nigeria/en/eu-funded-project-sponsors-forensic-workshop.html (Date of use: 23 February 2013).

542 Iredia T "Who is crippling the EFCC" http://www.vanguardngr.com/2012/12/who-is-crippling-the-efcc/ (Date of use: 23 February 2013).

543 http://www.efccnigeria.org/efcc/index.php/about-efcc/efcc-academy (Date of use: 23 February 2013).

Law enforcement bodies in Nigeria rely heavily on training by foreign government agencies and private computer forensics companies for their capacity building. According to the UN Office on Drugs and crime (UNODC), forensic experts from the United Kingdom and United States provide training and mentoring for staff of the EFCC forensic lab on computer forensics through a mentoring programme funded by the European Union and implemented by the UN Office on Drugs and Crime (UNODC).[544] The programme is also geared towards training both judges and prosecutors.[545]

According to Rebricks Consult Limited, the company provides training on computer fraud for Nigerian police personnel with 400 senior police officers of various police commands already trained on combating fraud.[546] The company's training partner, First Digital & Techno-Law Forensics Company, provides training for computer forensics investigators.[547]

As far as the prosecutors are concerned, the Federal Ministry of Justice occasionally conducts capacity-building training for federal prosecutors in forensic evidence examination and presentation.[548] The training is conducted by a private company called the First Digital & Techno-Law Forensics Company.[549]

2.4.2 INDIA

In order to properly analyse the commitment and the steps taken by the Indian government to fight cybercrime within its jurisdiction, this research will examine the

---

544 http://www.unodc.org/nigeria/en/eu-funded-project-sponsors-forensic-workshop.html (Date of use: 23 February 2013).

545 http://www.unodc.org/nigeria/en/eu-funded-project-sponsors-forensic-workshop.html (Date of use: 23 February 2013).

546 Aginam E "FG trains legal officers on forensic evidence" http://www.vanguardngr.com/2012/11/fg-trains-legal-officers-on-forensic-evidence/ (Date of use: 24 February 2013).

547 Aginam http://www.vanguardngr.com/2012/11/fg-trains-legal-officers-on-forensic-evidence/ (Date of use: 24 February 2013).

548 Aginam http://www.vanguardngr.com/2012/11/fg-trains-legal-officers-on-forensic-evidence/ (Date of use: 24 February 2013).

549 Aginam http://www.vanguardngr.com/2012/11/fg-trains-legal-officers-on-forensic-evidence/ (Date of use: 24 February 2013).

existing law-enforcement bodies, the staff strength of these bodies, the funding of same and the technological resources relied upon by these bodies.

The Indian government has established several law enforcement bodies that in turn have evolved into various cybercrime sections or units within those law enforcement bodies in order to effectively combat the menace of cybercrime. These law enforcement bodies are now discussed.

i. THE CENTRAL BUREAU OF INVESTIGATIONS

The Central Bureau of Investigations (CBI) is the premier investigating police agency in India that investigates major crimes in India which have an interstate or international effect. Cybercrime, therefore falls within their purview.[550] The CBI is the law enforcement and investigative agency of the central government.[551]

In combating cybercrime, the CBI has established the Cyber Crimes Research and Development Unit, the Cyber Crime Investigation Cell, the Cyber Forensics Laboratory and the Network Monitoring Centre.[552] These units coordinate investigations into cybercrime offences, collaborate with international agencies to share skills and techniques in investigating cybercrime, cybercrime forensics lab investigation, monitoring of the internet for cybercrime incidents, cybercrime prevention and the provision of digital evidence.[553]

ii. THE CRIMINAL INVESTIGATION DEPARTMENT

---

550 http://cbi.nic.in/aboutus/cbiroles.php (Date of use: 14 February 2013).

551 Mehta D "Economic crime in a globalising society: Its impact on the sound development of the state – An indian perspective" in *Economic crime in a globalising society – Its impact on the sound development of the state* Papers delivered at the 126th Senior Seminar of United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI) 13 January-12 February 2004, Tokyo, 71-84.

552 http://cbi.nic.in/aboutus/manuals/Chapter_18.pdf (Date of use: 14 February 2013).

553 See also Mehta *Economic crime* 71. See also http://cbi.nic.in/aboutus/manuals/Chapter_26.pdf (Date of use: 14 February 2013).

The Criminal Investigation Department (CID) is a specialised unit of many state police commands in India.[554] Most of these state CIDs have set up cybercrime cells or police stations to prevent, investigate and prepare digital evidence for the prosecution of cybercrime.[555] These cybercrime units also have Computer Analysis Labs (CCAB) for their forensic investigations.[556] The local police stations normally send cases of cybercrime to the CID's cybercrime cell since they are not all equipped to handle cases of cybercrime.[557]

iii. LOCAL POLICE

A number of local police stations have set up specialised cyber units to help in the prevention and investigation of cybercrime within its jurisdiction. For example, in Nagpur in January 2013 the rural police station opened a cyber cell equipped with modern gadgets and software for the police's cybercrime investigations.[558]

2.4.2.1. STAFF RESOURCES

The cyber police stations or cyber cells of the various State Criminal Investigation Departments have a varying number of staff that combat cybercrime depending on the commitment of each state police to combat cybercrime. However, there is consensus that the staff strength of cyber police stations has been poor. For instance, in Bhopal the cyber police stations has a staff strength of 50 agents of varying ranks that tackle cybercrime through prevention, investigation and the production of digital evidence

554 The Indian Constitution puts the 'police' and 'public order' under the State list. Therefore, the police is raised and sustained by the state governments. See Mehta *Economic crime* 71.

555 http://cidwestbengal.gov.in/ (Date of use: 14 February 2013).

556 http://cidwestbengal.gov.in/ (Date of use: 14 February 2013).

557 Sinha S "Indian police not capable of solving hi-tech cyber crimes" http://www.indianexpress.com/news/-indian-police-not-capable-of-solving-hitech-cyber-crimes-/1009410 (Date of use: 14 February 2013).

558 Bose SS "Nagpur rural police gets modern cyber cell" http://timesofindia.indiatimes.com/city/nagpur/Nagpur-rural-police-gets-modern-cyber-cell/articleshow/18466610.cms (Date of use: 15 February 2013).

across the state.[559] However, there has been a proposal to increase the staff to 700 in order to keep up with the increase in cybercriminal activities that need to be investigated.[560]

As at May 2012, the cybercrime police station/cyber cell of the Banglore Central Investigation Department (CID) has 26 agents of different ranks that combat cybercrime.[561] As at July 2012, the Kerala state's cyber police station had 11 agents that enforce cyber laws and tackle cybercrime.[562] According to a 2007 report, the New Delhi cyber cell has a staff of 11 agents and is facing a staff and resource crunch under the burden of increasing cybercrime cases.[563]

2.4.2.2. TECHNOLOGICAL RESOURCES

According to the *Sakal Times*, there are four central forensic science laboratories in India that provide scientific analysis of evidence which includes evidence on cybercrime offences.[564] The Central Bureau for Investigation relies on the Central Forensic Science Laboratory in New Delhi for its forensics requirements.[565] *Sakal Times* reports that three new hi-tech laboratories are also being set up by the government.[566] On the other hand, most state criminal investigation departments have set up their Computer Crime

---

559 The report was produced in August 2012. See Sirothia A "Staff crunch cripple cyber crime cell" http://articles.timesofindia.indiatimes.com/2012-08-12/bhopal/33167201_1_cyber-cell-cyber-crime-crime-detection (Date of use: 15 February 2013).

560 Sirothia http://articles.timesofindia.indiatimes.com/2012-08-12/bhopal/33167201_1_cyber-cell-cyber-crime-crime-detection (Date of use: 15 February 2013).

561 http://ibnlive.in.com/news/cyber-crime-police-station-shortstaffed/255424-60-119.html (Date of use: 15 February 2013).

562 http://newindianexpress.com/states/kerala/article562041.ece?service=print (Date of use: 15 February 2013).

563 Makkar S "Who will tackle cyber crime: Delhi police debates" http://www.india-forums.com/news/sci-tech/45564-who-will-tackle-cyber-crime-delhi-police-debates.htm (Date of use: 15 February 2013).

564 http://72.78.249.187/SakaalTimesBeta/20121227/5600265108256631975.htm (Date of use: 15 February 2013).

565 http://72.78.249.187/SakaalTimesBeta/20121227/5600265108256631975.htm (Date of use: 15 February 2013).

566 http://72.78.249.187/SakaalTimesBeta/20121227/5600265108256631975.htm (Date of use: 15 February 2013).

Analysis Labs (CCAB).[567] The Central Bureau of Investigation and the Central Forensic Science laboratory run a Cyber Forensics and Digital Analysis Centre as a joint venture.[568]

The law enforcement bodies rely on a range of computer forensic investigation tools in analysing, investigating and producing admissible evidence for the prosecution of offenders. Some of these tools include the Encase forensics investigation tool produced by Guidance software to analyse and investigate digital evidence.[569] They also rely on the DIBS[570] range of computer software and hardware exclusively "designed to copy, analyse and present computer data in a forensically sound manner".[571] The Data Recovery and Analysis Computer (DRAC) forensic software is used for data recovery and investigations.[572] In addition, the Password Recovery forensics kit and many other computer forensics tools are used by the law enforcement agencies.[573] The Indian law enforcement bodies also place reliance on a portable forensic investigation tool named pCHIP designed by the Asian School of Cyber Laws and Data64 Techno Solutions Pvt Ltd.[574]

2.4.2.3. FUNDING

In September 2007, the Indian government announced the release of $853,000 to the Central Bureau of Investigation in order for the bureau to purchase modern tools and

---

567 For example, the West Bengal Criminal Investigation Department has its Computer Crime Analysis Lab (CCAB) that performs cybercrime forensics analysis. See http://cidwestbengal.gov.in/ (Date of use: 15 February 2013).

568 http://cbi.nic.in/aboutus/manuals/Chapter_26.pdf (Date of use: 15 February 2013).

569 http://cbi.nic.in/aboutus/manuals/Chapter_26.pdf (Date of use: 15 February 2013).

570 http://cbi.nic.in/aboutus/manuals/Chapter_26.pdf (Date of use: 15 February 2013).

571 http://www.dibsforensics.com/equipment.html (Date of use: 16 February 2013).

572 http://www.labsystems.co.in/drac.html (Date of use: 16 February 2013).

573 http://www.labsystems.co.in/drac.html (Date of use: 16 February 2013).

574 The pCHIP can recover crucial volatile digital evidence from a computer and then generate a report on them; detect and list password protected and encrypted files on a computer; attack and break diverse types of passwords; clone and retrieve deleted data; and generate a report containing the details of every USB device ever connected to a computer which is the subject matter of an investigation. See Hakim S "World's smallest cyber crime investigation device released by ASCL & Data64" http://cyberforensicsindia.blogspot.com/2010/08/worlds-smallest-cyber-crime.html (Date of use: 16 February 2013).

software to combat cybercrime.[575] It is evident that the law enforcement agencies in India are grossly underfunded.[576]

2.4.2.4 TRAINING AND EDUCATION

The CBI has a training academy that equips law enforcement agents with the requisite knowledge and skills to combat cybercrime; and the expertise of the Central Forensics Science Laboratory is used as part of the training.[577] The National Association of Software and Services Companies (NASSCOM), a non-governmental organisation, and its affiliate, Data Security Council of India (DSCI), provides training and capacity building for cybercrime law enforcement agencies in India through its several cyber laboratories across India that train cyber police officers, prosecutors and judicial officers in cyber forensics.[578] The Asia School of Cyber Laws (ASCL) (also a non-governmental organisation) and its subsidiary, Data 64 Techno Solutions Pvt Ltd, provide law enforcement bodies and prosecutors with adequate training in cybercrime forensics and investigations.[579]

2.4.3. SOUTH AFRICA

The South African draft national cyber-security policy framework observes that there are several state organs that ensure the enforcement of laws in cyberspace in South Africa. These law enforcement are listed below.

---

575 Raja M "The dark face of the internet in India" http://atimes.com/atimes/South_Asia/II20Df01.html (Date of use: 16 February 2013).

576 There is a dearth of information on the funding of the fight against cybercrime in India.

577 The CBI training academy is based at Ghaziabad. See http://cbi.nic.in/aboutus/div.php (Date of use: 16 February 2013).

578 http://www.dsci.in/cyber-labs (Date of use: 16 February 2013). See also Gill V "NASSCOM held an introductory training programme on cyber crime for Gurgaon police today. Topics covered included cyber forensics, ethical hacking, identity theft and privacy" http://timesofindia.indiatimes.com/topic/cyber-crime/news/ (Date of use: 16 February 2013).

579 The Asia School of Cyber Laws (ASCL) and its subsidiary Data 64 Techno Solutions Pvt Ltd are non-governmental organisations. See http://www.data64.in/about-us.php (Date of use: 16 February 2013).

i. THE STATE SECURITY AGENCY

The State Security Agency (SSA) is tasked alongside other government agencies with the duty of coordinating, implementing and developing cyber security measures for the country.[580] The SSA conducts cyber security investigations and also reports to the government on the state of cyber security in the country.[581]

ii. SOUTH AFRICAN POLICE SERVICE

The South African Police Service (SAPS) is the leading law enforcement body in South Africa. The SAPS is saddled with the responsibility of preventing, investigating and providing digital evidence for the prosecution of cyber crime.

The SAPS has a Directorate of Priority Crime Investigations (DPCI), which is a key unit in SAPS with expert investigative competence, focusing on national priority crimes, cybercrime and many other serious economic crimes.[582] The cybercrime unit is an arm of the Directorate of Priority Crime Investigations (DPCI) and has the capacity and responsibility of investigating and combating cybercrime.[583]

iii. NATIONAL PROSECUTING AUTHORITY

The National Prosecuting Authority (NPA) is the state's agency saddled with the responsibility of prosecuting a criminal on behalf of the state.[584] They are entrusted with the duty of prosecuting cybercrime offences and ensuring that all relevant cybercrime

---

580 http://www.info.gov.za/speech/DynamicAction?pageid=461&sid=25751&tid=59794 (Date of use: 19 February 2013).

581 http://www.cyanre.co.za/national-cybersecurity-policy.pdf (Date of use: 19 February 2013).

582 http://www.info.gov.za/view/DownloadFileAction?id=127117 (Date of use: 19 February 2013).

583 http://www.saps.gov.za/docs_publs/legislation/country_report/part_two.pdf (Date of use: 19 February 2013).

584 http://www.npa.gov.za/UploadedFiles/NPA%20Strategic%20Plan%202012%20-%202017.pdf (Date of use: 19 February 2013).

laws are aligned with the national cyber security policy framework to ensure a coherent cybercrime prosecution approach across South Africa.[585]

2.4.3.1. STAFF RESOURCES

At the launching of the Cybercrime unit of SAPS' Directorate of Priority Crime Investigations (DPCI), the unit consisted of 40 highly-experienced agents with forensic skills.[586]

2.4.3.2. TECHNOLOGICAL RESOURCES

The South African Police Service (SAPS) operate forensic science laboratories for the scientific analysis of tools used in the perpetration of criminal offences.[587] These forensic laboratories also engage in the analysis of cybercrime offences through its Scientific Analysis Unit.[588]

These law enforcement bodies rely on a variety of computer forensic investigation tools in analysing, investigating and producing admissible evidence for the prosecution of offenders. Some of these tools include "SalvationDATA's 3+1 data recovery flow"[589] for data restoration, extraction and retrieval,[590] and SalvationData's HD Doctor Suite and

---

585 http://www.cyanre.co.za/national-cybersecurity-policy.pdf (Date of use: 19 February 2013).

586 Mashabane P "Unit set to tackle cyber crime" http://www.citizen.co.za/citizen/content/en/citizen/local-news?oid=228630&sn=Detail&pid=334&Unit-set-to-tackle-cyber-crime (Date of use: 20 April 2013). There is a dearth of information on the staff resources of South African law enforcement agencies.

587 According to SAPS, the main laboratory is based in Pretoria, while decentralised offices have been established in Cape Town, Port Elizabeth and Durban. The forensics laboratories in Pretoria and the Western Cape have all the forensic units, while the Eastern Cape laboratory has only the ballistic and chemistry units and the laboratory in KwaZulu-Natal has only the ballistic unit. See http://www.saps.gov.za/_dynamicModules/internetSite/faqBuild.asp?myURL=273 (Date of use: 20 February 2013).

588 http://www.saps.gov.za/_dynamicModules/internetSite/faqBuild.asp?myURL=273 (Date of use: 20 February 2013).

589 http://recoverytoolsrus.com/forensic-data-recovery-news/news-11-27.html (Date of use: 20 February 2013).

590 http://www.salvationdata.com/data-recovery-examples/data-recovery-flow.htm (Date of use: 20 February 2013).

DC Premium forensics tools to "detect, extract, retrieve, recover, copy and wipe confidential information stored in the encrypted hard disk drives or hardly read disks".[591] They also rely on the Encase forensics investigation tool produced by Guidance software to analyse and investigate digital evidence,[592] and on the Access Data's Forensic toolkit 3[593] used for the recovery of deleted files and also to decrypt files.[594]

2.4.3.3. FUNDING

According to the *Bluechip* journal, the South African government has spent ZAR 7.1 million to combat cybercrime and to correct the damage done by cybercrime.[595] In addition, the Department of Justice and Constitutional Development stated that the South African Cabinet in 2012 approved ZAR150 million for the cybercrime unit of the South African Police Service (SAPS) (also known as the Hawks), the Special Investigating Unit and the National Prosecuting Authority.[596]

2.4.3.4. TRAINING AND EDUCATION

The SAPS has a training division which trains all members of the force, and this also involves specialised training for specialised police units such as the cybercrime unit.[597] Members of the forensics laboratory receive SAPS in-service training for the forensics unit in which the staff will work in, and this includes the scientific analysis unit which also

---

591 http://recoverytoolsrus.com/forensic-data-recovery-news/news-11-27.html (Date of use: 20 February 2013).

592 Kohn MD, Eloff JHP and Olivier MS "UML modelling of digital forensic process models (DFPMs)" Papers delivered at the Information Security for South Africa (ISSA) 2008 Innovative Minds Conference, 7-9 July 2008, Johannesburg, South Africa, 149-162.

593 Kohn *et al UML modelling* 149.

594 T Clark "Forensic toolkit information" http://www.jesc.co.za/downloads/products/1%20AccessData/10%20FTK%20Information.pdf (Date of use: 20 February 2013).

595 http://www.bluechipjournal.co.za/articles/cyber-crime (Date of use: 20 February 2013).

596 Radebe J "Results beginning to show in fight against crime/corruption" http://www.politicsweb.co.za/politicsweb/view/politicsweb/en/page71656?oid=281004&sn=Detail (Date of use: 20 February 2013) Information on funding the fight against cybercrime in South Africa is limited.

597 http://www.saps.gov.za/_dynamicModules/internetSite/HOnewsBuild.asp?myURL=33 (Date of use: 20 February 2013).

addresses cybercrime forensics.[598] The Department of Justice and Constitutional Development (DoJ&CD), for its part, provides training which includes cybercrime training for the prosecutors through its Justice College.[599]

The private sector is also involved in the training of law enforcement agents and forensics investigators. For example, a private forensics provider, Cyanre, provides law enforcement agencies in South Africa with training and skills transfer in areas such as forensic investigative tools, the application of the Criminal Law and Criminal Procedure Act, digital evidence and cybercrime.[600]

2.5. ADEQUACY OF CYBERCRIME LEGISLATIVE RESPONSES AND LAW ENFORCEMENT INITIATIVES

It is evident that several nations are making some effort to curb the menace of cybercrime. From the above comparative analysis of the various countries, it may be inferred that the commitment of the various countries in fighting cybercrime varies and it is tied to the level of socio-economic development experienced in that particular country. Countries that have shown serious commitment in fighting cybercrime are countries that are more dependent on computers and computer networks. These are mostly highly-industrialised countries.[601]

It is submitted that combating crime is a *sine qua non* for development. For example, from the above-mentioned discussions it is evident that the developed countries are

---

598 http://da.wwc.co.za/docs/9820/Fighting%20fit%20with%20forensics.pdf (Date of use: 20 February 2013).

599 http://www.npa.gov.za/UploadedFiles/NPA%20Strategic%20Plan%202012%20-%202017.pdf (Date of use: 20 February 2013).

600 Some Cyanre clients include the Special Investigation Unit; the Scorpions (which has now been merged with the South African Police Service (SAPS); and the SAPS. They also provide training for all state prosecutors and magistrates on cybercrime and electronic evidence. Also according to Cyanre, a member of its staff, Danny Myburgh, wrote the internal training manual for the South African Police Service members on the investigation of computer crime. See http://www.cyanre.co.za/what-sets-us-apart.html (Date of use: 20 February 2013).

601 Putnam TL and Elliot DD "International responses to cyber crime" in Sofaer AD and Goodman SE (eds) *The transnational dimension of cyber crime and terrorism* (Hoover Press Stanford 2001) 35-67.

exerting much energy in fighting cybercrime, while developing countries are still trying to find their bearing in the quest for a crime-free cyberspace. In this vein, therefore, the lesser the socio-economic development, the lesser the efforts and commitment to fight the menace of cybercrime. For example, South Africa and India joined the league of highly-industrialised countries,[602] and this is demonstrated in the extent of their efforts and commitment in funding, training and enacting adequate cybercrime legislation to address the menace of cybercrime, while Nigeria that has not joined the league, occupies the lower rung of socio-economic development and shows less effort and commitment in the fight against cybercrime. South Africa, in an apparent show of their desire to deal with information technology crime, has also become a signatory to the Council of Europe Cybercrime Convention, although South Africa has not yet ratified the Convention.[603] Surprisingly, though, India is not a party to the Council of Europe Cybercrime Convention.[604]

However, the question is whether these legislative responses and law enforcement initiatives in the developing countries are adequate. In looking at the adequacy or otherwise of the legislative responses and law enforcement initiatives in developing countries, more emphasis will be laid on the Nigerian situation which seems to occupy the lowest rung in the hierarchy of the combat of cybercrime.[605] Although Nigeria has finally enacted a cybercrime Act, a lot of other lesser developed countries are yet to enact a cybercrime legislative framework. The United Nations conference on trade and development reports that 18% of United Nations member states have no cybercrime legislation.[606] Such lesser developed countries like Mongolia, Chad, Afghanistan, Papua

602 http://www.ioha2012.net/?page_id=1945 (Date of use: 07 March 2013).

603 Madziwa S and Snail S "Cyber crime in South Africa" http://www.hg.org/article.asp?id=5351 (Date of use: 19 October 2014).

604 There have been several requests to India to become a party to the EU Cybercrime Convention in order to boost its preparedness to adequately fight information technology crime. See http://articles.economictimes.indiatimes.com/2009-03-30/news/28401922_1_cyber-terrorism-cybercrime-convention (Date of use: 19 October 2014).

605 It must be pointed out that this research has progressed considerably before the Nigerian Cybercrime Act of 2015 was enacted.

606 http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx (Date of use: 17 September 2018).

New Guinea, Democratic Republic of Congo, Central African Republic, Guyana, Sierra Leone and host of other developing countries, have no cybercrime legislation.[607]

A major factor that determines the criminalisation of a cyber activity largely depends on the national conscience of the country in question. This implies that cyber activities that will be deemed offensive within that national jurisdiction will be activities which offend the majority or the ruling class of a particular nation. For example, the strict *Lèse majesté* law of Thailand criminalises defamation or exposure of the King to any form of accusation and infraction of royal dignity, while accusing the head of a democratic state of various wrongdoings is the norm in democratic states.[608]

For any legislation to seek to tackle cybercrime at the minimal level, there are basic offences that the legislation must criminalise. For example, the Council of Europe Convention on Cybercrime establishes some minimum standards of relevant offences that has to be criminalised by national legislations.[609]

Under this sub-section, the model of categorisation of cybercrime and the offences highlighted by the Council of Europe Cybercrime Convention will be relied upon since there is consensus that the Council of Europe Cybercrime Convention is a trail blazer in the legislative response to cybercrime and that many nations participated in the drafting of the Convention. It is submitted, therefore, that legislation that is to have some level of effectiveness in tackling cybercrime must at least deal with the offences as classified by the Council of Europe Cybercrime Convention.[610] That is to say cyber activities that fall within offences that violate the confidentiality, integrity, availability of computer data and

---

607 http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx (Date of use: 17 September 2018).

608 Sec 8 of the Constitution of the Kingdom of Thailand, 2007 provides that "the King shall be enthroned in a position of revered worship and shall not be violated. No person shall expose the King to any sort of accusation or action." See also Aquino M "Thailand's strict *Lese Majeste* laws – The Thai reverence for the King" http://goseasia.about.com/od/thaipeopleculture/a/lesemajeste.htm (Date of use: 8 March 2013). Also, sec 112 of the Criminal Code of Thailand, 1956 provides that anyone who "defames, insults or threatens the King, the Queen, the heir-apparent or the regent will be punished with a jail term between three and 15 years".

609 Sec 33 Explanatory Report on Council of Europe Cybercrime Convention (ETS No 185).

610 Cap 2 Title 1 Council of Europe Cybercrime Convention (ETS No 185).

systems, computer-related offences (for instance, fraud, forgery and theft), content-related offences (for instance, child pornography), and offences related to the infringement of copyright and related rights.[611] In criminalising these offences, these categories of offences may be modified and expanded to adequately address the national peculiarities of each jurisdiction while also ensuring that the human rights of individuals within and outside the jurisdiction are not violated by the same legislation that seeks to tackle cybercrime.

As stated previously, developed countries and some developing countries have enacted laws that cover the above-mentioned four categories of offences. For example, the United States through its Computer Fraud and Abuse Act of 1986,[612] the Electronic Communications Privacy Act of 1986[613] and the different state legislations[614] variously seeks to protect the integrity, confidentiality and availability of computer data and systems by prohibiting unauthorised access to such computer systems. The United Kingdom, on the other hand, also has provisions to protect the confidentiality, integrity and availability of computer data and systems and to prohibit offences that will infringe on them.[615]

As far as South Africa[616] and India[617] are concerned, steps are also taken by their legislations to protect the confidentiality, integrity and availability of computer data and systems by the prohibition of hacking, unauthorised access or interception of data. In

611 See Cap 2, sec 1, arts 2-10 Council of Europe Cybercrime Convention (ETS No 185) The FBI cyber four-fold mission is to prevent cyber intrusions; prevent and identify online sexual predators; counteract crimes against intellectual property; and fight internet fraud. See http://www.hg.org/cyber-space.html (Date of use: 8 March 2013).

612 Title 18 USC sec 1030 United States of America Computer Fraud and Abuse Act of 1986.

613 This legislation seeks to prohibit unauthorised interception of electronic communication. Title 18 USC § 2511 United States of America Electronic Communications Privacy Act of 1986.

614 As previously highlighted in this research, the majority of the states seek to protect the confidentiality, integrity and availability of computer data and systems from "computer intrusions and damage caused by computer intrusions" and other forms of hacking. Various states expand their legislative sphere by trying to cover every aspect of hacking as is peculiar to its jurisdiction. See *Brenner 2001 Richmond JLT* 36.

615 The United Kingdom Computer Misuse Act of 1990 prohibits the "unauthorised access to computer material, unauthorised access with intent to commit or facilitate commission of further offences and unauthorised impairment of computer material".

616 Sec 86 South African Electronic Communications and Transactions Act 25 of 2002.

617 Sec 66 of the Indian Information Technology Act of 2000 prohibits hacking.

the course of this research and after much outcry, Nigeria was constrained to enact its Cybercrime Act which criminalised hacking and other forms of unauthorised access to a computer system.

As far as computer-related offences are concerned, the United States[618] and the United Kingdom as developed countries have taken adequate steps to proscribe computer-related offences through their legislations. For example, the United States federal legislations proscribe the use of computers, networks or systems for the commission of computer-related fraud[619] and computer-related forgeries.[620] A substantial number of United States state legislations prohibit computer-related fraud although a number of state legislations prohibit computer-related forgeries.[621]

In the case of the United Kingdom, computer-related fraud is proscribed by the Theft Act of 1968[622] as amended by the Fraud Act of 2006,[623] in addition to the provisions of the Computer Misuse Act of 1990, whereas computer-related forgery is partly proscribed by the Forgery and Counterfeiting Act of 1981[624] in addition to the provisions of the Computer Misuse Act of 1990.

In the case of South Africa, computer-related fraud and forgery are addressed by section 87 of the ECT Act, 2002.[625] The legislative framework in India also proscribes computer-related fraud through sections 66 and 74 of the Indian IT (Amendment) Act of 2008 and section 420 of the Indian Penal Code.[626] Computer-related forgery in India is prohibited by sections 463, 468 and 469 of the Indian Penal Code.[627]

---

618 Sec 4 Title 18 USC sec 1030 United States of America Computer Fraud and Abuse Act of 1986.
619 Sec 4 Title 18 USC sec 1030 United States of America Computer Fraud and Abuse Act of 1986.
620 Title 18 USC Sec 1028 United States of America Computer Fraud and Abuse Act of 1986 (fraud and related activity in connection with identification documents, authentication features, and information).
621 *Brenner 2001 Richmond JLT* 37.
622 Sec 15 United Kingdom Theft Act 60 of 1968.
623 United Kingdom Fraud Act 35 of 2006.
624 United Kingdom Forgery and Counterfeiting Act 45 of 1981.
625 South African Electronic Communications and Transactions Act of 2002.
626 http://www.alertindian.com/node/5 (Date of use: 14 March 2013).
627 http://www.alertindian.com/node/5 (Date of use: 14 March 2013).

In the case of Nigeria, the Cybercrime Act 2015, enacted after great clamour, also followed suit to regulate computer-related fraud or forgery.[628] The EFCC Act,[629] Advance Fee Fraud and Other Fraud Related Offences Act 2006[630] and the Nigerian Criminal Code[631] also prohibit advance fee fraud which entails obtaining property through false pretences.

In criminalising content-related offences, the CoE Cybercrime Convention highlights child pornography offences under this category.[632]

The United States have elaborate laws that protect minors and prohibit various forms of child pornography. These legislations prohibit obscene visual depictions of the sexual abuse of children; sexual exploitation of children with the aid of the computer system; transportation, distribution and other activities relating to materials involving the sexual exploitation of minors; reproduction, transportation, distribution and other activities relating to materials constituting or containing child pornography; using misleading domain names on the internet to deceive minors; using misleading words or digital images on the internet to deceive minors; and using interstate facilities to transmit information about a minor in order to entice or encourage the minor to engage in a sexual activity.[633]

The United Kingdom, for its part, has also enacted legislations to combat child pornography. The Protection of Children Act 1978 criminalises the making, distribution or publication of any indecent photograph of a minor.[634] The Act was amended by the Criminal Justice Act 1988 to include mere possession of such indecent photographs.[635] The Criminal Justice and Public Order Act 1994 added indecent pseudo-photographs of

628 Secs 11 and 12 Nigerian Cybercrime Act 2015.
629 Sec 6(b) Nigerian Economic and Financial Crime Commission (Establishment) Act of 2004.
630 Sec 1 Nigerian Advance Fee Fraud and Other Fraud Related Offences Act of 2006.
631 Sec 419 Nigerian Criminal Code Act of 1916.
632 Cap 2 Title 3 art 9 Council of Europe Convention on Cybercrime, 2001 (ETS No 185).
633 Title 18 USC 1466A, Title 18 USC 2251, Title 18 USC 2252, Title 18 USC 2252A, Title 18 USC 2252B, Title 18 USC 2252C and Title 18 USC 2425 respectively.
634 Sec 1 United Kingdom Protection of Children Act of 1978 cap 37.
635 Sec 160 United Kingdom Criminal Justice Act of 1988 cap 33.

minors to the list of prohibited sexual depiction of minors,[636] while the Coroners and Justice Act 2009 further criminalises the possession of non-photographic pornographic images in order to cover any other form that the pornographic material may take which is not photographic.[637]

In South Africa, child pornography and sexual exploitation are proscribed by sections 17 to 20 of the Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007.[638] In India, section 67b of the Indian IT Act proscribes the creation, publishing or transmission of materials in any electronic form depicting children in sexually-explicit acts.[639]

In Nigeria, the Child Rights Act of 2003 prohibits the production of child pornography or the production of any other form of child pornographic performance.[640] The Act, however, does not make mention of the transmission or publication of such pornographic material, neither does it mention the use of electronic means for such transmission. Fortunately the eventual enactment of the Nigerian Cybercrime Act in 2015 also provided Nigeria with the opportunity of proscribing the transmission or publication of pornographic material through electronic means.[641]

The fourth category of cybercrime offences, as highlighted earlier, which should form part of the basic offences to be criminalised by any government that seeks to combat cybercrime is the infringement of copyright and related offences.

In the United States, the legislature has enacted elaborate laws to combat copyright infringement of various forms. These laws criminalise the reproduction or distribution of copyright materials and also prescribe various punishments for the violations of such

636 Sec 84 United Kingdom Criminal Justice and Public Order Act of 1994 cap 33.
637 Secs 62 and 65 United Kingdom Coroners and Justice Act of 2009 cap 25.
638 As amended by the South African Judicial Matters Amendment Act 66 of 2008.
639 http://www.alertindian.com/node/5 (Date of use: 14 March 2013).
640 Sec 30 Nigerian Child's Right Act of 2003.
641 Sec 14 Nigerian Cybercrime Act, 2015.

copyrighted materials.[642] The United Kingdom proscribes any form of unlawful copyright infringement and criminalises such acts.[643]

In South Africa, copyright infringement is proscribed by the Copyright Act of 1978 (as amended).[644] In India, the Indian Copyright Act of 1957 (as amended) proscribes the various forms of copyright infringement.[645] Fortunately, in Nigeria there has been a legislation, the Copyright Act (as amended), that proscribed copyright infringement.[646]

From the foregoing, the question arises as to whether the legislative measures taken by the developing nations are adequate. As pointed out in the second section of this chapter, while analysing the legislative responses undertaken by United States, the United Kingdom, South Africa, India and Nigeria, every legislative response has its areas of inadequacy that need to be covered. Thus, even the developed countries have their areas of inadequacy. However, a look at the minimal legislative requirement that should be adopted by any government that intends to combat cybercrime shows that developed countries are really leading in the fight against cybercrime.

For the nations that are still developing but have joined the league of highly-industrialised nations, they have taken encouraging efforts in following the example of developed countries. However, most scholars have suggested that the ratification of the Council of Europe Convention on Cybercrime by these developing countries in the league of highly-industrialised nations holds the key to a successful fight against cybercrime. This is because the Convention attempts to create some consistency in the cybercrime legislation of various nations and also contains vital provisions that will aid law enforcement agencies in fighting trans-border cybercrime.[647]

---

642 Title 17 USC sec 506 provides for copyright criminal offences, while Title 18 USC sec 2319 provides for more adequate punishment for the infringement of copyright.

643 Sec 107 United Kingdom Copyright, Designs and Patent Act of 1988 as amended by The United Kingdom Copyright and Related Rights Regulations of 2003 .

644 Sec 27 South African Copyright Act 98 of 1978 (as amended).

645 Sec 63 Indian Copyright Act of 1957 (as amended).

646 Sec 18 Nigerian Copyright Act; Laws of the Federation of Nigeria 1990 (as amended).

647 Cassim F "Addressing the challenges posed by cybercrime: A South African perspective" 2010 *Journal of International Commercial Law and Technology* 118-123.

In the case of most developing nations that have not joined the league of highly-industrialised nation,[648] the legislative response in the fight against cybercrime is inadequate. Reliance is mainly placed on the antiquated legislations that were enacted before the advent of computer technology which cannot secure a conviction for any offending cyber activity since the existing criminal legislation does not include such activity as a criminal offence. However, some countries in this class (like Nigeria recently did) have been constrained after years of clamour to enact some cybercrime legislation which merely adapt the legislative responses of developed countries fraught with many inadequacies that make its implementation difficult.

This inadequacy in legislative response creates gaps that are exploited by cybercriminals to commit crimes from jurisdictions that would not punish them for the offence. Subsequent chapters in this thesis will make recommendations and attempt to proffer solutions to the apathy of several developing nations in making adequate legislative provision that will combat the menace of cybercrime.

In looking at the adequacy of the law enforcement initiatives of the highlighted nations, the developed countries blaze the trail. As already shown, the nature and utility of the technological resources and software used in investigating cybercrime incidents, the number of staff involved in fighting cybercrime, the level of training to keep the agents technologically up to date and the funds to run the agencies to some extent are being taken care of by developed countries.

However, the zenith in addressing cybercrime has not yet been attained by these developed countries since there are still a number of unsolved cybercrime cases and the available e-forensic skills and expertise struggle to catch up with the sophistication

---

[648] Since Nigeria has now enacted its cybercrime Act, Nigeria may now be excused from countries without an legislative response. Unfortunately, other countries like Mozambique do not have any form of legislative intervention on cybercrime. https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx (Date of use: 13 October 2018).

of cybercriminals.[649] For example, according to Santorelli, the police of several nations do not possess the requisite skills and technological resources, and when law enforcement agents are successfully trained to combat cybercrime, they leave the law enforcement agency to go to a more lucrative private organisation.[650] However, law enforcement agencies in developed countries are constrained to tap into the expertise of the private sector in order to augment their resources when it is stretched to its limits.[651]

Unfortunately, developing countries have fared worse in their law enforcement initiatives. As earlier observed in the legislative responses of developing nations, the countries in the league of highly-industrialised nations (South Africa and India) seem to closely follow the efforts of developed countries, especially in terms of technological resources and software used in investigating cybercriminal incidents, the level of training to keep the agents technologically up to date and the funds put in by both government and private organisations to run the law enforcement agencies.

In the case of Nigeria, the law enforcement initiative is a disaster although some level of success has been recorded. The law enforcement agencies do not have an efficient legislative backing to investigate and prosecute major cybercriminal activities.[652] They rely on traditional methods of investigation, are grossly understaffed and underfunded.[653] As a result, the majority of offensive cyber activities go unreported

649 http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf (Date of use: 23 March 2013).

650 Dalton W "Cyber-crime policing completely inadequate, says ex-Scotland Yard detective" http://www.itproportal.com/2012/11/22/cyber-crime-policing-completely-inadequate-says-ex-scotland-yard-detective/ (Date of use: 25 March 2013).

651 Ashford W "Cyber skills a top challenge, says UK police cyber crime unit" http://www.computerweekly.com/news/1280094331/Cyber-skills-a-top-challenge-says-UK-police-cyber-crime-unit (Date of use: 25 March 2013).

652 According to Brenner, "law enforcement officials cannot effectively pursue cybercriminals unless they have the legal tools necessary to do so. These legal tools include an arsenal of well-defined cybercrime offences for use in prosecuting cybercriminals and procedural rules governing evidence-gathering and investigation". See Brenner S "Cybercrime investigation and prosecution: The role of penal and procedural law" http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan003073.pdf (Date of use: 25 March 2013).

653 During the period of this research, the researcher's principal in chambers (a legal practitioner) had his computer system and e-mail hacked with the hacker sending fraudulent e-mail messages

because the average citizen does not know the right agency to complain to when he or she becomes a victim since the level of awareness about these law enforcement bodies is extremely low. Furthermore, the average Nigerian does not generally believe in the sincerity and ability of the law enforcement agencies to tackle crime which is exacerbated by corruption.

2.6. CONSIDERING THE NATURE OF THE APATHY OF DEVELOPING NATIONS

From the foregoing, it is apparent that the level of commitment to the fight against the menace of cybercrime varies between nations depending on the level of socio-economic development of that nation. Developed countries, therefore, lead in the fight against cybercrime, and among the developing countries, the countries in the league of highly-industrialised nations try to emulate the developed countries, albeit with many constraints. Unfortunately, the fight against cybercrime is at its lowest ebb among countries that have not joined the league of highly-industrialised nations. There seems to be some apathy in the developing countries that contribute to their lackadaisical attitude in fighting cybercrime. The situation gets even worse when countries classified as least-developed countries are looked into. Countries like Mozambique, Chad and Democratic Republic of Congo; that belong to the class of least-developed countries do not even have cybercrime legislation.[654] The same goes for other countries that are within that class. Thus even where the Nigerian situation is abysmal, the apathy of countries within the league of least developed countries is phenomenal.

These factors conceal from policymakers the simple fact that the easiest approach to framing a legislative response is to adopt existing cybercrime legislations from

---

to all the contacts asking for money to be sent to a particular bank account. Upon the realisation of the hacking and fraudulent message, the researcher's principal reported the activity to the Nigerian Police, the Nigerian State Secret Service and Economic and Financial Crime Commission (EFCC) who all demanded money from the said principal in order to commence the investigation. The said principal, however, obtained records of the account number and location of the culprit and gave the information to these agencies, who did nothing. The culprits were never apprehended.

654 https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx (Date of use: 13 October 2018).

developed countries, and that there are many sources of guidance from where they can develop their legislative response and law enforcement initiatives. For example, during the drafting of the Council of Europe Convention of Cybercrime, several countries that are not part of the European Union took part in the drafting, and the Cybercrime Convention allows more countries to adopt and ratify the Convention.[655] This will relieve a nation from embarking into a further in-depth study of cyber-criminal offences since a good foundation has already been laid. On the other hand, where the policy makers are constrained by the clamour from within and outside their jurisdiction to follow suit, they merely copy the existing laws relied upon by developed countries without adapting it properly to suit the country's peculiar circumstances.

This section of the chapter will attempt to look into some of the factors that aid and exacerbate the apathy of developing countries in taking serious decisive steps in the fight against cybercrime.

In examing some of these factors, this section will place more emphasis on, and will use Nigeria as a case study since Nigeria has not yet joined the league of highly-industrialised nations and is a clear example of countries that have taken few or no steps in fighting cybercrime.

Some of the major factors that contribute to the apathy of developing countries in fighting cybercrime can broadly be classified under regulatory or political factors and socio-cultural factors.[656] These factors will be addressed *ad seriatim*.

---

655 Vatis MA "The Council of Europe Convention on Cybercrime" in *Proceedings of a workshop on deterring cyberattacks: Informing strategies and developing options for US Policy* Papers delivered at Committee on Deterring Cyberattacks: Informing strategies and developing options for US Policy 10-11 June 2010, Washington DC, 207-226.

656 It will difficult to correctly state all the existing factors that contribute to the apathy of developing nations to be be identified as national values vary, but this thesis will only attempt to unravel the main factors.

2.6.1. REGULATORY/POLITICAL FACTORS

There are several regulatory/political factors that help create the apathy of most developing countries in the fight against cybercrime, and these factors directly or indirectly affect the various facets of formal and government institutions within a national jurisdiction. These factors affect and direct policies that govern cybercrime prevention, and they cut across legislative bodies, law enforcement bodies, government agencies that oversee the activities of the law enforcement bodies, and various regulatory agencies that direct the conduct of individuals, private organisations and public bodies in cyberspace within a select national jurisdiction.

In the case of developing countries with inefficient cybercrime prevention strategies, the implication is that the formal institutions are definitely weak in respect of its fight against cybercrime and cannot propel any meaningful activity in combating cybercrime. Thus "they lag behind the curve in enacting and enforcing cybercrime related regulative laws and have very little legislation specific to cybercrime and cyber-security".[657]

Some of the regulatory/political factors will be examined below.

2.6.1.1. ABSENCE OF ADEQUATE CYBERCRIME REPORTING AND PROPER DOCUMENTATION OF THE THREAT

A major way of keeping track of the rate of crime in any jurisdiction revolves around the statistics collated on the particular crime which will give the regulatory agencies an idea of the incidence of crime and steps that needs to be taken. Unfortunately, crime reporting in most developing countries, especially Nigeria, is almost non-existent and cybercrime is not left out. This loophole makes room for speculation about the rate of the crime and allows the government and other regulatory bodies to pretend that the

657 Kshetri N "Cybercrime and cybersecurity issues in the developing Pacific island economies: The current state, future prospects and policy measures" in *Harnessing disruption: Global, mobile, social, local* Papers delivered at 34th Annual Pacific Telecommunications Conference 15-18 January 2012, 1023-1051.

said crime is minimal and, therefore, is not a threat. This also gives the formal institutions the impression that developed countries are the only target of cybercriminal activities.

2.6.1.2. GOVERNMENT PRIORITY

Every government has its priorities with its major national problems on the top of its scale of preference. Government priorities rub off on other regulatory agencies, law enforcement agencies and legislative bodies. One of the major features of most developing countries is poverty, and most government policies in such jurisdictions are geared towards alleviating the menace of poverty and providing the basic necessities of life. In Nigeria, for example, the basic necessities of life – shelter, housing and food – still elude the majority of the populace.[658] Fighting cybercrime, therefore, will not be the main feature in such major government policies.

On the other hand, as is the case in most developing countries, the government sometimes decides to take some action with respect to cybercrime, criminalising some aspects of cybercrime. According to Schinder and Cross,[659] the government prioritises and decides the type of cybercrime that will be criminalised and fought based on a number of factors which will be looked into below.

2.6.1.2.1. EXTENT OF HARM

Schinder and Cross point out that cyber-criminal activities that involve violence or potential violence, especially to the vulnerable (for example sexual crimes against children), are normally of the highest priority,[660] while cyber-criminal activities against property that will result in substantial monetary loss will be of higher priority than cyber-

---

658 The Nigerian National Bureau of Statistics suggests that approximately 120 million Nigerians live below the poverty line of $1 a day. See Omoh G "How government impoverished Nigerians, poverty on rampage" http://www.vanguardngr.com/2012/02/how-government-impoverished-nigerians-poverty-on-rampage/ (Date of use: 31 March 2013).

659 Schinder DL and Cross M *Scene of the cybercrime* (Syngress Burlington 2008) 1-39.

660 Schinder and Cross *Scene* 28.

criminal activities that will result in a lesser monetary loss.[661] For example, in Nigeria, child pornography and advance fee fraud (a property crime that leads to a high monetary loss) were the existing cybercriminal offences that have been criminalised in Nigeria before the advent of the cybercime Act of 2015.

2.6.1.2.2. FREQUENCY OF OCCURRENCE

Schinder and Cross also point out that cyber criminal activities that frequently occur receive more attention than those that seldom occur.[662] The majority of advance fee fraud cases emanate from Nigeria and some also take place in Nigeria. Nigeria has gained prominence with advance fee fraud, now also called “419”, in line with section 419 of the Nigerian Criminal Code which prohibits advance fee fraud. In the Nigerian example, advance fee fraud thus gains more attention from government and law enforcement agencies with various legislative interventions channelled towards addressing the crime.

2.6.1.2.3. AVAILABILITY OF PERSONNEL

In the case of law enforcement agencies, cybercriminal activities that can be investigated by fewer detectives will receive more attention than activities that are sophisticated and require many investigators.[663] A look at the Nigerian situation reveals that advance fee fraud commands the attention of law enforcement agencies because, although somewhat complicated in its investigation, it is easier and requires fewer investigators compared to hacking, computer forgeries and many other cybercriminal activities.[664]

2.6.1.2.4. TRAINING OF PERSONNEL

The types of cybercrimes that are investigated within a national jurisdiction are largely dependent on the type of cybercrime that investigators are trained to deal with.[665] The

---

661 Schinder and Cross *Scene* 28.
662 Schinder and Cross *Scene* 28.
663 Schinder and Cross *Scene* 28.
664 This position has been highlighted while discussing the Nigerian legislative response and law enforcement initiatives.
665 Schinder and Cross *Scene* 28.

main cybercrime training given to Nigerian law enforcement agencies, such as the Economic and Financial Crime Commission (EFCC), revolves around investigations on advance fee fraud crimes.

2.6.1.2.5. JURISDICTION

Schinder and Cross also point out that the cybercrimes that are normally given preference to, are cybercriminal activities that affect the citizens of the nation in question because the government's responsibility first is to its citizens.[666] They further point out that even in cases where the national law enforcement agencies have international jurisdiction, they might be wary of spending its resources on crimes that cross jurisdictional boundaries.[667] In the Nigerian situation, the majority of advance fee fraud crimes are perpetrated by Nigerians and targeted mainly against citizens of developed countries, but Nigerian citizens also are targets of this crime.

2.6.1.2.6. DIFFICULTY IN INVESTIGATION

Another factor that may affect the government's priority in deciding which cybercrime deserves more attention is the difficulty in investigation and the likelihood of success.[668] Again looking at the Nigerian situation, investigating advance fee fraud, though difficult, is somewhat less complicated in its investigation when compared to some other genres of cybercrime, such as hacking, which may span various national jurisdictions. Mr Vijay Mukhi of the Indian Foundation of Internet Security and Technology pointed out that agents of the Indian police are averse to registering incidents of cybercrime as their prosecution can prove complicated.[669]

2.6.1.2.7. POLITICAL FACTORS

The consciousness of the political class also plays a major role in influencing the cybercrime that takes priority. These politicians make and also execute the law and influence the activities of the law enforcement agencies. In most developing countries,

---

666 Schinder and Cross *Scene* 28.
667 Schinder and Cross *Scene* 28.
668 Schinder and Cross *Scene* 28.
669 Messmer E "Ineffective law enforcement, bad economy fueling cybercrime" http://www.pcworld.com/article/155178/cybercrime_increasing.html (Date of use: 3 March 2013).

such as Nigeria, most individuals that dominate the political class belong to a certain age bracket (40years and above) and they have limited knowledge of the computer and its network and, therefore, do not appreciate the extent of the menace of cybercrime.[670]

Mukhi pointed out that Indian politicians and judges find cybercrime difficult to tackle chiefly because only a few of them use the internet.[671]

It is submitted that the major issue that revolves around the above-mentioned factors is the absence of the right statistics on cybercrime. This is so because the extent of harm, frequency of occurrence and other above-mentioned factors cannot really be determined in a jurisdiction where crime is rarely reported. When the crime is reported, it is not properly recorded to provide the government agencies and other regulatory bodies with the necessary information to determine the crimes that really hurt the economy of the country and the individuals.

2.6.1.3 STATE/GOVERNMENT ADVANTAGE

The proceeds of cyber-criminal activities may be beneficial to the government, economy or majority of the individuals in a national jurisdiction, and this can create some apathy in fighting IT crime by the relevant agencies. According to Yasin, being a cybercrime haven may sometimes be of benefit to a nation.[672] He further opined that in such cases, the criminals may hijack the legislative and political process through threats and bribes,

---

670 Computer penetration in Nigeria started in 2002 and by the time computer use became popular, the youth embraced the computer while most of the current political office holders, who can no longer be classified as youths, found it difficult to embrace the computer and its complexities. The internet society in Nigeria reported that many government offices do not have computers. This shows the level of computer ignorance in political circles. See Massari G "Internet as instrument to spring Nigeria into the millennium" http://www.isocnig.org.ng/News.html (Date of use: 3 March 2013).

671 Messmer E "Ineffective law enforcement, bad economy fueling cybercrime" http://www.pcworld.com/article/155178/cybercrime_increasing.html (Date of use: 3 March 2013).

672 Yasin M "Global nature of computer crimes and the convention on cybercrime" (2006) *Ankara Law Review* 129-142.

ensuring that the relevant laws to combat cybercrime are not enacted.[673] As also posited by Yasin, the country might decide to become a cybercrime haven in order to attract significant aid from developed countries.[674] Nations with such motives therefore will hope to receive large sums in the form of grants or aid to take part in the fight against cybercrime.[675]

It is also submitted that the funds or benefits generated from the proceeds of such crimes may be beneficial to the country that decides to allow itself to become a cybercrime haven. For example, information obtained from a hacked computer system from a developed country's security and law enforcement outfit (for example, the United States' CIA) may be beneficial to a developing country that has become a cybercrime haven which may be part of an espionage activity on the target country. Also, illegal funds which are the proceeds of a cybercriminal activity such as fraud will boost the economy of the nation that decides to become a cybercrime haven. This will undoubtably contribute to the apathy of the country which deliberately does nothing to fight electronic crime and allows its jurisdiction to become a cybercrime haven.

2.6.2. SOCIO-CULTURAL FACTORS

The social and cultural aspects of a country affect its response to the menace of cybercrime. These aspects relate to the ideologies, opinions and culture of the individuals that make up that jurisdiction and impact on their perceptions of issues and even criminal activities. For example, the socio-cultural dictates of the American society holds the idea of freedom of speech as an inalienable fundamental right while, in Thailand, insulting the King is a taboo and illegal.[676] Therefore, there are certain socio-

673 Yasin *Global nature* 2006 *Ankara LR* 130. For instance, some former nations of the Soviet Republic have become foremost *de facto* cybercrime havens. See Lewis BC "Prevention of computer crime amidst international anarchy" (2004) *American Criminal Law Review* 1353-1372.

674 Yasin *Global nature* 2006 *Ankara LR* 130. For example, the United States Department for State released the sum of $250,000 to facilitate the training of judges and prosecutors of East African nations. See http://www.state.gov/r/pa/prs/ps/2012/12/201786.htm (Date of use: 3 March 2013).

675 Yasin *Global nature* 2006 *Ankara LR* 130.

676 http://apt46.net/2013/01/18/thai-guy-convicted-of-insinuating-something-about-his-king/ (Date of use: 3 March 2013).

cultural factors that contribute to the apathy of developing countries in joining the fight against cybercrime.

Some of the socio-cultural factors will be examined.

2.6.2.1. CORRUPTION

Corruption[677] has become a way of life in most developing countries. According to Barr and Serra, "when the private returns to corruption are high or due to weak institutions the likelihood or consequences of detection are limited, individuals are inclined to act corruptly".[678]

The evils of corruption[679] wrongly impact on society at large and completely skew the entire country's justice and police system. The legislative response is wrongly impacted because the legislators are only interested in enacting laws that would protect them and promote their interests. For example, in Nigeria more stringent laws (such as capital punishment) that will deter kidnappers were enacted by states only when political office holders became targets of kidnapping. However, when foreigners and ordinary citizens were being kidnapped, the government and legislators did not deem it necessary to make the crime of kidnapping a capital offence.[680]

---

677 Serra and Barr describe corruption as a cultural concept. See Serra D and Barr A "Culture and corruption" http://economics.ouls.ox.ac.uk/14043/1/gprg-wps-040.pdf (Date of use: 3 March 2013).

678 Serra and Barr http://economics.ouls.ox.ac.uk/14043/1/gprg-wps-040.pdf (Date of use: 3 March 2013).

679 Corruption normally is mostly borne out of societal values, the absence of moral rectitude, and customs and beliefs.

680 See Ezugwu BN "Law on kidnapping: Matters arising" http://www.gamji.com/article8000/NEWS8473.htm. See also Iferi B "New law gives life jail term to kidnappers" http://www.dailytimes.com.ng/article/new-law-gives-life-jail-term-kidnappers (Date of use: 3 March 2013).

The law enforcement agencies are also affected because funds meant for their training and technological advancement are squandered by a few individuals and this will definitely adversely affect the success of investigations.[681]

The law enforcement agencies are also tempted to compromise their investigations which will entail that only petty cybercriminals who cannot compromise law enforcement agents are apprehended and prosecuted.[682] The judiciary therefore will not have the right legislation and proper evidence to convict a cyber-criminal. The executive arm of government on its part does not get its priorities right while making policies that will enrich the few in government.[683]

2.6.2.2. ICT PENETRATION

The level of ICT penetration in developed countries is higher than that of developing countries.[684] In developed countries, virtually all businesses have their presence on the cyberspace. On the other hand, businesses in developing countries have a lesser presence in cyberspace. This social factor is still prevalent as a result of a lack of awareness about the benefits of the internet and how businesses can be enhanced through same; the fear that the internet is not secure; the ignorance of many private organisations or businesses that are wary of relying on newer technology to advance their businesses since they are used to their traditional way of doing business; the low quality of service from internet service providers; and lack of adequate electricity to power ICT equipment.[685] This social factor gives the government the impression that businesses with a presence on cyberspace are mainly foreign businesses and should be protected by their own countries.

---

681 For example, see http://www.hrw.org/world-report/2013/country-chapters/nigeria (Date of use: 19 October 2014).

682 Fakoya G "The police and the Nigerian public" http://saharareporters.com/2012/02/16/police-and-nigerian-public (Date of use: 19 October 2014).

683 Obamwonyi SE and Aibieyi S "Public policy failures in Nigeria: Pathway to underdevelopment" (2014) *Public Policy and Administration Research Journal* 38-42.

684 http://www.itu.int/net/pressoffice/press_releases/2013/05.aspx#.VESyyVPlxnY (Date of use: 19 October 2014).

685 Chinn MD and Fairlie RW "ICT use in the developing world: An analysis of differences in computer and internet penetration" (2010) *Review of International Economics* 153-167.

Also since ICT penetration in developing countries is lower than that of developed countries, the level of cybercriminal incidents in developing countries will definitely be lower, giving the impression that cybercrime is lower in developing countries without the government considering the level of ICT penetration within its jurisdiction in relation to the cybercrime incidents. This factor also limits the level of pressure that will be mounted on government agencies by these private businesses to ensure that the government takes the right steps to ensure that cybercrime is combated within its national jurisdiction.

2.6.2.3. ATTACKS ON DEVELOPED COUNTRIES

Cybercrime attacks are mostly targeted at developed economies with some attacks emanating from developing countries.[686] The attraction to attack the computer infrastructures in developed countries from developing countries stems from the fact that it is more lucrative to do so since their economy is better and there are wealthier people to be defrauded than in developing countries. This factor, however, gives the impression that developing countries are not susceptible to cybercrime attacks and in cases where they are attacked, these are only minimal. This contributes to the apathy of developing countries in joining the fight against cybercrime.

2.6.2.4. NATIONAL AFFINITY

There is the cultural affinity that exists between individuals in a country which causes cyber-criminals to prefer to attack nationals of another country than fellow nationals.[687] The cultural concept that it is better to defraud a foreigner than a fellow countryman

686 http://mac-antivirus-software-review.toptenreviews.com/the-geography-of-cybercrime.html (Date of use: 19 October 2014).

687 For example, some Russians in a show of patriotism send botnets developed by a Russian programmer to nationals of the United States and other countries that imposed sanctions on Russia for supporting separatists fighting the Ukraine government. See Kovacs E "Cybercriminals use patriotic Russians to revive Kelihos botnet" http://www.infosecisland.com/blogview/23951-Cybercriminals-Use-Patriotic-Russians-to-Revive-Kelihos-Botnet.html (Date of use: 19 October 2014).

exacerbates the incidence of cybercrime targeted at nationals of other countries. This cultural factor makes government agencies believe that its national jurisdiction is safe from major cybercrime attacks, and they will therefore not make concerted efforts to combat cybercrime.

2.6.2.5. VICTIMS UNWILLINGNESS TO REPORT CYBERCRIME

Having the correct statistics on cyber-criminal incidents helps the government to decide which offensive conducts to criminalise.[688] This will also enable the law enforcement agencies to determine the cyber-criminal activities that would have more resources channelled towards in order to tackle IT crime. Thus, where there is an unwillingness to report cybercrime activities by victims of such activities, this will lead to apathy to tackle cybercrime by the relevant government agencies.

The unwillingness to report cybercriminal activities may be as a result of:

- **LACK OF AWARENESS OF THE NECESSARY STEPS TO TAKE IN REPORTING CYBERCRIME**.

- **LONG HISTORY OF UNSOLVED CRIME**: In most developing countries, crimes are seldom solved and this leads to the belief that reporting crimes is useless since in most cases the culprits will never be brought to book. There is also the fear that the victim of the crime may be accused of being the perpetrator of the crime or information on the crime report by the victim leaked to the perpetrator and the victim is put in danger of a reprisal attack.[689]

This attitude has become entrenched in societies where crimes are normally left unsolved, the law enforcement agents are corrupt and the victim of the crime can become a target of a violent attack once the perpetrator of the crime becomes aware

---

688 Verton D "FBI chief: Lack of incident reporting slows cybercrime fight" http://www.computerworld.com/article/2578278/cybercrime-hacking/fbi-chief--lack-of-incident-reporting-slows-cybercrime-fight.html (Date of use: 19 October 2014).

689 Ladapo OA "Effective investigations, a pivot to efficient criminal justice administration: Challenges in Nigeria" (2011) *African Journal of Criminology and Justice Studies* 79-94.

that the victim reported the criminal act to the law enforcement agency.[690] As also observed by Ladapo, the law enforcement agencies often require a victim that reports the crime to fund the investigation while making numerous visits to the law enforcement agency's office for flimsy reasons, leading to a substantial loss of manhours.[691]

- **SUPERSTITIOUS BELIEFS**: A cultural factor prevalent in most developing countries such as Nigeria is the superstitious inclination of individuals which includes computer users. Individuals are highly superstitious and allow their security to be governed by providence.[692] Computer users do not believe that they can be victims of cybercrime and, therefore, do nothing to protect themselves from harm.[693] Unfortunately, when they become the targets of cyber-criminal activities, victims do not bother to complain to the appropriate agencies as they believe that a complaint will not resolve the damage.[694]

CONCLUSION

In conclusion, this chapter has demonstrated that although the menace of cybercrime has become more eminent, most developing countries are lagging behind in taking decisive steps to address the menace of IT crime. In establishing this, the chapter analysed the legislative responses of developed countries using the United Kingdom and United States of America as case studies, and compared same with the legislative responses of developing countries using Nigeria, South Africa and India as case studies. The chapter also considered the law enforcement initiatives and capabilities of both the developed and developing countries under review, in order to find out how equipped they are in addressing the menace of cybercrime. In considering the law

690 Ladapo *Effective investigations* 2011 *African JCJS* 81.
691 Ladapo *Effective investigations* 2011 *African JCJS* 81.
692 Gragido W, Molina D, Pirc J and Selby N *Blackhatonomics: An inside look at the economics of cybercrime* (Syngress Burlington 2012) 5-6.
693 During this research, inquiries made by the researcher from computer users in Nigeria revealed that most of the users simply do not believe that they can be victims of cybercrime.
694 Law enforcement agencies in developing countries usually are accused of corruption and inefficiency in their operations, prompting victims of crime rarely to complain but rather to lick their wounds.

enforcement capabilities of the countries used as case studies, the chapter analysed the funding, staff resources, technological resources, training and education of the developed and developing countries under review in this discourse**.**

The chapter showed that the level of commitment to the fight against the menace of cybercrime varies between nations depending on the level of socio-economic development attained by that nation. Invariably, addressing the issue of crime is tied to the socio-economic development of a country. Thus, developing countries that have not yet joined the league of highly-industrialised nations are doing little or nothing to tackle internet crime within their jurisdictions, especially with respect to their legislative responses and law enforcement initiatives.

This chapter in considering the extent of the involvement of developing countries in tackling the menace posed by cybercrime also considered the factors that impede the active participation of developing nations in taking decisive steps in joining the fight against cybercrime. The chapter comparatively analysed the legislative responses and law enforcement initiatives of select developed and developing countries and showed that although developed countries are miles ahead of developing countries in taking effective steps in tackling cybercrime a lot of work still needs to be done even by the developed countries.

This chapter further considered the nature of the apathy of developing countries in effectively addressing the menace of cybercrime. The chapter then highlighted some factors that exacerbate the apathy of most developing countries in addressing the issue of electronic crime. Chapter 5 of this research will further consider in more details the socio-economic factors that cause the apathy of developing countries in addressing cybercrime and then proffer some socio-economic steps that will elicit the participation of developing countries in addressing cybercrime.

It is therefore imperative that on one hand, developed and developing countries should take decisive steps in eliminating the various inadequacies that still obstruct their fight against cybercrime. On the hand, developing countries must in addition, address the various issues that exacerbate their apathy in dealing with cybercrime with developed

countries lending a helping hand in nipping these issues in the bud rather than playing the ostrich.

The next chapter – chapter 3 will make a case for the evolution of a specialised and harmonised legislation that will accommodate the participation of developing countries in addressing cybercrime. The chapter will highlight the need for and also propose a common taxonomy that will lead to the development of the harmonised legislation.
The chapter will also proffer a number of principles and steps that should be taken in evolving the said harmonised legislation that will forestall any setback in achieving a harmonised legislation. Subsequent chapters - chapter 5 (5.2.) in this research will try to proffer solutions to the apathy of most developing countries in addressing the issue of cybercrime.

CHAPTER 3

EVOLVING A SPECIALISED AND HARMONISED LEGISLATION THAT ACCOMMODATES THE PARTICIPATION OF DEVELOPING COUNTRIES IN ADDRESSING CYBERCRIME: A COMPARATIVE ANALYSIS

INTRODUCTION

The dangers posed by the prevalence of cybercrime are not felt by developed countries alone, but developing countries and its citizens are also victims of the threat. Thus, the global nature of the threat of cybercrime dictates that any legislative initiative that must tackle the dangers of cybercrime has to be a global legislative initiative requiring global cooperation.[695] Several scholars have called for a globally harmonised cybercrime legislation that will be spearheaded by a worldwide organisation, preferably the United Nations.[696]

Unfortunately, evolving a regional or national cybercrime legislation has been easier than creating a global harmonised cybercrime legislation to tackle a global problem which the existing national/regional legislative initiatives have been unable to tackle adequately. For instance, in 2010 a proposal for the emergence of a global cybercrime treaty was rejected by the UN when there was disagreement between Russia, China

695 Harley B "A global convention on cybercrime?" http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/ (Date of use: 14 July 2013).

696 Li X "International actions against cybercrime: Networking legal systems in the networked crime scene" http://www.webology.org/2007/v4n3/a45.html (Date of use: 14 July 2013).

and a few developing countries, on the one hand, and the United States, the United Kingdom, Canada and the European Union, on the other.[697]

This chapter observes that the apparent divergence in the various existing cybercrime taxonomies[698] and legislations contributes to the growing menace of computer crime. This chapter also posits that reliance on national or regional legislative initiatives to tackle a global threat is inadequate and only a global legislation will adequately address the impact of cybercrime.

The chapter also highlights some differences in cybercrime taxonomies and legislations between nations and identifies the inherent disadvantages these differences pose in forming a unified front by various countries in the fight against cybercrime.[699] The chapter suggests the use of a common taxonomy to address the issue of cybercrime.[700] The chapter also focuses on the need for harmonised cybercrime legislation and analyses the various steps already taken by international and regional bodies to create a harmonised cybercrime treaty and the attendant failures. The chapter concludes with a proposal for a harmonised legislation and proffers necessary steps that will lead to the proposal coming to fruition.

3.1. THE NECESSITY OF A COMMON TAXONOMY

Walden pointed out that the purpose of taxonomy is to provide a framework to effectively analyse various types of criminal activities present in cyberspace.[701] The clearly different interpretations and definitions of the nature and classification of what amounts to information technology crime have led to a wide range of divergent

697 Masters G "Global cybercrime treaty rejected at UN" http://www.scmagazine.com/global-cybercrime-treaty-rejected-at-un/article/168630/ (Date of use: 14 July 2013).

698 Taxonomies refer to a scheme of classification into named groups. See http://www.thefreedictionary.com/taxonomy (Date of use: 27 September 2014).

699 The issues presented by the divergence in taxonomies were dealt with in chapter 1 of this work.

700 For example, in creating taxonomy, the computer can viewed from the role it played in the commission of a crime, for instance the computer as a target of the crime or the tool used in perpetrating the crime.

701 Walden I *Computer crimes and digital investigations* (Oxford University Press Oxford 2007) 16-17.

classifications and a cacophony of answers to the attendant menace of e-crime. As a result of the varying taxonomies, an activity that will amount to a computer crime will be dependent on the classification that the activity falls under, and this varies across jurisdictional precincts. Jurisdictional boundaries therefore, will determine cyber activities that would amount to criminal activities.

For example, the Australian High-Tech Crime Centre classified e-crime under two categories, namely, computer-enabled crime and computer-enhanced crime.[702] Carter classified cybercrime as computer as target; computer as instrumentality; computer as an incidental to other crime; and crime connected with the prevalence of a computer.[703] Parker[704] classified high-tech crime as an activity where the computer is the object of the crime,[705] or the computer is the subject of the crime,[706] or the computer is used as a tool for executing or planning the crime,[707] or where the symbol of the computer can be used to deceive or intimidate.[708] The US Department of Justice, for its part, classified cybercrime as a criminal activity where the computer is the target of the activity or where the computer is used as a weapon in committing an offence or where the computer is an accessory.[709] Oates classified cybercrime as virtual, hybrid and augmented traditional crimes.[710]

The G8 summit[711] has classified cybercrime in terms of threats and thus categorised e-crime into computer infrastructure attacks[712] and computer-assisted threats.[713] In a bid

---

702 http://www.afp.gov.au/~/media/afp/pdf/f/fighting-the-invisible.ashx (Date of use: 14 July 2013).

703 Axelrod EM *Violence goes to the internet: Avoiding the snare of the net* (Charles C Thomas Publishers Springfield 2009) 5-16.

704 Casey E *Digital evidence and computer crime: Forensic science, computers and the internet* (Elsevier Waltham 2011) 35-48.

705 For example, when the computer itself is stolen or destroyed. See Casey *Digital evidence* 40.

706 For example, when the computer is attacked by a virus. See Casey *Digital evidence* 40.

707 For example, using a computer to hack into another computer or network. See Casey *Digital evidence* 40.

708 For example, where the existence of a computer system is used to deceive individuals about the ability to perform a certain task, thereby extorting the individuals who are now under a mistaken belief. Casey *Digital evidence* 40.

709 http://www.cybercitizenship.org/crime/crime.html (Date of use: 31 March 2012).

710 Fafinski S, Dutton B and Margetts H "Mapping and measuring cybercrime" www.law.leeds.ac.uk/assets/files/staff/FD18.pdf (Date of use: 31 March 2013).

711 http://www.mofa.go.jp/policy/i_crime/high_tec/conf0105-6.html (Date of use: 14 July 2013).

to be comprehensive, these classifications sometimes omit some aspects or types of cybercrime which then cannot be classified under the taxonomy provided by the proponent. For instance, although the classification provided by the CoE Convention on Cybercrime is broad, the classification by the Convention leaves out offences such as identity theft.[714] Also relying only on the UN classification of cybercrime, which classified cybercrime into cybercrime in a narrow sense (computer crime) and cybercrime in a broad sense (computer-related crime),[715] crimes such as copyright infringement and online bullying will then be excluded from being criminalised.[716]

Having a consistent taxonomy is essential in fighting e-crime as it will enhance crime reporting, collaborative working among agencies, knowledge sharing and ease in communication between law enforcement agencies.[717] It will also enhance consistent interpretation and consistent best practices among law enforcement agencies irrespective of jurisdictional boundaries or constraints since the consistent classification will highlight the similar characteristics.[718] This will enable agencies to have a clear measurement on the impact of cybercrime across jurisdictions in order to take appropriate steps to tackle the crime.

The absence of a common taxonomy will hamper knowledge sharing and crime reporting on the extent of cybercrime, and will endanger international cooperation in

---

712 Computer Infrastructure attack covers operations to disrupt, deny, degrade or destroy the information resident in computers and computer networks, or the computers and networks themselves. This would cover malicious acts, unauthorised access, theft of service and denial of service. See also Alkaabi A *et al* "Dealing with the problem of cybercrime" in Baggili I (ed) *Digital forensics and cyber crime* (Springer Heidelberg 2011) 1-18.

713 Computer-assisted threat will cover malicious activities such as fraud; drug trafficking; money laundering; infringements of intellectual property rights; child pornography; hoaxes; the gathering of information; and illegal copying of data which is facilitated by the use of a computer. The computer is used as a tool in the commission of these offences/threats. Alkaabi *et al Dealing with the problem of cybercrime* 6.

714 See Council of Europe Convention on Cybercrime, 2001 ETS No 185. See also Alkaabi *et al Dealing with the problem of cybercrime* 4.

715 http://cyber-law-web.blogspot.com/2009/07/united-nations-definition-of-cybercrime.html (Date of use: 3 March 2012).

716 Alkaabi *et al Dealing with the problem of cybercrime* 5.

717 Alkaabi *et al Dealing with the problem of cybercrime* 5.

718 Maidment M "Taxonomies in the public sector" http://www.nglis.org.uk/tips/tipsben.htm (Date of use: 14 July 2013).

addressing the menace of cybercrime. For instance, Broadhurst has pointed out that in many jurisdictions where e-crime is reported, law enforcement agencies are unable to differentiate e-crime from other fraud reports, commercial crimes, criminal damage statistics or other categories of criminal offences, thus making the extent of IT crime uncertain.[719]

The UN pointed out that the absence of consensus on the legal definitions of criminal conduct, categories of activity that would amount to cybercrime and harmonisation of national procedural laws that govern cybercrime investigations, hampers international cooperation in addressing Cybercrime.[720] A consistent taxonomy will easily lead to harmonised cybercrime legislation.

3.1.1. PROPOSING A COMMON TAXONOMY

The mode of classification that several researchers and agencies rely upon to classify cybercrime is dependent on certain factors as perceived by the researcher or the agency proposing the classification. For instance, the mode of classification may be dependent on the role of the computer system in the commission of the crime, or on the perpetrators of the offence. Thus, when the definition is perceived from the role the computer system played in the commission of the crime, cybercrime can then be classified as computer-enabled crime and computer-enhanced crime,[721] or as crimes perpetrated using computers and traditional crimes facilitated through the use of computers.[722]

719 Broadhurst R "Developments in the global law enforcement of cyber-crime" 2006 *International Journal of Police Strategies and Management* 408-433.

720 http://www.uncjin.org/Documents/EighthCongress.html (Date of use: 14 July 2013).

721 This is the classification as posited by the Australian High-Tech Centre. See http://www.afp.gov.au/~/media/afp/pdf/f/fighting-the-invisible.ashx (Date of use: 14 July 2013).

722 This is the classification as posited by Foreign Affairs and International Trade of Canada. See Alkaabi *et al Dealing with the problem of cybercrime* 4.

On the other hand, a proponent may classify cybercrime in terms of the threat such offence poses. In that case, cybercrime may then be classified as a computer infrastructure attack and computer-assisted threat.[723]

It is submitted that the best mode of classifying cybercrime should be based on the role of the computer system in the commission of the offence. This is in line with the researcher's earlier definition of cybercrime as "any crime where the computer or network is used to aid the commission of the crime or where the computer, network or data is the target of the crime". This classification should be coined in a broad sense so as to accommodate all forms of cybercrime plaguing various jurisdictions that are currently in existence, and to make room for new genres of crime that may be created in future. This will remove the need for reclassification upon the emergence of new offences.

In creating a common taxonomy, this research will adapt the format provided by Alkaabi *et al*,[724] because similar to this research's objective of creating a taxonomy based on the role of the computer system in the commission of an offence, it also creates its taxonomy based on the role of the computer system. Computer crime will therefore in this thesis be divided into two categories and classified as Role I and Role II.[725] This classification or roles will be classified broadly and then further subdivided into smaller sub-groups or categories.[726] This will ensure that any cyber-criminal offence can fall under a sub-group or category which is under either Role I or Role II.

Role I computer crimes are committed when the computer or network is used to aid the commission of the crime (or is the tool). Under this classification, four sub-categories of offences will be grouped under it. These include the following:

---

723 This is the classification posited by the G8 Summit. See http://www.mofa.go.jp/policy/i_crime/high_tec/conf0105-6.html (Date of use: 14 July 2013).

724 Alkaabi *et al Dealing with the problem of cybercrime* 5-8.

725 Alkaabi *et al Dealing with the problem of cybercrime* 5-8.

726 The sub-classifications in this section will be adapted from some of the terms used in the Council of Europe Convention on Cybercrime, 2001 (ETS 185).

i content violation offences:[727] offences such as child pornography, hate crimes and forgery fall in this sub-category;

ii unauthorised modification of data:[728] the offences of identity theft and online fraud fall in this sub-category;[729]

iii misuse of information technology devices:[730] criminal activities such as spamming,[731] cyber-stalking,[732] harassment,[733] threats,[734] cyber-homicide,[735] cyber-terrorism, money-laundering, phishing and several other traditional crimes perpetrated with the aid of the computer or its networks will fall under this sub-category;[736]

iv piracy and copyright infringement.[737]

The category Role II cybercrime encompasses crimes where the computer, network or data is the target of the crime. Under this classification also, four sub-categories of offences will be grouped under it.[738]

i illegal access offences:[739] hacking, computer sabotage, computer espionage falls in this sub-category;[740]

---

727 Council of Europe Convention on Cybercrime, 2001 (ETS No 185) Explanatory Report. See also Alkaabi *et al Dealing with the problem of cybercrime* 6.

728 Clifford RD (ed) *Cybercrime: The investigation, prosecution and defense of a computer-related crime* (Carolina Academic Press Durham 2011) 15-38. See also Alkaabi *et al Dealing with the problem of cybercrime* 6.

729 http://www.uncjin.org/8th.pdf (Date of use: 25 December 2013). See also Alkaabi *et al Dealing with the problem of cybercrime* 6.

730 Alkaabi *et al Dealing with the problem of cybercrime* 6.

731 Clifford *The investigation, prosecution and defense of a computer-related crime* 34.

732 Clifford *The investigation, prosecution and defense of a computer-related crime* 34.

733 Clifford *The investigation, prosecution and defense of a computer-related crime* 34.

734 Clifford *The investigation, prosecution and defense of a computer-related crime* 34.

735 Brenner SW "State cybercrime legislation in the United States of America: A survey" 2001 *Richmond Journal of Law and Technology* 28-36.

736 See also Alkaabi *et al Dealing with the problem of cybercrime* 6.

737 See Council of Europe Convention on Cybercrime, 2001 (ETS No 185) Explanatory Report.

738 Alkaabi *et al Dealing with the problem of cybercrime* 6.

739 http://www.uncjin.org/8th.pdf (Date of use: 25 December 2013). See also Alkaabi *et al Dealing with the problem of cybercrime* 6.

740 Alkaabi *et al Dealing with the problem of cybercrime* 6.

ii malicious code offences:[741] the offences of dissemination of viruses, worms and other malicious codes that will destroy or alter the data in a computer system will fall in this sub-classification;[742]

iii interruption of service offences:[743] denial of service attacks and similar attacks will fall under this category;[744]

iv theft or misuse of service offences:[745] computer theft, information theft, software theft, computer hardware theft and several thefts where the computer system is the target of the offensive activity will fall under this category;[746] the misuse of another person's internet domain name or internet account will also fall in this sub-category.[747]

These classifications and the examples are not sufficiently extensive to cover every known facet of existing cybercriminal activities; rather it provides a springboard for a comprehensive classification of all forms of cyber-criminal activities which presently exist and those that will emerge in the near future. As pointed out by Alkaabi,[748] in the case of several offences the computer may play dual roles (that is, as the target of the offence or the tool in the commission of the offence), thus implying that an offence may fall into the two existing taxonomies or roles posited. For example, online fraud can fall within both taxonomies; where the perpetrator uses a computer system to hack into a bank's computer system to move funds from different accounts or perform other fraudulent activities. In that case, the first computer system is used as the tool in aiding the commission of the offence while the second computer (the bank's computer system) is the target of the criminal activity.

---

741 Clough J *Principles of cybercrime* (Cambridge University Press Cambridge 2010) 120-130. See also Alkaabi *et al Dealing with the problem of cybercrime* 6.

742 Alkaabi *et al Dealing with the problem of cybercrime* 6.

743 Nemerofsky J "The crime of "interruption of computer services to authorized users". Have you ever heard of it?" 2000 *Richmond Journal of Law and Technology.* See also Alkaabi *et al Dealing with the problem of cybercrime* 6.

744 Nemerofsky 2000 *Richmond JLT*. See also Alkaabi *et al Dealing with the problem of cybercrime* 6.

745 Alkaabi *et al Dealing with the problem of cybercrime* 6.

746 Brenner 2001 *Richmond JLT* 28.

747 Koenig D "Investigation of cybercrime and technology-related crime" http://www.neiassociates.org/cybercrime-and-technology/ (Date of use: 27 December 2013). See also Alkaabi *et al Dealing with the problem of cybercrime* 6.

748 Alkaabi *et al Dealing with the problem of cybercrime* 6.

Although in the view of scholars such as Sommer the creation of a taxonomy is an artificial and pointless exercise,[749] it is however submitted that based on the highlighted benefits of establishing a taxonomy, e-crime should be classified broadly into two categories -based on the role the computer system or network plays in the commission of the cyber-criminal activity (computer-enabled crime) or where the computer is the tool in the commission, and where the computer is the target of the offence.

3.2. THE NEED FOR A HARMONISED CYBERCRIME LEGISLATION

In addressing divergent national cybercrime legislations, it is evident that a nation's interest in criminalising certain cyber-criminal activities should not be for the protection of its citizens or individuals within its national borders alone, since cyber-criminal activities are not confined within national boundaries.[750] Cybercriminals exploit the gap in the divergent national legislations to perpetuate their nefarious activities, and in some cases law-abiding citizens may be obeying their national laws but violating the laws of another country because of the divergent legislations.

The nature of cybercrime which erodes the principles of sovereignty and jurisdiction makes it imperative that, in order to properly address the menace of cybercrime, a transnational consistency in legislation holds an important key.

According to Brenner *et al*, one way of achieving this consistency is by the creation of a single code of legislation that would govern the commission of cybercriminal activity anywhere in the world.[751] This single piece of legislation will have to be agreed upon by the various national authorities.[752] However, Brenner *et al* were quick to point out that nations normally are not inclined to give up their national legislations in favour of

749 Fafinski S, Dutton WH and Margetts H "Mapping and measuring cybercrime" www.law.leeds.ac.uk/assets/files/staff/FD18.pdf (Date of use: 28 December 2013).

750 Brenner S and Goodman M "Cybercrime: The need to harmonize national penal and procedural laws" http://www.isrcl.org/Papers/Brenner.pdf (Date of use: 14 July 2013).

751 Brenner and Goodman http://www.isrcl.org/Papers/Brenner.pdf (Date of use: 14 July 2013).

752 Brenner and Goodman http://www.isrcl.org/Papers/Brenner.pdf (Date of use: 14 July 2013).

international legislation. This is so because giving up one's national legislation resembles giving up a nation's identity and is an affront to the nation's sovereignty.

Brenner *et al* also suggested the creation of a set of regulatory codes or laws that adequately cover all facets of high-tech crime which countries can adopt in enacting its cybercrime legislation.[753] Broadhurst agrees that having legislative consensus is the best strategy for the suppression of e-crime, but also pointed out that achieving a strict enforcement agenda is not feasible.[754] He also fears that over-regulation could stifle commercial and technological development.[755]

It is submitted that having a harmonised e-crime legislative framework holds an important key in addressing the menace of information technology crime. This legislative code can simply be ratified by nations or where a country already has its national legislative framework in place, the country will be obligated to update its legislation to be in alignment with the global harmonised legislative code. This is so because in the first place, a harmonised global legislative framework addresses inconsistencies in the criminalisation of offensive conduct and eliminates the emergence of safe havens.[756] For example, where conduct is criminalised in a certain jurisdiction and the same conduct is not criminalised in another jurisdiction, the second jurisdiction becomes a lucrative safe haven for offenders who perpetrate such activities. These safe havens will frustrate the efforts of law enforcement agencies since the ubiquitous nature of the internet still makes them susceptible to the criminal activities of offenders who are protected by the laxity of the legal framework in the "safe haven".

On the other hand, a harmonised global legislative framework will enhance international cooperation in dealing with e-crime. Bande points out that uniformity in the legislative

753 Brenner and Goodman http://www.isrcl.org/Papers/Brenner.pdf (Date of use: 14 July 2013).
754 Broadhurst 2006 *International JPSM* 408-433.
755 Broadhurst 2006 *International JPSM* 408-433.
756 Bande LC "The making of cybercrime legislation in Malawi: A comparative analysis of Malawi's proposed cybercrime law against international standards and best practices" https://lirias.kuleuven.be/bitstream/123456789/404618/1/The+Making+of+Cybercrime+Legislation+in+Malawi+Pdf.pdf (Date of use: 12 September 2013).

framework enhances the cooperation of varying jurisdictions in tackling crime,[757] since the principles of reciprocity[758] and double criminality[759] are the main pivots driving international cooperation in criminal jurisprudence and extradition of offenders.[760] Bande further points out that it is impracticable for nations to cooperate in addressing crime where there is disharmony among the nations on the criminal nature of the offending activity or the punishment to be attached to such activity.[761] It is submitted that Bande's assertion is tenable.

Therefore, the ubiquitous nature of the internet dictates that evolving a harmonised global cybercrime legislative framework is essential to ensure international cooperation in addressing the menace of cybercrime and is a veritable step that must be taken if the growth and attendant problems associated with e-crime are to be nipped in the bud.

The following sub-topics of this chapter will consider the emergence of harmonised cybercrime legislation.

3.2.1. JOURNEY TO A UNIFIED CYBERCRIME LEGISLATION

The various initiatives embarked upon by several countries in enacting and further updating their national legislation on e-crime have yielded quite some results. For example, the US Department of Justice reports that between the years 2006 and 2010, approximately 1,177 persons were convicted and sentenced for various cyber-criminal

---

757 Bande https://lirias.kuleuven.be/bitstream/123456789/404618/1/The+Making+of+Cybercrime+Legislation+in+Malawi+Pdf.pdf (Date of use: 12 September 2013).

758 Ambos K "The International Criminal Court and the traditional principles of international cooperation in criminal matters" in Takamaa K and Koskenniemi M (eds) *The Finnish yearbook of international law 1998* (Kluwer Law International Hague 2000) 413-425.

759 Ambos *Traditional principles* 413.

760 Rezek JF "Reciprocity as a basis of extradition" (1982) *British Yearbook of International Law* 171-203. See also Bande https://lirias.kuleuven.be/bitstream/123456789/404618/1/The+Making+of+Cybercrime+Legislation+in+Malawi+Pdf.pdf (Date of use: 12 September 2013).

761 Bande https://lirias.kuleuven.be/bitstream/123456789/404618/1/The+Making+of+Cybercrime+Legislation+in+Malawi+Pdf.pdf (Date of use: 12 September 2013).

activities.[762] In South Africa, the Deputy Minister of Justice reports that a 97.6 per cent success rate in cybercrime prosecutions has been achieved,[763] and the Economic and Financial Crimes Commission of Nigeria reveals that it has recovered over $170 million, intercepted over 12,000 scam e-mails, and secured over 300 convictions.[764]

However, the problem of jurisdiction and the inconsistencies in legislations have been a barrier to a more effective fight against cybercrime. The desired zenith has not been attained. For example, a study conducted by Norton reveals that in 2012, 1.5 million persons were victims of cybercrime resulting in a cost of about US $110 billion over a period of 12 months. [765] This has increased to about 700 millon victims while the cost is projected to get to $6 trillion by 2021,[766] thus implying that existing global efforts have not yet scratched the surface.

Several countries, regional bodies and international agencies have taken various steps to provide a unified or consistent cybercrime legislation that will address the gaps created by the inconsistencies in cybercrime legislation within their sphere of influence. Some of the steps taken towards achieving some level of consistency in e-crime legislation by some international and regional bodies are examined below.

3.2.1.1. UNITED NATIONS

The UN, as the international body saddled with the responsibility of engendering the promotion of global peace, has taken several steps in providing various strategies that

---

762 Marcum CD, Higgins GE and Tewksbury R "Doing time for cyber crime: An examination of the correlates of sentence length in the United States" (2011) *International Journal of Cyber Criminology* 824-835.

763 Rademeyer J "Conviction rates an unreliable benchmark of NPA success" http://africacheck.org/reports/conviction-rates-an-unreliable-benchmark-of-npa-success/ (Date of use: 29 December 2013).

764 Kshetri N "Cybercrime and cybersecurity in sub-Saharan African economies" in *Cybercrime and cybersecurity in the global south* (Palgrave Macmillan Hampshire 2013) 152-170.

765 http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02 (Date of use: 29 December 2013).

766 O'Driscoll A "100+ terrifying cybercrime and cybersecurity statistics and trends (2018 edition)" https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/#gref (Date of use: 29 September 2018).

would create some harmony in national cybercrime legislations. The UN General Assembly[767] has come up with a number of resolutions to initiate the enactment of consistent cybercrime legislations across member states. For example, in 1985 the UN passed Resolution 40/71 requesting governments and international organisations to "take action, where appropriate, in conformity with the Commission's recommendation so as to ensure legal security in the context of the widest possible use of automated data processing in international trade".[768] The UN Commission on International Trade Law (UNCITRAL) further requested governments to take steps to review their legal rules in relation to the use of computer records as evidence during trials and to ensure such rules are consistent with current technological trends.[769]

Resolution 55/63 of the UN General Assembly[770] stipulated that the laws and practice of member states should be modelled to eliminate safe havens for cyber-criminals; law enforcement agencies should cooperate in their investigation and prosecution of cyber-criminal activities; and member states' legal systems should be modelled to "protect the confidentiality, integrity, and availability of data and computer systems from unauthorised impairment". The Resolution also requires states to protect individuals' freedom and privacy, and make individuals aware of the need to prevent and fight cybercrime while mandating governments to increase its capacity to combat cybercrime.[771] In a bid to engender some level of legislative consistency, Resolution 56/121 further encourages member states to consider the work and policies of other

---

767 The resolutions of the United Nations General Assembly are not legally binding on member states, although they can lead to legally-binding conventions and treaties. See http://www.un.org/cyberschoolbus/untour/subgen.htm (Date of use: 21 July 2013).

768 http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/477/78/IMG/NR047778.pdf?OpenElement (Date of use: 24 July 2013). See also "United Nations Commission on International Trade Law, Yearbook: 1985 Vol XVI" (United Nations Publication 1988) 47.

769 http://www.uncitral.org/pdf/english/texts/electcom/computerrecords-e.pdf (Date of use: 2 August 2013).

770 Resolution 55/63 of 4 December 2000 on combating the criminal misuse of information technologies. See http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf (Date of use: 21 July 2013).

771 http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf (Date of use: 21 July 2013).

international or regional organisations when developing its national laws, policies and practices that will address cybercrime.[772]

Several UN institutions such as the International Telecommunication Union (ITU) and United Nations Office on Drugs and Crime (UNODC) have also taken some initiatives towards propelling the harmonisation of cybercrime legislations among UN member states. The ITU brought together a High-Level Experts Group (HLEG) upon the launch of the Global Cyber-Security Agenda (GCA), to provide a platform that will create a framework for global discourse and cooperation aimed at proposing strategies that will enhance security in cyberspace.[773] The central strategy and plan of the Global Cybersecurity Agenda (GCA) as it relates to legislative measures embarked upon by member-states, is the amplification of strategies for the creation and growth of a harmonised model cybercrime legislation that is globally applicable.[774]

Various proposals have therefore been made to the ITU as a template for a model harmonised cybercrime legislation that should be adopted by the UN as part of the panacea to tackling the lacunae created by divergent national or regional legislations. For instance, Schjølberg[775] and Ghernaouti-Helie proposed a global treaty on cybersecurity and cybercrime.[776] The draft code requires member states to criminalise certain cyber activities such as illegal access; illegal interception; data interference; system interference; misuse of information technology devices; computer-related forgery; computer-related fraud; identity theft; offences relating to child pornography;

---

772 Resolution 56/121 of 19 December 2001 on combating the criminal misuse of information technologies. See http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf (Date of use: 21 July 2013).

773 Schjølberg S and Ghernaouti-Helie S "A global treaty on cybersecurity and cybercrime" http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf (Date of use: 2 August 2013).

774 Schjølberg S "The history of global harmonization on cybercrime legislation – The road to Geneva" http://www.cybercrimelaw.net/documents/cybercrime_history.pdf (Date of use: 2 August 2013).

775 Stein Schjølberg was the Chairperson of the High-Level Experts Group (HLEG) for ITU's Global Cybersecurity Agenda (GCA) See http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/foreword_chair.html (Date of use: 3 August 2013).

776 Schjølberg and Ghernaouti-Helie http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf (Date of use: 2 August 2013).

massive and coordinated cyber-attacks against critical communications and information infrastructures; terrorism and serious cyber-attacks; and preparatory acts that will enable the commission of an offence.[777]

The American Bar Association's Privacy and Computer Crime Committee, for its part, put together a sample toolkit for the ITU[778] after an analysis of the cybercrime legislation of developed nations and the Council of Europe, aimed at providing countries with sample legislative language that will assist in establishing harmonised cybercrime legislation.[779] The sample toolkit suggests certain cyber activities that should be criminalised. These activities include unauthorised access to computers, computer systems, and networks; unauthorised access to computer programmes, computer data, content data, traffic data; system interference or disruption; data interception; computer misuse and transmission of malware; digital forgery; digital fraud; aiding, abetting and attempting to commit computer-related crimes; and corporate liability for the commission of e-crime.[780]

Reaching consensus on a global protocol by the UN or its affiliates being a difficult venture has severally been postponed and several suggestions to that effect has not yet been implemented for various reasons. For example, the General Assembly postponed the consideration of the adoption of Resolutions 55/63 and 56/121 (United Nations General Assembly Resolutions on combating the criminal misuse of information technologies), pending the outcome of the plan of action against high-technology crime considered by the Commission on Crime Prevention and Criminal Justice.[781] The Eleventh Congress also deferred action on the development of a UN cybercrime treaty

---

777 http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/chapter_1.html (Date of use: 4 August 2013).

778 http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf (Date of use: 4 August 2013).

779 The ITU left the said toolkits open for more input by individuals and organisations before publishing the revised version; http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf (Date of use: 4 August 2013).

780 http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf (Date of use: 4 August 2013).

781 Li X "International actions against cybercrime: Networking legal systems in the networked crime scene" http://www.webology.org/2007/v4n3/a45.html (Date of use: 5 August 2013).

after the UN Secretary-General had gone to great lengths to explore the option of the creation of a global treaty on e-crime.[782] A proposal for a global cybercrime treaty was also rejected in 2010 after 10 days of dialogue on the subject matter.[783]

A United Nations global protocol seems elusive and is yet to be attained. Li posits that the UN being a multifunctional international organisation over the years has malfunctioned in some sense and the diversified legal systems of member-states hamper the conclusion and emergence of a global UN protocol.[784]

3.2.1.2. ASIAN PACIFIC ECONOMIC COOPERATION

ASIAN PACIFIC ECONOMIC COOPERATION (APEC) is made up of 21 inter-governmental bodies of the Asian-Pacific region.[785] The body has also taken steps to compel member-economies to take adequate legislative measures to address the menace of cybercrime in the member-states' jurisdiction and the Asian-Pacific region as a whole. The body has also taken several steps to create a harmonised cybercrime legislative framework in the region. The focus of APEC originally revolved around the promotion of economic growth and trade, and then also moved on to issues affecting cross-border police cooperation.[786] In line with technological developments APEC has gone forward to also channel its focus to other areas relevant to cybercrime enforcement.[787]

For instance, in 2001 the Telecommunications and Information Working Group of APEC requested the cooperation of member-states in providing adequate security from cyber attacks, and sharing information with respect to member state's efforts in response to

782 Broadhurst 2006 *International JPSM* 418.
783 Chang Y *Cybercrime in the greater China region* (Edward Elgar Publishing Cheltenham 2012) 89-145.
784 Li http://www.webology.org/2007/v4n3/a45.html (Date of use: 5 August 2013).
785 http://www.apec.org/About-Us/About-APEC/Member-Economies.aspx (Date of use: 10 August 2013).
786 Broadhurst 2006 *International JPSM* 429.
787 Broadhurst 2006 *International JPSM* 429.

Resolution 55/63[788] of the UN General Assembly.[789] Also, the regional body pointed out the need for improved cooperation among member states in fostering information security, public or private cooperation in promoting information security, and the need to establish a legal foundation for combating IT crime.[790]

In 2002 APEC leaders made a commitment to "endeavour to enact a comprehensive set of laws relating to cyber security and cybercrime that are consistent with the provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 and the Convention on Cybercrime by October 2003".[791] During 2004, at the Ministerial meeting in Chile, a statement by APEC was issued agreeing to "strengthen the respective economies ability to combat cybercrime by enacting domestic legislation consistent with the provisions of international legal instruments, including the Convention on Cybercrime, and relevant United Nations General Assembly Resolutions".[792]

Again the APEC (TEL)[793] recommended that member economies should ensure that their legal frameworks expeditiously adopt broad, procedural, substantive and mutual assistance regulations and policies in addressing IT crimes, with the adequate assistance and effort of member economies facilitated by APEC.[794] The

---

788 UN General Assembly Resolution 55/63 requests member states to take appropriate legislative measures to ensure that information technology crime safe havens are eliminated. See Resolution 55/63 "Combating the criminal misuse of information technologies" www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf (Date of use: 10 August 2013).

789 Westby JR (ed) *International guide to cyber security* (ABA Chicago 2004) 35-102.

790 This was pointed out at the 5th APEC Ministeral Meeting on Telecommunications and Information Industry (TELMIN5) Shanghai Declaration. See "Fifth APEC Ministeral Meeting on Telecommunications and Information Industry (TELMIN5)" http://www.asianlii.org/apec/other/agrmt/fammotaiisc819/ (Date of use: 10 August 2013).

791 Schjølberg http://www.cybercrimelaw.net/documents/cybercrime_history.pdf (Date of use: 2 August 2013).

792 Schjølberg http://www.cybercrimelaw.net/documents/cybercrime_history.pdf (Date of use: 2 August 2013).

793 "Recommendation by the APEC telecommunications and information working group (TEL) to APEC senior officials (SOM) for an APEC cybersecurity strategy" http://www.cybersecuritycooperation.org/moredocuments/International%20Agreements/Cybersec%20Strategy%20TEL%20final.htm (Date of use: 10 August 2013).

794 "Recommendation by the APEC telecommunications and information working group (TEL) to APEC senior officials (SOM) for an APEC cybersecurity strategy"

recommendation further stipulated that member economies should present their reports on the status of their various comprehensive, substantive, procedural and mutual assistance laws and policies.[795]

Another notable step by APEC in facilitating the harmonisation of e-crime legislation among member economies is the institution of the Cybercrime Legislation and Enforcement Capacity Building Conference of Experts and Training seminar, which was aimed at promoting the growth of comprehensive legal frameworks among member economies, provision of assistance in the development of law enforcement e-crime units, and improving the cooperation between the industry and law enforcement units in combating cybercrime.[796]

In 2012 APEC[797] urged its member economies to take strategic measures to promote a safe and trusted ICT environment, protect consumers and enhance mutual cooperation among member economies in order to increase cyber security.[798]

APEC has taken various steps in ensuring the emergence of cybercrime legislative initiatives amongst its member economies. Its directive that these legislative measures should consider the Council of Europe Convention on Cybercrime and UN Resolution 55/63 is a worthy directive that will engender the harmonisation of e-crime legislation among APEC member-economies.[799] However APEC's decisions, although arrived at

---

http://www.cybersecuritycooperation.org/moredocuments/International%20Agreements/Cybersec%20Strategy%20TEL%20final.htm (Date of use: 10 August 2013).

795 "Recommendation by the APEC telecommunications and information working group (TEL) to APEC senior officials (SOM) for an APEC cybersecurity strategy" http://www.cybersecuritycooperation.org/moredocuments/International%20Agreements/Cybersec%20Strategy%20TEL%20final.htm (Date of use: 10 August 2013).

796 Westby *International guide to cyber security* 35-102.

797 The 9th APEC Ministerial Meeting on Telecommunications and Information (TELMIN8) was held in St Petersburg, Russia, on 7-8 August 2012.

798 http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2012_tel.aspx (Date of use: 10 August 2013).

799 "Recommendation by the APEC telecommunications and information working group (TEL) to APEC senior officials (SOM) for an APEC cybersecurity strategy" http://www.cybersecuritycooperation.org/moredocuments/International%20Agreements/Cybersec%20Strategy%20TEL%20final.htm (Date of use: 10 August 2013).

by open dialogue and consensus, are voluntary and non-binding.[800] It is submitted that the chances of ensuring the harmonisation of cybercrime legislation among member-states by APEC as a region are slim when the decisions by the member-states have no binding effect on members of the regional body.

The efforts of APEC revolve around issuing directives to member bodies to create their cybercrime legislations and capacity building. Its efforts in creating harmonised cybercrime legislation has yielded no results.[801] Most members of the regional body have taken their initiatives to create their own cybercrime legislations or taken a cue from the CoE Cybercrime Convention.[802]

3.2.1.3. COUNCIL OF EUROPE

The Council of Europe (CoE) as a regional body has taken various initiatives in addressing the threat of cybercrime starting from the Council of Europe Conference on Criminological Aspects of Economic Crime in Strasbourg in 1976.[803] In a bid to create some harmony among national legislations, the CoE selected a team of experts to look into the legal issues involving computer-related crime, and this gave birth to the emergence of a summary of guidelines for national legislatures to adopt.[804] The recommendations which had an outline of substantive cyber-offences were non-binding

800 http://digitalreview.asia/content/sub-regional-perspectives/asia-pacific-economic-cooperation (Date of use: 10 August 2013).

801 Li http://www.webology.org/2007/v4n3/a45.html (Date of use: 10 August 2013).

802 Most members are developed countries such as Australia, the United States, and Canada that have taken the issue of cybercrime seriously; http://www.apec.org/about-us/about-apec/member-economies.aspx (Date of use: 13 August 2013).

803 At the conference, categories of computer crime were introduced. See Schjølberg http://www.cybercrimelaw.net/documents/cybercrime_history.pdf (Date of use: 2 August 2013).

804 The guidelines were presented in the Recommendation of 1989. The Recommendation stipulated the minimum list of offences that should be criminalised by various national legislatures, namely, unauthorised access; unauthorised interception;computer fraud; computer forgery; damage to computer data; computer sabotage; unauthorised reproduction of a protected computer programme; and unauthorised reproduction of a topography. See Schjølberg S and Hubbard AM "Harmonizing national legal approaches on cybercrime" http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf (Date of use: 13 August 2013).

on member states and, therefore, had a limited ability to create a harmonised legislative initiative across member-states.[805]

Driven by the need to create a more harmonised legislative initiative which will enhance the ability of law enforcement agencies to effectively address the growing threat of cybercrime, the Council of Europe created a more binding treaty and opened same for signatures both to member-states and non-member states.[806] As at September 2018, sixty-five countries are signatories to the Convention and 61 countries have ratified same, while 4 countries have signed but not ratified the Convention.[807]

The Convention clearly specified certain conducts that national legislative initiatives should proscribe. These include offences against the confidentiality, integrity and availability of computer data;[808] computer-related offences;[809] content-related offences;[810] and offences related to infringements of copyright and related rights.[811] The CoE, in line with the growing acts of racism and xenophobic tendencies perpetrated and targeted on individuals with the aid of the computer system, rose up to address such acts through the drafting of an additional protocol to the Convention on Cybercrime,

---

805 Schjølberg and Hubbard http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf (Date of use: 13 August 2013).

806 The Council of Europe Convention on Cybercrime, 2001 ETS No 185 was opened for signature in 2001; http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG (Date of use: 13 August 2013).

807 http://conventions.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?desktop=true (Date of use: 21 September 2018).

808 Art 2 proscribes illegal access of a computer system; art 3 proscribes the illegal interception of data to and from a computer system; art 4 proscribes data interference; art 5 proscribes system interference; while art 6 proscribes the misuse of computer-related devices including the production, sale, procurement for use, import or distribution or otherwise making available of such device. See Broadhurst 2006 *International JPSM* 429. See also The Council of Europe Convention on Cybercrime, 2001 ETS No 185.

809 The traditional crimes of computer-related forgery and computer-related fraud fall under this category. See arts 7 and 8 of the Council of Europe Convention on Cybercrime, 2001 ETS No 185.

810 Child pornography falls in this category of offences and it also criminalises the procurement, possession or distribution of child pornography. See art 9 the Council of Europe Convention on Cybercrime, 2001 ETS No 185.

811 Art 10 of the Council of Europe Convention on Cybercrime makes it an offence to wilfully infringe on a commercial scale the copyrights or related rights when such infringement was done by means of a computer system.

concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.[812]

The Convention makes adequate provision for the establishment of harmonised procedural rules by adopting conventional measures such as search and seizure, and creating new measures, such as real time collection of data, interception of data and expedited preservation of data, to enable the effective investigation and prosecution of IT crime.[813] Broadhurst pointed out that the Convention includes strong procedural guarantees and, except in cases of official criminal investigations, the Convention does not validate the surveillance of private communications by either service providers or law enforcement agencies.[814]

The Convention also addresses the issue of jurisdiction by establishing the criteria upon which parties to the Convention can assume jurisdiction over the criminal offences stipulated in the Convention. Parties can assume jurisdiction where the offence was committed within "its territory; or on board a ship flying the flag of that state-party, or on board an aircraft registered under the laws of that state-party, or by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any state".[815] The Convention also requires international cooperation and mutual assistance among parties, and requires states to consult with a view of determining the most appropriate jurisdiction where more than one party can assume jurisdiction over an offence.[816] The Convention, as part of its efforts in creating harmony in addressing e-crime, established the legal basis for an international computer crime assistance network. This requires states to

---

812 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, 2006 (ETS No. 189)**.**

813 Broadhurst 2006 *International JPSM* 429. See also arts 16-21 CoE Convention on Cybercrime*.*

814 Broadhurst 2006 *International JPSM* 429.

815 Art 22 CoE Cybercrime Convention.

816 Art 22 CoE Cybercrime Convention*.*

designate contact points that are available 24 hours everyday in order to ensure immediate assistance when a cyber-criminal activity takes place.[817]

Although regarded as the most significant international cybercrime agreement, the Convention is fraught with certain flaws that contribute to its inability to translate into an instrument accepted by all nations, which will create the emergence of a harmonised treaty. One such flaw is that the CoE Convention is a regional binding agreement which in its scope of operation is limited to parties to the Convention that have ratified the Convention. Thus, the Convention is not a global agreement. The Convention has been ratified by 61 countries and, even at the regional level, not all Council of Europe members such as Russia are signatories to the Convention.[818] Another flaw is that there are several reservations on the human rights implications of the enforcement of the CoE Cybercrime Convention among parties. For instance, according to the electronic privacy information centre, the Convention infringes upon an individual's right to privacy and lacks a "dual criminality provision"[819] which would enable a foreign law enforcement agency to investigate an activity which, although legal in the US, is a crime in the investigating state, and the US will be compelled to cooperate with that state.[820] The pirate party of Australia objected to the ratification of the Convention and pointed out that the Convention would open up Australia to allowing the release of citizens' data or communications to countries that allow capital punishment or penalties exceeding $100,000.[821]

Most civil liberty organisations also objected to the Convention stating that the requirement for the retention of data on customer activities by internet service providers was a derogation on the privacy rights of citizens and encourages improper monitoring

---

817 This 24/7 point of contact network would enable states to respond more appropriately to the law enforcement challenges posed by information technology crime. See Broadhurst 2006 *International JPSM* 424. See also art 35 CoE Cybercrime Convention.

818 See CoE Convention on Cybercrime.

819 "*Dual criminality* requires that an accused be extradited only if the alleged criminal conduct is considered criminal under the laws of both the surrendering and requesting nations." See Doyle C *Extradition to and from the United States* (Nova Science Publishers New York 2008) 7.

820 http://epic.org/privacy/intl/ccc.html (Date of use: 18 August 2013).

821 http://pirateparty.org.au/2013/03/05/cybercrime-convention-ratification-leaves-lingering-concerns/ (Date of use: 18 August 2013).

of private communications.[822] They also pointed out that article 14 of the Convention, which sets out the conditions for the search and seizure of stored computer data, lacks essential procedural safeguards to protect the rights of the individual and to ensure due process of law since there is nothing that will ensure that an independent judicial review takes place before the search and seizure.[823] There has also been another concern, namely, that the Convention validates the transfer of personal data to countries without adequate data protection laws.[824]

However, most of the concerns raised by various bodies, especially by the civil liberty organisations on the human rights implications of the CoE Cybercrime Convention, have been debunked as unsubstantiated.[825] The promoters of the CoE Convention on Cybercrime, such as Bellia, have further stated that some of these fears on the infringement of individuals' human rights are properly protected by the provisions in the Convention and the existing national legal framework that guarantee the protection of human rights.[826] Nevertheless, the acknowledgement of the CoE Convention on Cybercrime by various scholars, organisations and even the UN, that the CoE Convention is the foremost and relevant standpoint on any harmonisation efforts on e-crime, has achieved little success in propelling more countries to become parties to or ratify the Convention.[827]

Scholars have also pointed out several other reasons that contribute to the inability of the CoE Convention on Cybercrime to translate into an instrument accepted and adopted by all nations. Some leading world economies such as China, Russia and other authoritarian regimes on the international scene, drive policies that discourage trans-

822 http://gilc.org/privacy/coe-letter-1000.html (Date of use: 18 August 2013).
823 http://gilc.org/privacy/coe-letter-1000.html (Date of use: 18 August 2013).
824 http://pirateparty.org.au/2013/03/05/cybercrime-convention-ratification-leaves-lingering-concerns/ (Date of use: 18 August 2013).
825 Marler SL "The Convention on Cybercrime: Should the United States ratify?" (2002) *New England Law Review* 183-219.
826 Lemos R "International cybercrime treaty finalized" http://news.cnet.com/2100-1001-268894.html (Date of use: 31 December 2013).
827 Lewytzkyj M "Tactics in cybersecurity: Russia and US – Don't forget the Council of Europe Cyber-Crime Convention" http://www.examiner.com/article/tactics-cybersecurity-russia-us-don-t-forget-the-council-of-europe-cyber-crime-convention (Date of use: 31 December 2013).

national cooperation.[828] For instance, Russia opposes the Convention on the grounds that the Convention permits criminal investigations in a foreign jurisdiction without prior notice to the local authorities.[829] Most authoritarian countries take serious objection to any form of international effort that may impinge on its sovereignty or meddle in its domestic affairs.[830]

According to Kamlu, most of these developed countries with authoritarian governments do not take the issue of addressing cybercrime seriously and, therefore, object to the CoE Convention on Cybercrime since they benefit from the proceeds of such cyber-criminal activities in terms of espionage and foreign exchange or economic growth.[831] Unfortunately, any international cybercrime agreement that will engender the harmonisation of cybercrime legislations will require a high level of international cooperation which the policies of most authoritarian regimes do not encourage.[832] It is also important to note that where major world powers take divergent positions on global issues, the likelihood of the success of any effort to tackle such global issues will be slim since each world power has nations that are in alignment with their position on any global issue.

A further major impediment to the success and acceptance of the Convention is the fact that the negotiation and development of the Convention revolved around a few states and did not receive wide coverage and consultation.[833] The Convention was drafted by a committee of experts on crime in cyber-space formed by the Council of Europe with no input from most non-member states who are urged to become parties to the

828 Pei M "China's political evolution: Implications for Beijing's foreign relations" http://www.thefreelibrary.com/China%27s+political+evolution%3a+implications+for+Beijing%27s+foreign...-a0155824547 (Date of use: 18 August 2013).

829 Giles K "Russia's public stance on cyberspace issues" in Czosseck C, Ottis R and Ziolkowski K (eds) papers delivered at 4th international conference on cyber space conflict, 5-8 June 2012, Tallinn, Estonia 63-75.

830 Pei http://www.thefreelibrary.com/China%27s+political+evolution%3a+implications+for+Beijing%27s+foreign...-a0155824547 (Date of use: 18 August 2013).

831 http://www.themoscowtimes.com/news/article/ex-soviet-hackers-dominate-cyber-crime-world/484999.html (Date of use: 29 August 2013).

832 Giles *Russia's public stance in cyberspace issues* 133.

833 Harley http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/ (Date of use: 30 December 2013).

agreement.[834] This further diminishes the status of the CoE Convention on Cybercrime from assuming global status to being a mere regional agreement. Some scholars have posited that the best approach will be the drafting of a more global treaty with greater international participation in its drafting.[835] As pointed out by Archick, the countries that took part in the negotiations of the CoE Cybercrime Convention are not the "problem countries" that provide a safe haven for cyber-criminals, but rather the countries that are already fighting cybercrime and have some measure of existing legislative framework to tackle the issue of cybercrime.[836] These safe havens are exploited by the perpetrators of e-crime in routing their nefarious activities which does not criminalise their activity, thereby relying on the principle of jurisdiction as a shield from the law.[837]

Despite the flaws and criticisms that trail the emergence of the CoE Convention on Cybercrime, the Convention remains the leading binding treaty that can be used as a springboard in engendering the harmonisation of national legislative initiatives on cybercrime. Unfortunately this regional effort, which seeks to propel the harmonisation of various national cybercrime laws, has not attained the success as anticipated by its proponents, and many nations are not taking the necessary steps to become parties and/or to ratify the said Convention. For example, of all the African countries only South Africa, Mauritius, Morocco and Senegal have signed the treaty and only Mauritius, Morocco and Senegal has assented to same.[838]

These inconsistencies in national cybercrime legislations are further exacerbated by the reluctance of many countries to be part of existing efforts by international bodies to create harmonised legislation, and this has greatly hampered the quest to properly

---

834 The United States, Canada and South Africa were the only non-CoE nations that at some stage participated in the drafting of the Convention. See Rodota S "Opinion 4/2001 on the Council of Europe's draft Convention on Cyber-Crime" http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp41_en.pdf (Date of use: 18 August 2013). See also http://epic.org/privacy/intl/ccc.html (Date of use: 18 August 2013).

835 Harley http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/ (Date of use: 30 December 2013).

836 Archick K "Cybercrime: The Council of Europe Convention" http://fpc.state.gov/documents/organization/58265.pdf (Date of use: 1 January 2014).

837 Li http://www.webology.org/2007/v4n3/a45.html (Date of use: 18 August 2013).

838 http://conventions.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?desktop=true (Date of use: 21 September 2018).

address the menace of cybercrime. As a result of the ubiquitous nature of the internet, the usefulness and impact of the CoE Cybercrime Convention will be felt when more states accede to the Convention and enforce the provisions of the Convention.[839]

3.2.1.4. THE AFRICAN UNION

The African Union (AU) is a regional body with the highest concentration of developing and under-developed countries as its members. A few of the nations within the AU have taken some steps to enact cybercrime legislations. Of the 54 countries that make up the Union, only a few countries[840] have enacted distinct national cybercrime laws.[841] A few[842] other countries within the AU have drafted cybercrime bills which have been passed to its national assembly for consideration and eventual enactment as law.

Within the African continent or AU steps are being taken by various regional blocs to propel members of such blocs to create some form of cybercrime legislation and to engender harmonisation of the bloc's member states' national cybercrime legislation. For instance, the Southern African Development Community (SADC)[843] has held several meetings and made recommendations geared towards engendering

---

839 Archick http://fpc.state.gov/documents/organization/58265.pdf (Date of use: 1 January 2014).

840 These include South Africa, Kenya, Mauritius, Cameroon, Zambia, Uganda, Algeria, Namibia and Botswana. See Kharouni L "Africa: A new safe harbour for cybercriminals?" http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-africa.pdf (Date of use: 29 August 2013). See also Sikuka K "Southern Africa: Region cracks down on cyber crime" http://allafrica.com/stories/201204120866.html (Date of use: 31 August 2013). See also Mwaita P and Owor M "Workshop report on effective cybercrime legislation in Eastern Africa" http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/2571_EastAfrica_WS_Report.pdf (Date of use: 12 October 2014).

841 http://www.ictparliament.org/legislationlibrary/Cybercrime (Date of use: 29 August 2013). See also Becker R "How many countries in Africa? How hard can the question be?" http://africacheck.org/reports/how-many-countries-in-africa-how-hard-can-the-question-be/ (Date of use: 29 August 2013).

842 These include Tanzania and Angola. See Kshetri *Cybersecurity* 165-166. See also Mwaita and Owor http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/2571_EastAfrica_WS_Report.pdf (Date of use: 12 October 2014).

843 The Southern African Development Community (SADC) is an inter-governmental body that seeks to promote the integration of economic development in countries in the Southern African region. Its member states include Angola, Botswana, the DRC, Lesotho, Madagascar, Malawi, Namibia, Mozambique, Seychelles, South Africa, Swaziland, Tanzania, Zambia and Zimbabwe. See http://www.sadc.int/about-sadc/overview/history-and-treaty/ (Date of use: 31 August 2013).

harmonised cybercrime legislation amongst its member states.[844] However, member states with some form of cybercrime legislation are Botswana, Mauritius, South Africa and Zambia while, according to *Sikuka,* the *"o*ther 11 member states are either developing cybercrime legislations or have started national consultations on the matter".[845] The Eastern African regional bloc[846] of the African continent or AU are working on steps that will propel the emergence of a harmonised set of cybercrime laws within the bloc as a means of facilitating regional trade.[847]

The AU as a body, in a bid to propel the harmonisation of cybercrime legislation among its member states, has drafted a cybercrime convention that will help to chart the course in addressing the menace of cybercrime in Africa.[848] However, it is submitted that considering the fact that Africa is made up of a large number of developing and underdeveloped countries, has limited internet penetration, is plagued with poverty and bigger national issues and have very few existing national legislations on cybercrime, very few member states will embrace the draft AU cybercrime convention.

3.3. ADEQUACY OF THE EXISTING APPROACH IN ACHIEVING A HARMONISED LEGISLATIVE FRAMEWORK

From the above analysis of the existing international and regional efforts to create a harmonised legislative framework within and outside the body's sphere of influence, it is evident that the efforts already embarked upon either are not yielding efforts, or are under serious opposition or bereft of seriousness in its implementation, and are thereby inefficient and ineffective. Therefore, although global efforts and international cooperation on the issue of cybercrime are encouraging, international consensus on

---

844 Sikuka K "Southern Africa: Region cracks down on cyber crime" http://allafrica.com/stories/201204120866.html (Date of use: 31 August 2013).

845 Sikuka http://allafrica.com/stories/201204120866.html (Date of use: 31 August 2013).

846 The East African Community (EAC), an intergovernmental regional organisation on the African continent, has five member-states which include Burundi, Kenya, Rwanda, Tanzania, and Uganda. See http://www.eac.int/ (Date of use: 31 August 2013).

847 Okuttah M "EAC eyes trade growth with cyber laws" http://www.businessdailyafrica.com/EAC-eyes-trade-growth-with-cyber-laws/-/539444/945130/-/xd5eh7z/-/index.html (Date of use: 31 August 2013).

848 African Union convention on Cyber Security and personal data protection, 2014.

cybercrime still is far-fetched.[849] Some opponents of the harmonisation of any international criminal law in general argue that legislative frameworks on criminal law should only be born out of a people's culture, historical background, national convictions and values.[850]

Various existing international efforts in addressing cybercrime presently revolve around raising awareness, examining current cybercrime trends and providing recommendations on best practices, requesting governments to enact their national cybercrime legislation, producing reports, monitoring cyber activities and establishing some form of police collaboration.[851] The existing international harmonisation efforts mostly are regional agreements with limited acceptance and beleaguered by a number of factors. The developed countries are the ones primarily preoccupied with making the necessary international efforts at harmonisation, while the developing countries take few or no steps to address same and are only encouraged to take part in the efforts created by the developed countries.[852] Li points out that such international efforts will be ineffective since treaties are not meant for third parties and will be effective when signatories to the treaty take effective action.[853] International harmonisation has also been plagued with pluralisation which pitches different groups at divergent standpoints on a single issue and invariably propels the enactment of divergent solutions or measures in addressing a single issue.[854]

The difficulty in reaching consensus on harmonisation efforts and the inability to regularise these efforts imply that harmonisation efforts must be intensified. Nations, international bodies and stakeholders must ensure that not only are calls for harmonisation made, but concrete steps are embarked upon by all stakeholders to

---

849 Li http://www.webology.org/2007/v4n3/a45.html (Date of use: 31 August 2013).

850 Spinellis D "Opportunité et Légitimité de l'Harmonisation" http://hal.archives-ouvertes.fr/docs/00/41/96/45/PDF/OPPORTUNITE_ET_LEGITIMITE_DE_L_HARMONISATION_-_Donysios_SPINELLIS.pdf (Date of use: 31 August 2013).

851 Pakalniškis S *What factors explain why there is not a common and comprehensive global response to cyber threats?* (LLM dissertation, Leiden University, 2012) 35.

852 Li http://www.webology.org/2007/v4n3/a45.html (Date of use: 13 August 2013).

853 Li http://www.webology.org/2007/v4n3/a45.html (Date of use: 13 August 2013).

854 Li http://www.webology.org/2007/v4n3/a45.html (Date of use: 13 August 2013).

ensure the creation of a binding universal agreement.[855] The ubiquitous nature of the internet dictates that efforts that will effectively address crime on cyberspace must be born out of a comprehensive global agreement.

3.4. PROPOSING A HARMONISED CYBERCRIME LEGISLATION

As pointed out earlier, evolving a harmonised global cybercrime legislation at the international level holds the key to addressing the various inconsistencies prevalent in the existing national cybercrime legislations, and will go a long way towards propelling developing countries without adequate cybercrime legislations into evolving their cybercrime legislation. It is submitted that the UN would be the appropriate body to spearhead and create a globally-acceptable harmonised legislative framework or treaty since it is the foremost international body with about 98 percent of sovereign nations of the world as members.[856] Watney warns that a global treaty should not replace national and transnational cybercrime laws, but should rather provide the chance for nations to align their laws with the global agreement, thereby leading to the harmonisation of cybercrime legislations across borders and enabling trans-border investigations, prosecution and prevention.[857] It is further submitted that the CoE Convention on Cybercrime and its additional protocol should be used as a springboard and precedent for the drafting and creating of this global harmonised cybercrime legislation.[858]

In proposing the evolution of a globally-acceptable internet crime legislative agreement, certain principles must be adhered to, to forestall the apathy and setbacks that has greeted the existing e-crime regional agreements. Certain principles should be

---

855 Li http://www.webology.org/2007/v4n3/a45.html (Date of use: 13 August 2013).

856 See Rosenburg M "Non-members of the United Nations" http://geography.about.com/od/politicalgeography/a/nun.htm (Date of use: 3 January 2014).

162 Watney M "The way forward in addressing cybercrime regulation on a global level" (2012) *Journal of Internet Technology and Secured Transactions* 61-67.

858 The United Nations, in directing its member-states to update its cybercrime laws, directed them to take into consideration the CoE Convention on Cybercrime. See Broadhurst R and Chang YC "Cybercrime in Asia: Trends and Challenges" in Liu J and Hebenton B (eds) *Handbook of Asian criminology* (Springer New York 2013).

observed in the drafting of the harmonised cybercrime legislation.[859] These principles will be useful tools in the creation and drafting of a harmonised global cybercrime legislation. They will also ensure that the varied interests of nations are adequately protected, forestalling later disenchantment of some member states in the outcome of the harmonised legislation. These principles are listed below.

i. ONLINE-OFFLINE UNIFORMITY[860]

A major principle in the creation of a harmonised cybercrime legislation is the regulation of online criminal conduct in the same way real world criminal conduct is regulated in the best practicable terms.[861] Thus, criminalising an online activity is necessary if the same activity is deemed offensive in the real world, and the punishment for these activities should be meted out with similar severity since the only difference between the conduct is the location and medium of the commission.

ii. USE OF TECHNOLOGY-NEUTRAL LANGUAGE

Another principle that has to be adhered to in the creation of harmonised e-crime legislation is the use of technology-neutral language.[862] The rate of technological advancement dictates that the use of technology-specific language may render legislative terms in a cybercrime legislation obsolete when new technological equipment that was not envisaged at the time of drafting the said legislation comes into being.[863] The constant advancement also entails that the manner of the commission of offensive conduct will in the course of time evolve beyond the scope of the drafters of such legislation.[864] Thus, harmonised legislation must be drafted to take care of existing

---

859 Bande https://lirias.kuleuven.be/bitstream/123456789/404618/1/The+Making+of+Cybercrime+Legislation+in+Malawi+Pdf.pdf (Date of use: 12 September 2013).

860 Bande https://lirias.kuleuven.be/bitstream/123456789/404618/1/The+Making+of+Cybercrime+Legislation+in+Malawi+Pdf.pdf (Date of use: 12 September 2013). See also Downing RW "Shoring up the weakest link: What lawmakers around the world need to consider in developing comprehensive laws to combat cybercrime" (2005) 43 *Columbia Journal of Transnational Law* 705-762.

861 Clough J *Principles of cybercrime* (Cambridge University Press Cambridge 2010) 3-21.

criminal conduct while making room for evolving conducts through the use of technology-neutral language to avoid the constant amendment of such pieces of legislation. However, reliance on the *sui generis* rule or the use of technology-neutral language does not presuppose that the legislative language will then be ambiguous rendering the legislation ineffective.[865]

iii. RESPECT FOR FUNDAMENTAL HUMAN RIGHTS

Laws are made to protect human beings and their interests. However, a major critique of various cybercrime legislative initiatives is that its provisions derogate the fundamental rights of individuals that the same law seeks to protect.[866] Any acceptable harmonised cybercrime legislation must overtly and covertly show in its provisions that fundamental human rights must be protected and efforts to derogate same is not encouraged by the legislation.

Bande points out that the requirement and the measures to respect and protect the fundamental human rights of individuals must cut across the substantive provisions and procedural provisions of the legislation, and is essential in cybercrime legislative drafting.[867] The definitions, interpretations and applications of the substantive crimes, and the investigating and prosecuting measures of the procedural provisions of the

---

862 Reed C "Taking sides on technology neutrality" http://www2.law.ed.ac.uk/ahrc/script-ed/vol4-3/reed.asp (Date of use: 3 January 2014).

863 Reed http://www2.law.ed.ac.uk/ahrc/script-ed/vol4-3/reed.asp (Date of use: 3 January 2014).

864 For example, the use of the word 'viruses' in cybercrime legislation will grow obsolete with the emergence of other forms of malicious codes since technology is not static.

865 Moses LB "*Sui generis* rules" in Marchant GE, Allenby BR and Herkert JR (eds) *The growing gap between emerging technologies and legal-ethical oversight: The pacing problem* (Springer 2011) 77-93. See also Bande https://lirias.kuleuven.be/bitstream/123456789/404618/1/The+Making+of+Cybercrime+Legislation+in+Malawi+Pdf.pdf (Date of use: 12 September 2013).

866 For example, the CoE cybercrime legislation has been widely criticised on the grounds that its provisions allow for the derogation of the privacy rights of individuals. See http://gilc.org/privacy/coe-letter-1000.html (Date of use: 13 September 2013).

867 Bande https://lirias.kuleuven.be/bitstream/123456789/404618/1/The+Making+of+Cybercrime+Legislation+in+Malawi+Pdf.pdf (Date of use: 12 September 2013).

harmonised cybercrime initiative also must not derogate the human rights of individuals.[868]

However, it is submitted that for the human rights of individuals to be adequately protected, some infringement may have to take place.[869] In such circumstances, the courts or a body established by law to analyse the supervening exception should be the only empowered entity to grant such minor exception after a thorough analysis of the circumstances with due regard to the rule of law and the preservation of societal peace.

iv. PRESENCE OF *MENS REA*

It is essential that cybercrime offences are not strict liability[870] offences and the presence of adequate *mens rea* should be determined in order to place liability on the offender. The mental element that shows that the offender intended to commit the offence is necessary in order to place sufficient blameworthiness on the offender. The law intends that any person who acts purposely, knowingly or recklessly is aware of the circumstances of the action.[871]

v. INCHOATE LIABILITY

Another principle that will make for effective harmonised cybercrime legislation is making adequate provision and requisite punishment for inchoate offences.[872] Inchoate

---

868 Bande https://lirias.kuleuven.be/bitstream/123456789/404618/1/The+Making+of+Cybercrime+Legislation+in+Malawi+Pdf.pdf (Date of use: 12 September 2013).

869 For instance, the right to privacy may in certain circumstances be infringed in order to place surveillance on suspected terrorists.

870 Strict liability offences are wont to be harsh and lead to injustice, thus the law presumes that *mens rea* is required to prove criminal liability. See *Sweet v Parsley* (1970) AC 132.

871 Robinson PH "*Mens rea*" https://www.law.upenn.edu/fac/phrobins/mensreaentry.pdf (Date of use: 28 September 2013).

872 Inchoate offences refer to incomplete crimes, which take place where an individual takes appropriate steps to commit a crime, attempt to commit a crime or indirectly participate in the commission of a crime. See *DPP v Stonehouse* [1978] AC 55. See also Stenson T "Inchoate crimes and criminal responsibility under International law" https://www.law.upenn.edu/journals/jil/jilp/articles/1-1_Stenson_Thomas.pdf (Date of use: 14 September 2013).

crimes cut across the doctrines of conspiracy, solicitation, attempt and incitement, which should be adequately covered by any harmonised e-crime legislative initiative.[873] The essence of inchoate liability is to prevent to some extent the eventual occurrence of the planned criminal conduct since the perpetrator has exhibited the intent to commit such offence but could not put the intent into fruition because of an intervening circumstance.

vi. **COUNTRY-SPECIFIC LEGISLATION**

An effective harmonised cybercrime legislation should be drafted in such a way as to allow countries to modify their cybercrime legislation to suit their jurisdictional specifications without eroding the intentions of the harmonised cybercrime legislation. This is because although e-crime is a global issue, it does not totally eliminate national boundaries since such offences are perpetrated from specific locations and the effects are also felt within specific locations. As pointed out earlier, the impact of e-crime differs across national boundaries, the national priorities in tackling cybercrime also differ, the resources available in tackling cybercrime and the genre of online activities that are viewed as criminal also vary along national boundaries. It is therefore expedient that legislative initiatives also reflect these variations and harmonised legislations to make room for country-specificity.[874] In making room for country-specific provisions, a proper balance has to be struck so that the purpose of harmonisation is not defeated. For instance, it will be impracticable to have the same rules regarding the punishment of offences for all national jurisdictions. It will be assumed that the kind of punishment meted out in the case of offline crimes will be the same as or almost similar to the punishment meted out in the case of a similar online offence within a jurisdiction. Thus, having a harmonised law will not guarantee that every section of the harmonised legislation will be adopted *verbatim*. Creating a proper balance can be achieved by specifying minimum standards/punishment which will permit domestic legislative

873 Bande https://lirias.kuleuven.be/bitstream/123456789/404618/1/The+Making+of+Cybercrime+Legislation+in+Malawi+Pdf.pdf (Date of use: 12 September 2013).

874 Bande https://lirias.kuleuven.be/bitstream/123456789/404618/1/The+Making+of+Cybercrime+Legislation+in+Malawi+Pdf.pdf (Date of use: 12 September 2013).

initiatives to expound on such provisions to fit into its national consciousness and needs.[875]

vii. JURISDICTION

The transnational nature of e-crime makes the issue of jurisdiction an intricate one. The fact that national legislative initiatives vary makes it more complex.[876] Jurisdiction raises the issue of the national legislation that will be applied or enforced in the event of a cyber-criminal activity and what determines same. The question arises as to whether it is the location of the computers, the location of the persons, the location of the effect, the nationality of the perpetrator, or the nationality of the victim.[877]

The issue of jurisdiction must be adequately addressed by the harmonised legislation while making recommendations on how the various national legislative initiatives should address the issue of jurisdiction both for investigations and prosecution of cybercriminal offences. According to Brenner *et al*, the right to assume jurisdiction over a criminal conduct is not attained only when the offender is physically present in a national jurisdiction.[878] A nation can assume jurisdiction to prescribe laws when the

> "conduct that, wholly or in substantial part, takes place within its territory; the status of persons, or interests in things, present within its territory; conduct outside its territory that has or is intended to have substantial effect within its territory; the activities, interests, status, or relations of its nationals outside as well as within its territory; and certain conduct outside its territory by persons not

875 Bande https://lirias.kuleuven.be/bitstream/123456789/404618/1/The+Making+of+Cybercrime+Legislation+in+Malawi+Pdf.pdf (Date of use: 12 September 2013).

876 For instance, the punishment stipulated by various national legislative initiatives for a particular cyber offence will differ depending on the impact of such cyber-activity on each jurisdiction and the punishment for the offence when committed offline.

877 Brenner SW and Koops B "Approaches to cybercrime jurisdiction" (2004) *Journal of HighTechnology Law* 1-46.

878 Brenner and Koops cybercrime jurisdiction *Journal of HTL* 8.

its nationals that is directed against the security of the state or against a limited class of other state interests".[879]

However, when the exercise of jurisdiction for an offence or person that has connection with another state is unreasonable, the state will not assume jurisdiction.[880]

According to August, the courts have established certain nexuses that must exist between the regulating state and the offence or criminal in order to entitle a state to assume jurisdiction.[881] These nexuses include the principle of territoriality;[882] protective nexus;[883] nationality principle;[884] and the universality principle.[885] In order to ensure an effective harmonised cybercrime legislative framework, an offender must be prepared to face the consequences of his cyber-offensive activity irrespective of his location/jurisdiction or jurisdiction of the target/effect of the offence.[886]

The enactment of a globally-acceptable harmonised cybercrime legislation will undoubtedly be a Herculean task considering the various divergent national interests, cultures, historical backgrounds and moral inclinations. However, upon the adherence

---

879 Brenner and Koops cybercrime jurisdiction *Journal of HTL* 8. See also sec 402 Restatement (Third) of Foreign Relations Law of the United States Section of 1987.

880 Brenner and Koops cybercrime jurisdiction *Journal of HTL* 8. See also sec 402 Restatement (Third) of Foreign Relations Law of the United States Section of 1987.

881 August R "International cyber-jurisdiction: A comparative analysis" (2002) *American Business Law Journal* 531-574.

882 This principle posits that jurisdiction is determined by the location of the commission of the crime. Thus, a state assumes jurisdiction over an offence committed within its borders. Also, when an offence is commenced within a jurisdiction, even though it is consummated abroad, the state where the offence was commenced will also assume jurisdiction. See also August (2002) *American BLJ* 534.

883 This principle posits that a state can also assume jurisdiction where the national or international interest of that state has been injured or will be injured by the offender. See also August (2002) *American BLJ* 534.

884 This principle posits that the nationality or national character of the offender is another factor that can contribute to the assumption of jurisdiction by a state. See also August (2002) *American BLJ* 534.

885 This principle posits that states can assume jurisdiction over certain offences that are acknowledged by the community of nations as being of general and grave concern. See also August (2002) *American BLJ* 534.

886 Chik WB "Challenges to criminal law making in the new global information society: A critical comparative study of the adequacies of computer-related criminal legislation in the United States, the United Kingdom and Singapore" www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc (Date of use: 3 January 2014).

of the above-mentioned seven principles in drafting or creating the universal harmonised cybercrime treaty, five strategic steps have to be taken in the evolution of the global cybercrime treaty.[887] This five-step strategy requires regional participation.[888] These strategies include:

a. Identifying the key players

The efforts of national and regional legislative initiatives are limited in addressing the menace of cybercrime on a global level. Also, the majority of countries that are taking effective legislative steps to address the issue of cybercrime are developed countries. It therefore is evident that a global body holds the key in ensuring that developing countries participate with developed countries in evolving a harmonised cybercrime legislation. A regional initiative cannot ensure the acceptance of all nations into its cybercrime legislative initiative, but a global body will be well suited to address the menace of cybercrime through the creation of global harmonised cybercrime legislation and global cooperation.[889] The UN has almost all the countries of the world as its members[890] and, therefore, will be well suited to bring into existence global harmonised cybercrime legislation. In achieving this, it is submitted that the UN could make use of an arm of its organisation, for instance the ITU, to negotiate and draw up a harmonised cybercrime framework with the active participation of all member states, which will be ratified by the General Assembly.

It will also be expedient that other international and regional bodies that have made concerted efforts to legislate on, prosecute and/or investigate transnational cybercriminal activities should make some input into the global agreement.[891] Also, players such as human rights agencies, trans-border law enforcement agencies and other bodies that have taken steps to ensure that law and order is achieved in cyber-

887 These steps were proposed by Alkaabi *et al* problem of cybercrime 12.

888 Alkaabi *et al* problem of cybercrime 12.

889 Harley http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/ (Date of use: 10 October 2013). See also Alkaabi *et al* problem of cybercrime 12.

890 Only three countries are not members of the United Nations. See Rosenberg http://geography.about.com/od/politicalgeography/a/nun.htm (Date of use: 10 October 2013)

891 Alkaabi *et al* problem of cybercrime 12.

space must be identified and their input into this global agreement solicited. Alkaabi *et al* opine that existing and accepted international legislative initiatives such as the CoE Convention should be referred to in order to provide a foundation for the harmonisation efforts.[892]

b. **Identifying the various sub-players**

Pundits have posited that regional agreements are easier to achieve than a global treaty since regional bodies have a more common purpose.[893] For instance, it was easier to enact the CoE Cybercrime Convention while a proposal for a global treaty had been rejected by the UN.[894] Therefore, harmonisation will be easier and speedier when deliberations on a global legislation are deliberated at the regional level and the regional agreements are passed unto the global body (the UN).[895] The various continental or regional umbrella bodies can create an arm of its organisation to oversee this regional agreement which will be transmitted to the UN as the region's input to the evolution of a globally-acceptable cybercrime legislation.

The regional bodies would be more suited to understand their regions' specific requirements and will be able to identify the extent and impact of a UN cybercrime legislation on its region and how best to implement such legislation in its region.[896] This is so because regional legislations reflect the regions' cultures and common heritage which impacts on the regions' legal systems. Thus, the UN's harmonised cybercrime legislation must consider the various regional requirements, collate these, prioritise the requirements and then incorporate the most essential provisions that will create a globally-accepted cybercrime legislation.[897] Region-specific requirements which will not suit other regions could either be removed entirely from the UN Convention or be made

---

892 Alkaabi *et al* problem of cybercrime 12.
893 Alkaabi *et al* problem of cybercrime 12.
894 Ballard M "UN rejects international cybercrime treaty" http://www.computerweekly.com/news/1280092617/UN-rejects-international-cybercrime-treaty (Date of use: 10 October 2013).
895 Alkaabi *et al* problem of cybercrime 12.
896 Alkaabi *et al* problem of cybercrime 12.
897 Alkaabi *et al* problem of cybercrime 12.

optional for countries that find such requirements essential. The regional deliberations will stem from various national considerations and inputs. Inputs should be made by human rights organisations, law enforcement agencies and other bodies that desire to add to the harmonised efforts and incorporated at the regional level.

c. Establishing effective networking

Any meaningful deliberation by the regional bodies, the UN and other international agencies that make an input into the emergence of the harmonised cybercrime legislation, will stem from an efficient networking and relationship between the negotiating or contributing bodies.[898] Agreements between various national, regional and international bodies are difficult to arrive at, as a result of the varying cultures, priorities and legal systems. Therefore, an effective system of communication, negotiation and bargaining must be worked out.

d. Developing a feasible timeframe

Having a feasible timeframe for regional bodies to deliberate, negotiate, agree on their input, and then transmit the agreement to the United Nations for the harmonised legislation is essential.[899] Also, it will be essential to create a timetable for other contributing international organisations to make their deliberations with their stakeholders, agree on a common input, and transmit same to the UN.[900] Creating a timetable will ensure that various aspects of the work that will go into the creation of the harmonised cybercrime are completed within the given time frame since stakeholders intending to make an input are held accountable to a specified period.[901]

---

898 Alkaabi *et al* problem of cybercrime 12.

899 Alkaabi *et al* problem of cybercrime 12.

900 Alkaabi *et al* problem of cybercrime 12.

901 When timetables are not followed, the defaulting body can be questioned about the delay, issues that led to the delay can be tackled, and countries that hamper the progress can be sanctioned with the help of a higher authority – the UN.

e. Deliberation and reconciliation at the United Nations level

The final step in the harmonisation process will be deliberation on and reconciliation of the various inputs to the Convention.[902] Also, feedbacks and further clarifications may be sent to and from the participating bodies in order to arrive at a final conclusion on the contents of the legislation.[903] After this stage, the General Assembly of the UN can accede to the Convention as harmonised international law on cybercrime.

CONCLUSION

In conclusion, this chapter highlights the need for a joint global consistent effort in tackling the issue of cybercrime. The ubiquitous nature of the internet presupposes that any legislative effort that will effectively tackle e-crime will be a global one with the apt participation of both developed and developing countries. This chapter has looked at the existing efforts of developed countries or regional bodies to provide a consistent legislative framework, and these efforts have failed to provide the desired result.

The chapter has proffered steps that must be taken to achieve a more acceptable harmonised legislative framework which will stem from the participation of all types of economies of the world. The chapter has also demonstrated the importance of having a consistent cybercrime taxonomy that will ensure adequate crime reporting, collaborative working among agencies, knowledge sharing and clear measurement on the impact of cybercrime across jurisdictions in order to take appropriate steps to tackle same. The chapter has also proffered some e-crime classifications that will ensure consistency and enhance various efforts in tackling the menace of cybercrime.

It is imperative that nations, regional bodies and the UN wake up from their slumber, and resolve the various divergent positions that hamper efforts to ensure that the rule of law is witnessed in cyber-space. The UN as a body should rise again as it has risen

902 Alkaabi *et al* problem of cybercrime 12.
903 Alkaabi *et al* problem of cybercrime 12.

before in its defence of human rights, and take steps to forestall the break-down of law and order in cyberspace since it is evident that the economies of nations, the sanctity of human rights/life and the real world/offline world is under threat unless law is allowed to perform its duty of effecting order in any society.

Chapter 4 of this research will focus on pursuing uniformity in global law enforcement as a means of effectively tackling the menace of cybercrime. The chapter will examine the existing law enforcement mechanism employed in addressing cybercrime and shall highlight how the procedural hurdles in investigating, prosecuting and preventing trans-border electronic crime has been a clog in the efforts by committed nations in effectively addressing cybercrime. The chapter will then make a case for the evolution of an online global law enforcement agency which will be an integral part and an offshoot of INTERPOL. The chapter will also make a case for the emergence of an international judicial body that will adjudicate on cybercrime and its attendant issues albeit with an appellate jurisdiction in consonance with the various national judicial systems.

CHAPTER 4

SCALING THE PROCEDURAL HURDLE IN CYBERCRIME PROSECUTION AND PREVENTION – A COMPARATIVE STUDY ON HOW TO MAKE DEVELOPING COUNTRIES PART OF THE PROCESS

INTRODUCTION

Various countries, regional and international bodies have taken some initiatives to address the menace of electronic crime. Unfortunately, addressing trans-border crimes has been beset by several procedural hurdles both in the offline and the online world. These procedural hurdles, coupled with the concept of jurisdiction and sovereignty of nations, hamper the investigation, prosecution and eventual prevention of these transnational crimes. For instance, where an IT crime originates from a developing country and is routed through various national jurisdictions, investigating and prosecuting such offence will be impossible without the requisite international collaboration within the various national legal frameworks.[904] The challenges posed by these hurdles become more prominent in tackling IT crime because online activities, among other challenging features, are carried out with a high degree of anonymity.

Most developed countries that have taken significant steps to ensure that their citizens are protected from various trans-border crimes are embarking on giant strides to ensure that they find a way around these procedural hurdles. Their law enforcement agencies collaborate and go to great lengths to ensure that the barriers placed by national sovereignty and jurisdiction are scaled in order to bring a criminal to justice, albeit with many failures.

---

904 Golubev V "International cooperation in fighting cybercrime" http://www.crime-research.org/articles/Golubev0405/ (Date of use: 15 February 2014).

Developing countries, for their part, have done little to tackle electronic crime within its borders and thus find trans-border crimes and their challenges daunting. Therefore, they take few or no steps once the cyber-criminal activity goes beyond its national realm.

Cybercrime, a crime which most often is transnational, cannot be adequately addressed without law enforcement agencies finding some way around the procedural hurdles besetting trans-border crimes. Furthermore, developing countries must be an integral part of this solution because leaving them behind will mean that the procedural barriers will be reinforced when the offending criminal activity emanates from such developing country.

This chapter examines the procedural hurdles that hamper the investigation, prosecution and prevention of trans-border electronic crime. The chapter will concentrate more on transnational cyber-criminal activities. The chapter will also make more reference to investigation since investigation leads to the apprehension and prosecution of the perpetrator, and the eventual prevention of further criminal activities.

The chapter observes that the present synergy existing between various law enforcement agencies has failed to provide the desired solution to the procedural hurdles that bedevil the investigation and prosecution of trans-border cyber-criminal activities. The chapter further observes that the inability of developing countries to be an integral part of this synergy further exacerbates these procedural hurdles.

The chapter posits that the emergence of a uniformed law enforcement agency that will transcend the procedural barriers that characterise trans-border crime holds an important key in investigating, prosecuting, preventing and tackling cybercrime. The chapter also posits that the emergence of an international judicial body that will adjudicate on issues peculiar to cybercrime, albeit mainly with an appellate jurisdiction,

will ensure compliance with the regulatory mechanisms put in place by the harmonised cybercrime legislative initiative and the uniformed law enforcement agency.

Any effort to instil justice and security in cyberspace can be achieved only through the instrumentality of international law and the concerted efforts of international law enforcement bodies and an international judicial institution.[905]

4.1. PROCEDURAL HURDLES IN THE INVESTIGATION, PROSECUTION AND PREVENTION OF CYBERCRIME

The capability of any criminal law to successfully deter any criminal activity lies in its ability to bring culprits to justice, with adequate forms of punishment meted out to the offender, thus preventing future occurrences.[906] Consequently, bringing offenders to justice lies in the ability of law enforcement bodies to properly investigate and prosecute offenders in a competent court of law. Investigating and prosecuting crime involves piecing various pieces of a puzzle together to find the culprit, assessing and gathering evidence from various locations and scene/s of the crime, putting those evidence together in a format that is admissible in court, arresting the culprit, interviewing the suspect and successfully putting the case forward before the judge or jury in a way that they can appreciate the evidence in order to find the culprit guilty.

Investigating and prosecuting trans-border crimes involve a barrage of hurdles which transcend the already difficult terrain of crime investigation and prosecution in a specific national/local jurisdiction. The investigation and prosecution of internet crime, which are mostly trans-border, are more complicated than other trans-border offences and the

905 Schjølberg S "Potential new international legal mechanisms against global cyber-attacks and other global cybercrime" http://www.cybercrimelaw.net/documents/New_international_legal_mechanisms.pdf (Date of use: 15 February 2014).

906 The essence of punishing a criminal offence is not merely to inflict some pain on the offender, or appease the person wronged, but punishment is also meant to make the said crime less attractive to future offenders who are restrained by their knowledge of the consequences of the action they intend to embark upon. Thus, punishment helps prevent crime.

challenges more daunting as data is intangible, cased with a high degree of anonymity and can move across national precincts within seconds.

The challenges that cybercrime investigation and prosecution presents include:

a. JURISDICTION

A major challenge faced by law enforcement agencies in the investigation and prosecution of online crime is jurisdiction. The challenges of jurisdiction transcend the issue of the law that will be applicable in prosecuting a cybercrime offender.[907] It emphasises the question of which country will take the lead in the investigation and prosecution in cases where various national interests are involved.[908] It also brings to the fore the fact that the offending activity may have been routed through several other countries with detailed records (evidence) of the offending communication scattered on different servers on different continents. It further brings to fore the question of the state/court in which the proceedings will be conducted, especially in cases where the offence committed affected several countries or where the victim and offender are in different national jurisdictions.[909] Again, challenges of jurisdiction can result in situations where no state will be willing to investigate or prosecute an offence because the offence cuts across a number of national boundaries.[910]

Conflicts in procedural laws and substantive laws of the various countries would also raise a major challenge.[911]

---

907 Westby JR (ed) *International guide to cyber security* (ABA Chicago 2004) 42-61.

908 Westby *International guide to cyber security* 42-61.

909 Smith RG "Impediments to the successful investigation of transnational high tech crime" http://www.aic.gov.au/publications/current%20series/tandi/281-300/tandi285.html (Date of use: 15 February 2014).

910 Smith http://www.aic.gov.au/publications/current%20series/tandi/281-300/tandi285.html (Date of use: 15 February 2014).

911 Smith http://www.aic.gov.au/publications/current%20series/tandi/281-300/tandi285.html (Date of use: 15 February 2014).

Traditional international law bars nations from carrying out investigations in another state's territory without the consent of that state where the investigation is being carried out.[912] Thus, when a crime emanates from a foreign country, the law enforcement agencies of the target country must seek and obtain the collaboration of the law enforcement agencies of the said foreign country. The law enforcement agency may have to obtain clearance to enter the foreign country, locate the criminal, take custody of the criminal, access the crime scene, take possible custody of the crime scene/equipment/computer used in perpetrating the act and extradite the criminal for possible prosecution.[913] These objectives cannot be achieved in isolation and without the positive contribution of the foreign country. States have to rely on various legal assistance mechanisms to bridge the gap between their powers to prescribe laws and their ability to enforce such laws when offenders are not within its territorial precincts.[914] Brenner points out that it already is a huge challenge to obtain evidence from a foreign state, and a bigger challenge to obtain custody of the suspect.[915]

The affected country may be constrained to rely on the law enforcement agencies of the offender's residence/location in investigating the crime or extraditing the offender.[916]

The challenges of jurisdiction, however, can be eased somewhat by the existence of a mutual agreement between both countries with regard to trans-border crime and extradition.

---

912 Bellia PL "Chasing bits across borders" http://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1430&context=law_faculty_scholarship (Date of use: 15 February 2014).

913 Megias A "Internet law: How cyber jurisdiction affects cybercrime prosecution" https://www.ibls.com/internet_law_news_portal_view.aspx?s=articles&id=32E51BFD-F186-4DEB-B121-F49D060E8118 (Date of use: 28 February 2014).

914 Bellia http://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1430&context=law_faculty_scholarship (Date of use: 15 February 2014).

915 Brenner SW *Cybercrime: Criminal threats from cyberspace* (Greenwood Publishing California 2010) 142-148.

916 Finklea KM "The interplay of borders, turf, cyberspace, and jurisdiction: Issues confronting US law enforcement" http://www.fas.org/sgp/crs/misc/R41927.pdf (Date of use: 3 March 2014).

Varying legislative initiatives can also push up jurisdictional barriers in the investigation, prosecution and further prevention of IT crimes.[917] For example, the principles of double criminality dictates that where an action is illegal in one country and legal in the second country, the first country seeking extradition of the offender who has taken refuge in the country where the action is legal will find it difficult to elicit the cooperation of the second country since the action is not an offence the in its jurisdiction.[918] Varying laws, therefore, act as an obstacle in investigating and prosecuting E-crimes.[919]

The country harbouring the offender may not have adequate procedural laws that will assist the law enforcement agents from the country affected by the criminal activity in taking custody of the culprit and accessing the crime scene for prosecution.[920]

The existence of overlapping investigative authority between national law enforcement agencies increases the friction between agencies that should otherwise have synchronised their investigative capabilities to apprehend an offender, but instead are preoccupied with locking horns in jurisdictional battles.[921]

Countries seeking to circumvent the restrictions posed by certain jurisdictional challenges resort to various traditional legal mechanisms to assist in the investigation, prosecution and eventual prevention of transnational e-crime. For instance countries often place reliance on the following:

- **Voluntary cooperation between governments and their law enforcement agencies**

---

917 Finklea http://www.fas.org/sgp/crs/misc/R41927.pdf (Date of use: 3 March 2014).

918 The principles of double criminality dictates that for extradition to take place, both the country seeking extradition and the one from where extradition is sought must have criminalised the same offence in their jurisdictions. See Sliedregt E and Stoitchkova D "International criminal law" in Joseph S and McBeth A (eds) *Research handbook on international human rights law* (Edward Elgar Cheltenham 2010) 241-271.

919 For example, according to the International Centre for Missing and Exploited Children, 53 countries do not have laws prohibiting child pornography. See http://www.icmec.org/missingkids/servlet/NewsEventServlet?LanguageCountry=en_X1&PageId=4877 (Date of use: 9 March 2014).

920 Westby *International guide to cyber security* 42-61.

921 Finklea http://www.fas.org/sgp/crs/misc/R41927.pdf (Date of use: 3 March 2014).

Brenner points out that informal voluntary cooperation is normally created where investigators network, and the opportunity for such networking mainly arises at conferences.[922] Also, such cooperation arises where there is an already-existing affable long-term relationship between the countries.[923] For example, United States agents are willing to assist British agents without the need for formal legal requests.[924]

Unfortunately, this voluntary cooperation most often eludes developing countries since they may not have the resources to network, and state relationships rarely exist between developed and developing countries.

- **Mutual legal assistance treaties (MLAT)**[925]

  Countries enter into these agreements to enable cooperation in requesting, gathering, obtaining and exchanging evidence/information that will enable the investigation and prosecution of trans-border offences.[926] However, legal assistance may be denied on non-existence of dual criminality, political or security grounds.[927]

  Stigall points out that even in the absence of a treaty, countries provide other countries with mutual legal assistance.[928] However, he further points out that most developing countries through their domestic laws create obstacles that will

---

922 Brenner *Cybercrime: Criminal threats from cyberspace* 142-148.

923 Brenner *Cybercrime: Criminal threats from cyberspace* 142-148.

924 Brenner *Cybercrime: Criminal threats from cyberspace* 142-148.

925 MLATs are relied upon when there is an absence of any official basis for some cooperation or obligation to legally assist a foreign country. These treaties outline the measures to be taken in gathering evidence in a foreign nation and also provide for direct communication between central law enforcement agencies of the countries that are parties to the agreement. See Westby *International guide to cyber security* 42-61.

926 Westby *International guide to cyber security* 42-61.

927 Stigall DE "Ungoverned spaces, transnational crime, and the prohibition on extraterritorial enforcement jurisdiction in international law" 2013 *Notre Dame Journal of International and Comparative Law* 1-50.

928 Stigall *Ungoverned spaces* 2013 *Notre Dame JICL* 22.

hamper mutual legal assistance and impair investigative cooperation between law enforcement agencies.[929]

Placing reliance on mutual legal assistance for trans-border investigations are mostly plagued by time-consuming bureaucracies and restrictions.[930] According to Westby, the process of authorising a request by the court in a foreign country may be subjected to time-consuming challenges and appeals.[931] He also observed that the offence for which the request for assistance is made must be in line with the principles of dual criminality[932] and must be an extraditable offence.[933] These principles place certain obstacles on trans-border e-crime investigation.

- **Letters rogatory**

  In gathering evidence, courts sometimes places reliance on letters rogatory to request a judicial body in another independent jurisdiction that a witness resident within that jurisdiction be examined through the use of interrogatories that accompany the request.[934] This method of gathering evidence is not devoid of complexities and is limited in use. Courts issue these letters when there is a pending case for which foreign evidence should be obtained.[935] Responses to

---

929 For example, art 59 of the Libyan Criminal Procedure Code criminalises international cooperation making it impracticable for Libyan authorities to share vital details of domestic Libyan investigation with foreign law enforcement authorities. See the case of *The Prosecutor v Saif al-Islam Gaddafi and Abdullah al-Senussi* http://www.icc-cpi.int/iccdocs/doc/doc1405819.pdf (Date of use: 16 March 2014). See also Stigall *Ungoverned spaces* 2013 *Notre Dame JICL* 22.

930 Westby *International guide to cyber security* 42-61.

931 Westby *International guide to cyber security* 42-61.

932 The principle of dual criminality requires that an offender may be extradited only when the individual's actions are a crime in both the requesting and requested states. See *US v Saccoccia* 18 F 3d 795 (1994). See also http://www.duhaime.org/LegalDictionary/D/DualCriminality.aspx (Date of use: 17 March 2014).

933 Westby *International guide to cyber security* 42-61.

934 Markus Funk T "Mutual legal assistance treaties and letters rogatory: A guide for judges" http://www.fjc.gov/public/pdf.nsf/lookup/mlat-lr-guide-funk-fjc-2014.pdf/$file/mlat-lr-guide-funk-fjc-2014.pdf (Date of use: 10 April 2014).

935 Bellia http://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1430&context=law_faculty_scholarship (Date of use: 15 February 2014).

this letter normally are bedevilled with substantial delays and states will honour this letter by reason of the comity that exists between both states.[936]

- **Extradition**[937]

  In gaining custody of an offender for further investigation and eventual prosecution, enforcement agencies request the transfer of such suspect in a foreign authority's jurisdiction.[938] However, for a country to be bound to accede to a request for extradition from a foreign authority, both countries must have entered into an extradition treaty.[939] The offence for which the offender is sought to be extradited must fall within the list of extraditable offences as agreed by both sovereign nations or mutually recognised as extraditable by both states in the absence of an extradition treaty.[940] Extradition also presents further challenges for law enforcement agencies.[941] For example, before a request for extradition would be sent by the United States to a foreign authority, four basic steps must be followed.[942] First, the Office of International Affairs (OIA) of the Department of Justice is contacted and this office determines the extraditability of the suspect based on a number of factors such as the nature of the offence charge,[943] citizenship[944] and the location[945] of the suspect.[946] The third step is for the OIA to

---

936 Bellia http://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1430&context=law_faculty_scholarship (Date of use: 15 February 2014).

937 Extradition is a legal process where a sovereign nation makes a formal request to another sovereign nation (the requested state) requesting custody of a fugitive located within the jurisdiction and control of the requested state in order to aid further investigation and prosecution of the offender. See Stigall *Ungoverned spaces* 2013 *Notre Dame JICL* 19.

938 Brenner *Cybercrime: Criminal threats from cyberspace* 142-148.

939 Westby *International guide to cyber security* 42-61.

940 Westby *International guide to cyber security* 42-61.

941 Westby *International guide to cyber security* 42-61.

942 http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00602.htm (Date of use: 11 April 2014).

943 The nature of the offence, viability of the trial of the suspect and sufficiency of the evidence to sustain a conviction to determine if the trial commences will justify the cost of the extradition. See Hunt H and Monhait JM "Extradition: Companies should invest in protecting their assets" 2013 *The Legal Intelligencer Journal* 1-3.

944 The citizenship of the suspect is paramount since some countries will not extradite its citizens. See Hunt and Monhait 2013 *The Legal Intelligencer Journal* 2.

945 The location of the suspect is also vital since the absence of treaty or other laws enabling extradition may not exist between the requesting nation and the requested nation. See Hunt and Monhait 2013 *The Legal Intelligencer Journal* 2.

decide whether it will make a provisional arrest, especially where there is suspicion that the suspect may flee the foreign nation.[947] Fourth, the supporting documents required to make the formal request for extradition is submitted.[948] The US Department of State then transmits the documents and makes its request to the foreign nation.[949]

Brenner points out that sometimes when it is evident that the offender is extraditable, and the OIA request for extradition and supporting documents are flawless, the requested state may still refuse the request for extradition.[950] The suspect may further delay his extradition by challenging the request for extradition which may take a long time for the foreign authority to make a decision on extraditing the suspect.[951]

It is evident that the various methods employed by law enforcement agencies to cross jurisdictional boundaries in their investigations, gathering of evidence and prosecution of offenders are inundated by many procedural challenges that hamper the efforts of these agencies. These traditional efforts are not sufficient to properly investigate and prosecute cybercrime offenders with the same promptness and speed that is the main feature of computer crime. These methods can be laced with bureaucratic bottlenecks making investigations and prosecutions slow and cumbersome.[952] The Commonwealth Director of Prosecutions pointed out that, for example, where an offender with sufficient resources decides to challenge every step of the extradition process through the courts, the process will take years to achieve its aim and such delays can frustrate the entire

946 Hunt and Monhait 2013 *The Legal Intelligencer Journal* 2.
947 Hunt and Monhait 2013 *The Legal Intelligencer Journal* 2. See also http://www.ag.gov.au/Internationalrelations/Internationalcrimecooperationarrangements/Extradition/Documents/Factsheet%20Provisional%20Arrest%20Requests.pdf (Date of use: 12 April 2014).
948 Hunt and Monhait 2013 *The Legal Intelligencer Journal* 2.
949 Hunt and Monhait 2013 *The Legal Intelligencer Journal* 2.
950 Brenner *Cybercrime: Criminal threats from cyberspace* 142-148.
951 Hunt and Monhait 2013 *The Legal Intelligencer Journal* 2.
952 Westby *International guide to cyber security* 42-61.

criminal process.[953] He further pointed out that in certain cases, extradition requests have been completely withdrawn because of the duration of the delay or the offender dying of natural causes while prolonging the extradition process, thereby obstructing the path of justice.[954] Brenner also pointed out that in situations where a law enforcement agent relies on MLAT or the letter rogatory to request and obtain evidence, the digital evidence may be deleted before the request reaches the proper authorities.[955]

Stigall, for his part, pointed out that an important element of the investigative[956] trans-border methods is that each mechanism, being requests from one state to another, is designed to respect the sovereignty of the other state, thus rendering the mechanisms ineffective where the requested state is unwilling to assist.[957]

Furthermore, where the offending activity is a capital offence in the target country and the country where evidence/assistance is sought from has abolished capital punishment, the country where evidence is sought from will deny the target country assistance so that its resident or citizen will not be made to face the consequences of a capital offence, namely, death.[958]

b. INFORMATION AND DATA SHARING:

Complications in the investigation and prosecution of cyber-criminal activities arise when multiple law enforcement agencies are involved in the effort. This is further exacerbated by the absence of compatible, centralised and comprehensive data which will impede the agencies' abilities to coordinate its investigations, share information and measure the true scope of criminal activities.[959] For example, in a country such as the

953 Bugg D "Commonwealth Director of Public Prosecutions (2002-2003 Annual report)" http://www.cdpp.gov.au/wp-content/uploads/CDPP-Annual-Report-2002-2003.pdf (Date of use: 16 April 2014).

954 Bugg http://www.cdpp.gov.au/wp-content/uploads/CDPP-Annual-Report-2002-2003.pdf (Date of use: 16 April 2014).

955 Brenner *Cybercrime: Criminal threats from cyberspace* 142-148.

956 Mutual legal assistance, letters rogatory, extradition, informal requests, etc.

957 Stigall *Ungoverned spaces* 2013 *Notre Dame JICL* 42.

958 Stigall *Ungoverned spaces* 2013 *Notre Dame JICL* 42.

959 Finklea http://www.fas.org/sgp/crs/misc/R41927.pdf (Date of use: 16 March 2014).

United States, various law enforcement agencies, such as the Federal Trade Commission, the Federal Bureau of Investigation (FBI),[960] the US Immigration and Customs Enforcement (ICE) and US Postal Inspection Service (USPIS), maintain separate databases on identity theft.[961]

These multiple databases and the inefficient collaboration among agencies deter the effective and speedy investigation and possible prosecution of offenders. Data sharing becomes more complicated where various nations are involved. Nations in the exercise of their sovereignty are unwilling to consistently share information with other nations and, in specific cases where the information is requested, nations are more inclined to protect their jurisdictions and residents.

Finklea further points out that even when law enforcement agencies have erected information-sharing mechanisms among themselves, inter-agency coordination may still not be allowed to take place.[962]

c. ANONYMITY

A key feature of cybercrime is the high degree of anonymity or pseudonymity that characterises the offence.[963] The offender can disguise his identity and bear the identity of another in perpetrating the criminal activity. Rasch points out that the fact that the name of a computer user or offender bears the name of someone within a location and a copy of the offending data is found on a computer account with an identical name and location, all raise circumstantial but not conclusive evidence on the culpability of the suspect.[964] This is so because the ability to use the identity of anyone and to also store files on the individual's computer account makes conclusive proof of the individual's

960 The FBI collaborates with the National White Collar Crime Centre in maintaining a database on identity theft through the Internet Crime Complaint Centre (IC3). See Finklea http://www.fas.org/sgp/crs/misc/R41927.pdf (Date of use: 16 March 2014).

961 Finklea http://www.fas.org/sgp/crs/misc/R41927.pdf (Date of use: 16 March 2014).

962 Finklea http://www.fas.org/sgp/crs/misc/R41927.pdf (Date of use: 16 March 2014).

963 Rasch MD "Criminal law and the internet" in Ruh JF (ed) *The internet and business: A lawyer's guide to the emerging legal issues* (1996) *Journal of the Computer Law Association* 141-148.

964 Rasch *Criminal law* 1996 *Journal CLA* 142.

culpability doubtful.[965] Rasch further points out that where a computer system has been the subject of attack and has been made vulnerable to alteration and destruction, data from the same corrupted system is retrieved and used in evidence, putting the integrity of the retrieved data in question.[966] This further exacerbates the problem of anonymity.

d. SKILL AND EXPERTISE OF LAW ENFORCEMENT BODIES

The level of skill and expertise of law enforcement agencies will determine their ability to successfully investigate a criminal activity. For example, Myburgh points out that the percentage of successful prosecution of crime in South Africa is approximately 6 percent and the percentage for cybercrime is much lower because of its technical nature.[967] E-crime investigations require the gathering of evidence carefully and legally, knowledge of the laws that govern electronic evidence and knowledge of the privacy rights of suspects and victims.[968] It also requires authentication of the retrieved evidence and its analysis.[969] The inability of law enforcement agencies to go through these processes in order to present authentic evidence before a court in a manner stipulated by the Evidence Act and appreciated by the judge/jury will render the prosecution of such offence ineffective. Law enforcement agencies require skilled investigators with detective and technical skills (IT software, hardware and forensic tools), and prosecutors with the requisite knowledge of cybercrime.[970]

Where multiple national law enforcement agencies are involved, which is the norm in transnational cybercriminal activities, the lack of skill and expertise on the part of some

---

965 Rasch *Criminal law* 1996 *Journal CLA* 142.

966 Rasch *Criminal law* 1996 *Journal CLA* 142.

967 Burrows T "SA fails on forensic readiness" http://www.itweb.co.za/?id=62964:SA-fails-on-forensic-readiness (Date of use: 16 April 2014).

968 Bui S, Enyeart M and Luong J "Issues in computer forensics" http://www.cse.scu.edu/~jholliday/COEN150sp03/projects/Forensic%20Investigation.pdf (Date of use: 10 March 2013).

969 Bui, Enyeart and Luong http://www.cse.scu.edu/~jholliday/COEN150sp03/projects/Forensic%20Investigation.pdf (Date of use: 10 March 2013).

970 Wolf U "Cyber-crime: Law enforcement must keep pace with tech-savvy criminals" http://www.digitalcommunities.com/articles/Cyber-Crime-Law-Enforcement-Must-Keep-Pace.html (Date of use: 16 April 2014).

agencies, especially where the crime scene is in a foreign national jurisdiction, will jeopardise any meaningful investigation and eventual prosecution. Most developing countries are victims to this dearth of technical expertise, and this will hamper any effort of a developed country interested in bringing an offender to justice for actions that affected the developed country or its citizens. The assistance of the local staff with jurisdiction over the offender cannot be dispensed with since they are versed with an understanding of the local terrain.

The existence or dearth of skill among law enforcement bodies, prosecutors and even judges is connected to the adequacy of the training, the availability of proper equipment, the availability of adequate funding/resources and the provision of well-defined personnel policies made available to these agencies.[971]

The non-existence of a central international law enforcement body on cybercrime alone contributes to the lack of skill of investigators. The existing international police bodies deal with networking and mere data sharing and not proper multi-jurisdictional investigations.[972] These international police bodies only provide a minute section of their institutions to cybercrime, while the larger part of the organisation deals with other genres of transnational crime. This will not promote any form of skill and expertise in cybercrime investigation.

e. HIGH COST OF INVESTIGATION

Law enforcement bodies have the duty to evaluate evidence and exercise some discretion in deciding whether a criminal activity is to be investigated or abandoned. Several factors, such as the strength of the case, the deterrence value of the prosecution and the government's enforcement priorities, are taken into consideration in

971 Sen ON *Criminal justice responses to emerging computer crime problems* (MSc dissertation, University of North Texas 2001) 48.

972 For example, the core of the duties of INTERPOL revolve around global police networking and communications, databases and sharing operations, training of national police forces, providing various degrees of assistance to local police forces, etc. See http://www.un.org/en/sc/ctc/docs/bestprac-interpol.pdf (Date of use: 16 April 2014).

deciding whether the investigation and prosecution should be continued.[973] The cost of the investigation and eventual prosecution is another important factor to be considered.[974] The high cost of investigation may discourage law enforcement bodies from investigating certain cyber-criminal activities, especially where such investigations cut across multiple agencies, countries and service providers who may be unwilling to assist in the investigation. It seems more economically viable to abandon a transnational IT crime investigation where the damage caused by the offender is lesser than the cost of investigation and, instead, to reimburse the victim for the loss.

f. LOGISTICAL AND ORGANISATIONAL HURDLES

Cybercrime investigation, especially when transnational in nature, entails the emergence of several logistic issues that are liable to crop up. For example, law enforcement bodies will have to establish some contact/communication between both/multiple countries, sometimes at inconvenient times, especially when the time zones vary.[975] Visas may have to be procured for investigating staff to enable their entry into the foreign jurisdiction for the investigation.[976] Documents written in a foreign language may have to be translated and interpreters may need to be procured for the witnesses and the investigating authority for ease of communication where parties speak different languages.[977]

These practical challenges become more difficult where the foreign authority ranks the fight against cybercrime as its lowest priority or encourages same (for financial or

---

973 Nahra KJ "Role of victims in criminal investigations and prosecutions" http://www.insurancefraud.org/downloads/Role_of_Victims.pdf (Date of use: 19 April 2014).

974 Nahra http://www.insurancefraud.org/downloads/Role_of_Victims.pdf (Date of use: 19 April 2014).

975 Smith RG "Impediments to the successful investigation of transnational high tech crime" http://www.aic.gov.au/publications/current%20series/tandi/281-300/tandi285.html (Date of use: 19 April 2014).

976 The application for the right of entry or visas may be refused especially where countries do not have a cordial relationship.

977 Smith http://www.aic.gov.au/publications/current%20series/tandi/281-300/tandi285.html (Date of use: 19 April 2014).

political gain),[978] is uncooperative, or corrupt or has inadequate local staff/police to provide the needed assistance to the visiting law enforcement body.

Where the correct environment and adequate security are not provided to the visiting investigating staff, e-crime investigation becomes a Herculean task, and the investigation and eventual prosecution are often abandoned. For example, Randy Miskanic, the Deputy Chief Postal Inspector, described Nigeria as a very dangerous place for them to work in during the investigations into the activities of some IT crime offenders, thus forcing them to channel their efforts towards other strategies.[979]

g. POLITICAL CHALLENGES

The prevalent political indices/relationship between countries contribute or negatively affect transnational IT crime investigations. Smith *et al* observed that where the political atmosphere between two countries is not cordial and police counterparts are not close, going the extra mile in assisting the apprehension of offenders will be most unlikely.[980] They further observed that even where the perpetrator is identified and there is a binding treaty that compels the nations to cooperate, when parties are disinclined to cooperate, the bureaucratic procedures of transnational investigations can become more complex, halting the entire process.[981]

h. CULTURAL ISSUES

The willingness and ability to assist and cooperate in criminal investigations and prosecutions can be affected by the cultural proclivities of nations. The notion of what amounts to criminality, appropriateness and proportionality of punishments, and

978 Smith http://www.aic.gov.au/publications/current%20series/tandi/281-300/tandi285.html (Date of use: 19 April 2014).

979 Wagley J "Battling cybercrime across borders" http://www.securitymanagement.com/article/battling-cybercrime-across-borders-007995 (Date of use: 20 April 2014).

980 Smith RG, Grabosky P and Urbas G *Cyber criminals on trial* (Cambridge University Press Cambridge 2004) 48-60.

981 Smith, Grabosky and Urbas *Cyber criminals on trial* 57-60.

investigative priorities are invariably tied to the cultural inclinations of a nation.[982] Countries in some situations, in following international trends, can enact laws to combat certain crimes but never implement such laws or even bother to investigate same because of their cultural consciousness. For example, bigamy is a crime in Nigeria, but no police in Nigeria will bother to investigate or prosecute anyone for that as, culturally, Nigerians believe in polygamy.

Kennedy posits that criminal activities in countries that are not adjacent to each other in geographical terms and that culturally largely differ in their widely varied legal systems/codes, pose serious obstacles to achieving any meaningful cooperation in assisting each other in the investigation of transnational crime.[983]

i. LEGAL FACTORS

In addition to the challenges posed by the legal concepts of sovereignty and jurisdiction, as previously highlighted, differing laws and procedures further complicate trans-border investigations. In situations where some countries (especially developing countries) do not update their laws to criminalise certain online activities, offenders who reside in such countries will be difficult to be apprehended by the victim's law enforcement agency because of the absence of the requirement of dual criminality.

KPMG observed that some countries enact restrictive data protection, privacy and labour laws that hamper any meaningful in-depth transnational investigations making obtaining evidence unattainable.[984]

---

982 Maghaireh AMS *Jordanian cybercrime investigations: A comparative analysis of search for and seizure of digital evidence* (PhD thesis, University of Wollonong, 2009) 251-252.

983 Great Britain: Parliament: House of Commons: Home Affairs committee *Justice and Home Affairs Issues at European Union Level* Third report of session 2006-07, Vol 2: Oral and written evidence (The Stationery Office Norwich 2007) 46-63. See also Maghaireh *Jordanian cybercrime investigations* 252.

984 Marais P and Ostwalt P "Cross-border investigations: Are you prepared for the challenge?" http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cross-border-investigations.pdf (Date of use: 21 April 2014).

4.2. UNIFORM LAW ENFORCEMENT – A REQUIRED EVOLUTION

It is evident that many challenges hamper the investigation, prosecution and eventual prevention of cybercrime, especially those that are perpetrated across national borders. In tackling these challenges, law enforcement bodies have attempted to evolve various means of circumventing the restrictions of sovereignty, jurisdiction and other negative factors and of ensuring that offenders and their activities are investigated, arrested and prosecuted. However, the preceding portion of this chapter illustrates that several lingering and daunting challenges either discourage or completely prevent law enforcement bodies from investigating trans-border IT crime. These challenges hamper any meaningful attempts to address the menace. The challenges are more pronounced where developing countries are involved.

In finding a way to surmount these challenges, several scholars have suggested various steps that may be adopted to ensure a smooth transnational investigation. Scholars have also justified some of the steps taken by law enforcement bodies that seek to circumvent the challenges of trans-border investigations. For example, Goldsmith justified the reliance on remote cross-border searches[985] by US law enforcement agencies as legitimate and, in fact, not inimical to the theory of sovereignty.[986] Some states are urging in various international forums that remote cross-border search be recognised, arguing that such power is an essential tool in addressing IT crime.[987]

Other countries (mainly developed countries) rely on intricate deceptive methods to manoeuvre these various jurisdictional impediments and challenges that hamper

---

985 Remote cross-border searches refer to cases where law enforcement agents use computers within their territories to access, examine and download/acquire data physically stored in another national jurisdiction because the data being Date of use: is relevant to their investigation, their own law authorises the search and the conduct being investigated affected persons within their jurisdiction. See Bellia http://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1430&context=law_faculty_scholarship (Date of use: 22 April 2014).

986 Goldsmith J "The internet and the legitimacy of remote cross-border searches" 2001 *Public Law and Legal Theory Working Papers* 1-12.

987 Bellia http://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1430&context=law_faculty_scholarship (Date of use: 22 April 2014).

transnational e-crime investigations.[988] For example, FBI agents investigating Russian hackers[989] (Russian authorities declined to render any assistance) had to lure the hackers to the US for a bogus job interview, asked them to demonstrate their hacking skills, and eventually used the information obtained to obtain evidence from their computer systems in Russia.[990]

Unfortunately these methods relied upon by agencies to circumvent the challenges of transnational investigation still are not foolproof. For example, some scholars argue that remote cross-border investigations end up violating the territorial sovereignty of the originating nation and also violate rights of privacy and free speech.[991] Goldsmith also observes that the fact that the Council of Europe's Convention on Cybercrime failed to authorise such search suggests that international law prohibits same except where there is consent from the originating nation.[992] Goldsmith, in his argument that remote cross-border searches are legitimate, also admitted that such methods could spin out of control and countries who implement such methods would not want the same method used by another country to obtain evidence within their territory.[993]

On the other hand, the reliance on intricate deceptive methods may end up pitting the originating nation against the target nation and stretching the already volatile relationship that caused the originating nation's reluctance to assist the target nation.

The position of developing countries with respect to trans-border investigations and invariably protecting its nationals from inimical transnational cyber activities is deplorable. Andreas *et al* point out that less-developed countries at best host police

---

988 Smith, Grabosky and Urbas *Cyber criminals on trial* 63.

989 The Russian hackers, Ivanov and Gorshkov, were investigated for financial crimes and hacking of the databases of up to 16 US companies, and acquiring information on an estimated 50 000 credit cards. See Jahnke A "Alexey Ivanov and VasiliyGorshkov: Russian hacker roulette" http://www.csoonline.com/article/2118241/malware-cybercrime/alexey-ivanov-and-vasiliy-gorshkov--russian-hacker-roulette.html (Date of use: 22 April 2014).

990 Jahnke http://www.csoonline.com/article/2118241/malware-cybercrime/alexey-ivanov-and-vasiliy-gorshkov--russian-hacker-roulette.html (Date of use: 22 April 2014).

991 Goldsmith *Public law and legal* 2.

992 Goldsmith *Public law and legal* 5.

993 Goldsmith *Public law and legal* 12.

attachés of developed nations, harmonise their criminal laws in line with foreign dictates, ratify international conventions initiated by developed nations and rely on other national/international policing efforts to address their cross-border law enforcement interests.[994] This leaves their trans-border investigative ability almost non-existent except for the little provided for by developed countries.

The status of existing international policing agencies has not ameliorated the challenges faced during cross-border law enforcement. These bodies do not possess the coercive force that a national police authority is supposed to wield within its jurisdiction, but are mostly bodies that enhance cooperation amongst national police bodies, assist national police agencies or provide assistance for other genres of transnational crime. They are either facilitating communication, cooperation and coordination among police officers of member states,[995] as in the case of INTERPOL, or promoting the maintenance of interim order in conflict zones and the training, restructuring, mentoring and re-establishment of post-conflict police services,[996] as in the case of the UN police.[997] However, as Esposito rightly puts it, "the fight against cyber-crime either is a global one or it makes no sense".[998]

4.2.1. ONLINE GLOBAL LAW ENFORCEMENT AGENCY

Several scholars, such as Goldsmith, posit that although sovereignty in cyberspace is a contentious issue, unilateral transnational enforcement and cross-border searches/seizures should be viewed as a necessary legitimate invasion of another

994 Andreas P and Nadelmann E *Policing the globe: Criminalization and crime control in international relations* (Oxford University Press New York 2006) 10.

995 Bowling B and Sheptycki J *Global policing* (Sage Publication London 2012) 1-28.

996 Durch WJ "United Nations police evolution, present capacity and future tasks" http://www3.grips.ac.jp/~pinc/data/10-03.pdf (Date of use: 19 July 2014).

997 The mandate of the UNPOL mostly comes to life in conflict zones, and during such era they can exercise the power of arrest, searches and detention. However, they are not considered law enforcement agents of their host nations and their powers are normally limited. See http://www.un.org/en/peacekeeping/sites/police/work.shtml (Date of use: 19 July 2014).

998 Broadhurst R "Developments in the global law enforcement of cyber-crime" 2006 *International Journal of Police Strategies and Management* 408-433.

country's sovereignty.[999] He further opines that such measures should rather be viewed as part of the inevitably messy process of devising new customary standards and rules of sovereignty to accommodate these emerging criminal conducts on the cyberspace.[1000] Although the concept of globalisation has whittled down the concept of absolute sovereignty, no nation will be willing to give up any aspect of its sovereignty lest the powers and control of its national government be punctured.

In light of the foregoing and other afore-mentioned challenges that trail transnational investigation, prosecution and its eventual prevention, it is submitted that a step in the right direction will be the development of an international crime control mechanism that effectively and efficiently tackles trans-border investigations while not eroding the sovereignty of states. Cybercriminal activities are mostly trans-border in nature.

It is submitted that the correct step is the establishment of an online global unified law enforcement agency. According to Bowling *et al,* the sociology of policing implies that the law enforcement body is saddled with the maintenance of social order through surveillance and coercion.[1001] Social order has been difficult to maintain in cyberspace where a larger percentage of criminal activities perpetrated through it go unpunished, as the sovereignty of nations and jurisdiction act as a clog for national police forces and international law enforcement bodies who do not possess the requisite coercive ability through arrests, seizures and detention.

Bowling *et al* further opined that the power to govern is meaningless without the ability to produce coercive powers. The existing structures of the international law enforcement bodies are limited in their ability to perform extensive surveillance and possess little or no power of coercion and, therefore, cannot ensure compliance with the rules. The former UN Secretary-General, U Thant, in 1963 foresaw some of these impediments and opined: "I have no doubt that the world should eventually have an international

999 Goldsmith *Public law and legal* 12.
1000 Goldsmith *Public law and legal* 12.
1001 Bowling and Sheptycki *Global policing* 129.

police force which will be accepted as an integral and essential part of life in the same way as national police forces are accepted".[1002]

Bowling *et al*, in pointing out that there is a difference between global policing and global police force, observed that unlike global policing, a global police force will possess universal jurisdiction and formal powers to arrest and detain suspects anywhere in the world, while global policing is the capacity for surveillance and use of coercive force without being hindered by jurisdiction.[1003]

The various areas of international vices such as child trafficking mostly are not trans-border and usually are characterised by some form of physical movement of either persons or objects across national borders. However, cyber-criminal activities are mostly transnational, can pass through many national boundaries in seconds and are intangible. Therefore, it is easier for ordinary international police networking/cooperation to deal with such international vices. However, in the case of IT crime, the stakes are higher.

It is submitted that establishing an effective online global uniform law enforcement agency will entail a fusion of the global policing model for the parent law enforcement body with the modified global police force model for the immediate cyberspace law enforcement unit within the parent body.

It is proposed that instead of starting a novel global law enforcement body on cybercrime, which will be a Herculean task, an existing international police body be modified to make room for the online global uniform law enforcement agency.[1004] The online global uniform law enforcement agency will be carved out as a distinct and most prominent unit of the said international police body.

1002 Jacovides A *International law and diplomacy: Selected writings of Ambassador Andrew Jacovides* (MartinusNijhoff Publications Leiden 2011) 155.

1003 Bowling and Sheptycki *Global policing* 129.

1004 The emergence of a new global body will require the consultation, lobbying, assent and input of various diverse national governments which may take decades to achieve.

It is further proposed that the International Criminal Police Organisation (INTERPOL) houses this online global uniform law enforcement agency (as a distinct section of INTERPOL), with the parent body (INTERPOL) maintaining a global policing model of operation while the online global uniform law enforcement agency (a distinct section inside INTERPOL) maintains a global police force model of operation.

The structure of INTERPOL has made it more positioned to adjust some part of its structure into this online global uniform law enforcement agency than the United Nations Police (UNPOL),[1005] the other existing international policing agency.

The following sub-topics will assess the desirability of the use and modification of INTERPOL by looking at the current structure of INTERPOL, subsequently suggesting some modifications that will enable the operation of an effective online global police force.

4.2.1.1. CURRENT STRUCTURE OF INTERPOL

INTERPOL has 190 countries as its members.[1006] Its hierarchy of command, which runs from the General Assembly[1007] to the Executive Committee,[1008] the General Secretariat,[1009] the National Central Bureaus,[1010] the Advisers[1011] and down to the

1005 The work of the UNPOL revolves mainly around peace-keeping missions, building and assisting local police agencies during conflicts depending on the mandate issued to them for each operation, while the duties of the INTERPOL revolve around consistent police collaboration and assistance orchestrated to curb international and trans-border offences. See http://unmiss.unmissions.org/Default.aspx?tabid=4307&language=en-US (Date of use: 22 July 2014). See also http://www.interpol.int/Member-countries/World (Date of use: 22 July 2014).

1006 http://www.interpol.int/Member-countries/World (Date of use: 22 July 2014).

1007 It is INTERPOL's highest body made up of delegates from each member nation and saddled with the responsibility of laying down rules that govern guiding policies of operation, finances, resources and activities of the agency. See http://www.interpol.int/About-INTERPOL/Structure-and-governance (Date of use: 23 July 2014).

1008 This arm of the governing body of INTERPOL is elected by the General Assembly, and headed by the president of the agency. It supervises the execution of policies and decisions reached by the General Assembly and directs the affairs of the agency. See http://www.interpol.int/About-INTERPOL/Structure-and-governance (Date of use: 23 July 2014).

1009 The agency's main implementation body has its main office in France with seven regional offices and is headed by INTERPOL's Secretary-General. This arm of INTERPOL serves as its crime international centre and maintains contact with national and international authorities to enable

Commission for the Control of Files,[1012] ensures the proper devolution of powers and proper representation of member nations in its scheme of affairs.[1013] It also ensures a global presence and input, effective data acquisition and sharing, and efficient/consistent trans-border collaboration among member nations and other relevant international bodies, in order to ensure that transnational crime is tackled and its perpetrators brought to book by the intervening national law enforcement body. INTERPOL, although not an arm of the UN, partners and works closely with the UN under a formal agreement.[1014]

One of the main areas of focus of INTERPOL is cybercrime, and it is committed to capacity building at national and international levels; the harmonisation of various stakeholders; research on cybercrime; and operational and forensic support during cyber-investigations in order to help tackle cyber-crime.[1015]

It is submitted that the current structure of INTERPOL makes it readily acceptable and more inclined to be taken to the next level by adapting its cybercrime division into a global police force model. It will be desirable to adapt its cybercrime division instead of starting from scratch a new law enforcement agency with the global police force model.

---

proper collaboration in tackling crime. http://www.interpol.int/About-INTERPOL/Structure-and-governance (Date of use: 23 July 2014).

1010 This portion of the agency is maintained by the member countries of INTERPOL and links the country's national police with INTERPOL's global network. This provides INTERPOL with the necessary data on crime and its perpetrators, which enables cooperation amongst nations on trans-national investigations and general police work. This arm of INTERPOL is the core of INTERPOL's operations and is manned by well-trained law enforcement officers of the various nations. See http://www.interpol.int/About-INTERPOL/Structure-and-governance (Date of use: 23 July 2014).

1011 Some experts are appointed in an advisory capacity to assist the organisation in some of its areas of interest. See http://www.interpol.int/About-INTERPOL/Structure-and-governance (Date of use: 23 July 2014).

1012 This arm of INTERPOL ensures that the processing of personal data complies with INTERPOL's rules and does not derogate the fundamental rights of the data owners. See http://www.interpol.int/About-INTERPOL/Structure-and-governance (Date of use: 23 July 2014)

1013 See art 5 of the INTERPOL Constitution.

1014 INTERPOL and the UN cooperate and work closely in responding to and assisting in trans-national and national crime, capacity building and public awareness, assisting the UN in implementing its mandates and assisting international courts in their duties. See http://www.interpol.int/About-INTERPOL/International-partners/United-Nations (Date of use: 23 July 2014).

1015 http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime (Date of use: 23 July 2014).

It has a global presence, unlike the European Union law enforcement agency (Europol) and other regional police organisations which possess only regional/continental presence.

It may be posited that any other law enforcement body/organisation apart from INTERPOL that does not emanate from the UN and intends to achieve international acclaim will find it difficult to receive world support. It is submitted that the cybercrime unit of INTERPOL should be modified into a global police force model while every other structure of INTERPOL remains the same.

4.2.1.2. MODIFICATIONS NECESSARY FOR AN ONLINE GLOBAL LAW ENFORCEMENT AGENCY

It is evident that INTERPOL is more poised to adapt some of its existing structure to accommodate a global police force model of operation in combating cybercrime. In order for the adaptation to take place, there must be certain aspects of the existing structure, the governing laws of INTERPOL, in general, and the cybercrime unit, in particular, that must be modified.

It is submitted that certain steps are to be taken to bring about the necessary modifications to INTERPOL that will see the birth of a functional cybercrime police unit. These steps include:

- CREATING THE LEGAL FOUNDATION

  The proper foundation for any legal system is the establishment of rules and norms that will stimulate the change or emergence of a new order. Therefore it is imperative that the rules governing INTERPOL are modified to change the nomenclature of the existing cybercrime unit.

  The Constitution of the INTERPOL must be amended to accommodate the necessary modifications. Article 2 of the INTERPOL Constitution of states that

the two goals of the institution are to promote mutual assistance among police authorities and establish/develop institutions that will contribute to the prevention of crime.[1016] Article 2 of the Constitution therefore should add a third arm to the aims/goals of INTERPOL. The aims/goals of INTERPOL should in line with this adaption be modified to provide that general police powers of arrest, search, seizure and detention should be employed by the cybercrime unit of the organisation as allowed by the rules enacted by the General Assembly and the unified global treaty on cybercrime to which INTERPOL will be a signatory.[1017] It is submitted that the use of general police powers by the cybercrime unit of INTERPOL would be in collaboration with the national police force. However, where the national police force refuses to collaborate/cooperate, INTERPOL can apply for an order of the International Criminal Court for Cyberspace (ICCC)[1018] authorising INTERPOL to conduct its independent investigation with the cooperation of willing nations (like the nations where the transnational criminal activity was routed or the victims are located).

Second, the General Assembly will have to enact rules that will govern the cybercrime unit, its operation, functions and other procedural legal requirements for an efficient performance of cyber-police duties.

The rules and Constitution governing the cybercrime unit of INTERPOL must expand its jurisdiction on transnational IT crime to allow the unit universal jurisdiction among all its member-states that are part of this progressive adaptation. Its jurisdictional powers must be clearly defined and separate from other units.

1016 See art 2 of the INTERPOL Constitution http://www.fd.uc.pt/CI/CEE/OI/INTERPOL/interpol-constitution.htm (Date of use: 23 July 2014).

1017 This research earlier on proposed the need for a unified global cybercrime treaty which UN member nations should be part of.

1018 The International Criminal Court for Cyberspace (ICCC) will be proposed in another section of this chapter.

The rules of this cybercrime unit must define the relationship of the unit with member-states, governments, the prosecution, service providers, academia, judiciary and other stakeholders.[1019] The rules must also state the substantive and procedural law that the unit will be enforcing.[1020]

- PERSONNEL/TRAINING OF THE UNIT

  A major aspect of this modification will be the establishment of the same standard of cybercrime units/office across all member states, to ensure that all units have the requisite capacity to investigate IT criminal activities. It is submitted that the cybercrime unit should be organised into investigative, computer forensics, and data and information analysis sections.[1021] This structure must be replicated in all national (branch) offices of the cybercrime unit to ensure consistency of standards. Each member-state that is a signatory to this modification must have a branch cybercrime unit of INTERPOL located in its national precincts that will form part of the general INTERPOL cybercrime unit working in collaboration with other national/branch offices of the unit and the central office of the INTERPOL cybercrime unit during investigations. Each national/branch office must be equipped with modern investigative, forensic and technological resources,[1022] since INTERPOL already has a robust system of information exchange among member-states with respect to international policing.

  It is proposed that the cybercrime unit will have a head at the INTERPOL headquarters that coordinates the entire activities of the cybercrime unit. The

---

1019 See Schjølberg S "Potential new international legal mechanisms against global cyber-attacks and other global cybercrime" http://www.cybercrimelaw.net/documents/New_international_legal_mechanisms.pdf (Date of use: 24 July 2014).

1020 Chapter 3 of this research recommended the enactment of substantive and procedural cybercrime laws by the UN. These laws promulgated by the UN should be the guiding substantive and procedural law for the cybercrime unit of INTERPOL.

1021 The various sections will have their dedicated staff pooling their synergies together.

1022 Technological resources such as Encase forensic toolkits, mobile phone examiners, digital decryption tools, password recovery and decryption tools, IP location tracers and other equipment that will aid the smooth running of the various offices and investigative labs are essential.

national/branch offices of INTERPOL will also have its head who is answerable to the head of the cybercrime unit at the INTERPOL headquarters. In order to make the work of the head of the cybercrime unit at the international office effective, officers may be appointed to head and oversee the activities of its branches on various continents of the world. This will imply that a national office of a continent may be chosen as the regional office of the cybercrime unit, and the head of that regional office will also double as the head of the national office where the office is situated.

A larger section of the officers at the branch office will be employed from the national police force and other national establishments[1023] of the member-state where the branch is situated. However, as an international body which should ensure transparency, it is suggested that the head of the branch office should not necessarily be a citizen of the nation where the branch is located, so that the branch will not simply become an appendage of the government of the member-state. Being an international body will entail that staff of any branch can be transferred to another branch as the organisation deems fit with the prospects of promotion through the ranks.

The officers will need to be carefully selected and consistently trained. Staff must possess a knowledge of computers, the internet, criminal investigations and rules governing same, cybercrime legislations,[1024] and special qualifications to be well suited for either computer forensics, data and information analysis. A mix of experts, police officers, programmers, analysts, technicians, administrative staff, forensics experts, drawn from the private sector, various member-states, police force would enhance the efficiency of the unit.

1023 The diverse cyber-criminal activities dictate that some staff members may not be core police officers but may be professionals such as psychologists and scientists, who are versed in other aspects of criminal investigations, such as forensics, etc.

1024 Branch staff must have knowledge of international legislation on cybercrime and the national legislation on cybercrime of the country where the branch is located.

It is submitted that prosecutors be appointed who should work closely and for the branch offices to prosecute offenders within the designated courts of member-states. The crop of prosecutors should be lawyers called to the bar of the member-state in question since lawyers are only qualified to practise within designated jurisdictions. These prosecutors must be clearly abreast and up-to-date with the various cybercrime legislations and various legal aspects of the cybercrime investigations and prosecution. The cybercrime unit must train these prosecutors and equip them with the complexities of cybercrime investigations and forensics analysis to enable them to appreciate the intricacies of cybercrime and enable them to present their evidence in court in the manner allowed by law.

It is also submitted that the various branches of the cybercrime unit must be properly equipped with every investigative and forensics tool to enable effective cybercrime investigation.[1025]

- KNOWLEDGE ABOUT THE UNIT AND ITS INDEPENDENCE

  The cybercrime unit must be visible, credible and modelled to be independent of government influences in order to effectively execute its duties.[1026] It is submitted that its activities should be checked by the hierarchy[1027] of INTERPOL and an International Criminal court for Cyberspace (ICCC).[1028] The unit should have the capacity to decide activities that it can investigate and the operational methods for such investigations.[1029] The unit's tools for collection of data, its collaboration with other international and national agencies, prosecutors and courts must be independently done and clearly delineated by its rules and internal norms.[1030]

1025 Ch 2 sub-sections 2.3.1.2. and 2.3.2.2., of this research made reference to essential forensic tools for cybercrime investigation.

1026 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf (Date of use: 1 August 2014).

1027 This would include the General Assembly and the Executive Committee of INTERPOL.

1028 Proposals for an international cybercrime court will be made in other sections of this chapter.

1029 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf (Date of use: 01 August 2014).

1030 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf (Date of use: 01 August 2014).

It is also proposed that a proper awareness of this unit must be created among national police forces, international bodies, individuals and corporate bodies. Complaints about cyber-criminal activities can be made directly to the national/branch office of this unit by an individual, agency or corporate body if the complainant is aware that the offence is transnational. Instances where the branch of the unit through its preliminary investigations finds that the activity is not transnational, the complaint would be transferred to the national police force where the criminal act took place.

The national police force of a member-state can also transfer cyber-criminal complaints with a transnational flavour to the branch office of this INTERPOL cybercrime unit. Thus, where an IT crime is reported to a national police force, the local police must first determine whether the activity is transnational and, once determined, the national police force can transfer the complaint/investigation to the cybercrime unit of INTERPOL.

It is submitted that the involvement of INTERPOL in cyber-criminal police work will be when the criminal activity is transnational affecting member-states that subscribe to this adaptation. The local national police will be versed with the full police powers when the activity is simply within its national precincts. This structure will undoubtably get developing countries involved since the main burden of implementation of cyber-criminal police work is taken off them and placed mainly on the international body. However, this will be done with the participation of member-states who will provide the environment, staff and other contingencies for the operation of the cybercrime unit.

4.2.1.3. BENEFITS OF AN ONLINE GLOBAL LAW ENFORCEMENT AGENCY

The structure and organisation of the unified law enforcement body will ensure that trans-border investigations are more efficient and effective while ensuring that national sovereignty is not eroded.

The various offices of the cybercrime unit of INTERPOL located in each member-state will ensure that investigations can be carried on simultaneously at various national jurisdiction, that is, the target country, the country where the perpetrator resides and countries through which offending data was routed. Issues such as extradition of cyber-criminals will rarely be needed except for possible prosecution at the International Criminal Court for Cyberspace. Extradition may also still be required for areas not criminalised by the uniform Cybercrime Convention since INTERPOL will not have the powers to investigate same or the International Criminal Court for Cyberspace may not adjudicate over same. The existence of various operating offices in each member state will ensure that officers in those operating offices keep abreast with the legal jurisprudence, the political and socio-economic terrain of the country in question, and this will reduce the possibility of the organisation running afoul of the country's legal system.[1031]

To tackle the hurdles of trans-border investigations, there is a need for a consistent international law enforcement body on cybercrime so that cooperation will not be denied or requested afresh when a new cybercriminal activity emerges, or harm is done. A unified international police will ensure that consistent networking and preparation exist. This regime of global policing will minimise the proliferation of safe havens for most cybercrime activities where criminals ordinarily would have flown to in order to escape investigation and prosecution.

The hierarchy that exists within that international enforcement body will ensure that the law enforcement/investigative standard that is obtained in their US office is the same as that in their Nigerian office as the hierarchy provides the operational guidelines, standards, training and equipment.

This law enforcement institution will be independent of national government interference and will possess the powers to recruit its staff and to disengage or sanction erring staff.

1031 Andreas P and Nadelmann E *Policing the globe: Criminalization and crime control in international relations* (Oxford University Press New York 2006) 17-58.

For example, the Nigerian office of the said international law enforcement body will not be manipulated by the Nigerian government, but will rather resemble an embassy of the UN or rather that of the international law enforcement body.

It is submitted that this law enforcement agency will be saddled with the responsibility of policing or intervening only on transnational cyber-criminal activity. The local or national police of each national jurisdiction should maintain its power of coercion within its national precincts and should investigate cyber-criminal activities that take place and are restricted to its national confines.

It is further submitted that individuals or companies affected by any cyber-criminal activity that falls within the purview of the enabling Convention of this global international law enforcement body and which is transnational in nature can complain directly to this international law enforcement body. On the other hand, the local/national enforcement body/police can also transfer cybercrime complaints and investigations that are transnational in nature and can request the collaboration or assistance of this international law enforcement body.

It is observed that where the cybercrime is of a national nomenclature, and it is the duty of the national police to investigate such, the national police, even when corrupt, will be bound to investigate such if the complaint was transferred to them by the INTERPOL. Police in developing countries are normally compelled to act right, when an international body propels them into action.

It is also submitted that INTERPOL remains in its current form but makes an exception in the case of cybercrime. The jurisdiction of the law enforcement body should revolve around certain universally-accepted activities that are delimited as generally offensive such as illegal access, illegal interception, system interference, data interference, forgery, fraud, misuse of devices, offences related to child pornography and any other

offences criminalised by the global uniform cybercrime legislation; which are transnational in nature.[1032]

Developed countries have made concerted efforts in their investigation, prosecution and eventual prevention of transnational cybercrime while developing countries have done little to tackle trans-border IT crime. The inept attitude of developing countries does not mean that developing countries do not have trans-border law enforcement interests; rather they have to either rely on the policing efforts of developed countries or allow the crime to go unpunished because of the technological backwardness and priorities of the developing countries. Therefore,it is this model of online global uniform law enforcement agency, spearheaded by INTERPOL, that can ensure that the challenges faced in cross-border investigations by developed countries and the incapacity exuded by developing countries are overcome. Also, this model will ensure the participation of developing countries.

4.3. PROPOSING AN INTERNATIONAL CYBER-CRIMINAL COURT

A major aspect of the prevention of cybercrime after criminalisation through legislative initiatives and subsequent investigations is the prosecution of offenders in a court of law. Ferencz points out that "there can be no peace without justice, no justice without law and no meaningful law without a court to decide what is just and lawful under any given circumstances".[1033]

Conversely, the same issues such as jurisdiction, varied legislations, and so forth that plague other aspects of IT crime prevention also plague the prosecution of offenders in a competent court. For example, national/local courts in countries that provide a safe haven for IT criminals would also shield them from extradition, assume jurisdiction to

---

1032 Offences that are not necessarily accepted as universal in nature such as "insult to monarchy" or *Lèsemajesté* should not be the preoccupation of this international law enforcement body. See, for example, sec 112 of the Thailand Penal Code.

1033 See Driscoll W, Zompetti JP and Zompetti S (eds) *The International Criminal Court: Global politics and the quest for justice* (The International Debate Association New York 2004) 24-29.

prosecute an offender and yet muddle up the trial and eventually acquit the criminal, denying the target country justice where the cybercrime was committed.

Judge Stein Schjølberg, arguing that cybercrime criminal prosecution needs an international criminal court, suggested adding the most severe cyber-criminal activities to the list of crimes in the jurisdiction of the existing International Criminal Court (ICC) or an outright establishment of an International Criminal Court or tribunal.[1034] It is convenient that, since there is an existing judicial structure on international crime, creating a distinct division that will adjudicate over crime in cyber space with jurisdiction over clearly stipulated areas of cross border IT crime activities will be ideal.

4.3.1. JURISDICTION

It is proposed that an International Criminal Court for Cyberspace (ICCC), which will be a subdivision of the International Criminal Court (ICC), should be established mainly as an appellate court although with a trial section (to deal with certain cases). Appeals to this court will lie from various national courts of the member-states. The Court's jurisdiction should revolve around stipulated global cyber-criminal activities which are transnational in nature. Thus, where a cyber-criminal activity evolves in a single national precinct, the perpetrators should be prosecuted in the country's national courts and through its various hierarchies of courts.

Conversely, where the criminal activity is transnational and falls within the purview of crimes that are criminalised by international cybercrime law,[1035] the perpetrator is prosecuted at the designated national court,[1036] and appeals will now lie to the International Criminal Court for Cyberspace (ICCC). The determination of the national court that can try the offender can be determined by certain factors. Ordinarily, various

---

1034 Schjølberg http://cybercrimelaw.net/documents/ISPAC.pdf (Date of use: 9 August 2014).

1035 The preceding chapter proposed the emergence of a harmonised cybercrime legislation spearheaded by the UN.

1036 In the case of a transnational crime, a perpetrator can be prosecuted in only one level/hierarchy of a national court (eg a High Court) Once there is dissatisfaction with the rulings or aspects of the trial, any appeal will be sent to the International Criminal Court for Cyberspace.

cybercrime regulations require states to assume jurisdiction over IT criminal activities whenever necessary.[1037] Traditionally, though, countries assume jurisdiction over an individual whose criminal action has an effect on the country, or when the offender is resident within its jurisdiction, or when the cause of action arose within its precincts.[1038] These factors can put a country in a proper position to assume jurisdiction to bring an offender to book.

It is also submitted that the ICCC can still have a trial court where certain cases are tried at that level and can then be appealed against to its appellate division. This situation will arise where the branch/national office of the cybercrime division of INTERPOL, the ICCC Prosecutor or other international/national law enforcement authority shows that the national court of a member-state does not possess the requisite capacity[1039] to effectively conduct the specific IT criminal proceedings. In this situation, the prosecution can take place at the trial division of the ICCC without recourse to the national court.

When there are circumstances where it is evident that the trial at the national court was not diligently prosecuted or the trial were either partial or designed to protect the offender from international responsibility; the ICCC, upon receipt of such appeal complaining of these, can order a retrial at the trial division of the court instead of the national court.[1040]

Natural and juristic persons can be prosecuted in this court for transnational offences that relate to illegal access, illegal interception, data interference, system interference, misuse of devices, forgery, fraud, offences related to child pornography and any other offences criminalised by the global uniform cybercrime legislation.[1041]

1037 For example, see art 22 of the Council of Europe Convention on Cybercrime, 2001 ETS 185.

1038 Rosenblatt B "Principles of jurisdiction" http://cyber.law.harvard.edu/property99/domain/Betsy.html (Date of use: 4 October 2014).

1039 The requisite capacity may refer to knowledge and skills of the judges of the national court to effectively adjudicate over an IT criminal trial.

1040 See also Schjølberg S http://cybercrimelaw.net/documents/ISPAC.pdf (Date of use: 9 August 2014).

1041 Schjølberg S http://cybercrimelaw.net/documents/ISPAC.pdf (Date of use: 9 August 2014).

It will be practicable for the ICCC to be guided by the rules of procedure and evidence already in operation at the International Criminal Court (ICC),[1042] albeit with some modifications that will allow for appeals to be entered from national courts. Schjølberg suggests that individual criminal responsibility for offenders cannot be diminished by state immunity or by hiding under the guise that the criminal act was done for and by the directives of a government or its officials.[1043]

It is submitted that with regard to the transnational and global nature of the cyber-criminal activities that form the pivot of the ICCC's jurisdiction, the Court's jurisdiction should pertain to wilful acts against computer systems relating to illegal access, illegal interception, data interference, system interference, misuse of devices, identity theft, forgery, fraud, offences related to child pornography.[1044]

4.3.2. COMPOSITION OF THE COURT

It is submitted that the proposed ICCC, being an offshoot of the ICC,[1045] be composed of three major organs:[1046] the Chambers,[1047] Prosecutor and Registry.[1048] The Chambers of the ICCC should, in line with the need for judicial participation by member-states, consist of the Pre-trial, Trial and Appeal Chambers. The pool of judges of the

---

1042 The provisions of the said rules of procedure govern both trials and appeals. See International Criminal Court Rules of Procedure and Evidence.

1043 Schjølberg http://cybercrimelaw.net/documents/ISPAC.pdf (Date of use: 11 August 2014).

1044 Schjølberg http://cybercrimelaw.net/documents/ISPAC.pdf (Date of use: 11 August 2014).

1045 The ICC has four organs with the Presidency as the first organ of the Court. The four organs are the Presidency, Chambers, Prosecutor and Registry. The Presidency is responsible for the administration of the ICC; allocates cases to Chambers; coordinates cooperation and agreements with member states; and does judicial review of some decisions of the Registrar. Therefore, there is no need for this organ of court to also exist in the International Criminal Court for Cyberspace (ICCC) since it is a branch of the main ICC body. See http://www.icc-cpi.int/en_menus/icc/structure%20of%20the%20court/Pages/structure%20of%20the%20court.aspx (Date of use: 11 August 2014).

1046 The ICC already has four organs which oversee the entire court. The ICCC being a branch of the ICC should have its officers/organs as subsidiaries to the main four organs of the ICC. See also http://www.icc-cpi.int/en_menus/icc/structure%20of%20the%20court/Pages/structure%20of%20the%20court.aspx (Date of use: 11 August 2014).

1047 The Chambers refer to the judicial divisions and hierarchies of courts that exist within the ICC.

1048 Schjølberg http://cybercrimelaw.net/documents/ISPAC.pdf (Date of use: 11 August 2014).

ICCC, being a distinct judicial division within the ICC, must be a combination of qualified and experienced judges in cyber law, international law, criminal law and procedure and human rights. The judges will be drawn from various member-states.

It is submitted that since the modification proposed for the ICCC is the emergence of a division whose core is its appellate nature, the duties of the pre-trial chambers will be minimal and limited to the situations where the national court of a member-state does not possess the requisite capacity to effectively conduct the specific IT criminal proceedings of a transnational nature. Where such situations arise, the pre-trial chambers of the ICCC can, in line with the existing procedure[1049] at the ICC, issue the Prosecutor upon his application, with the authority to pursue necessary investigative steps to ensure that evidence is preserved.[1050] It is submitted, though, that where INTERPOL works in tandem with the ICCC, it can also bring an application for such investigative steps where a member state becomes uncooperative in its investigations. The pre-trial chambers can also issue warrants of arrest.[1051] The pre-trial chambers, in line with its procedure at the ICC, may conduct preliminary hearings where the prosecutor can present sufficient evidence to establish sufficient grounds to convince the court that the suspect had committed the crime.[1052] It is submitted that part of the preliminary hearing will be to determine, irrespective of the overwhelming evidence, whether the crime is trans-border and whether the national courts cannot adequately try the said offence.

The trial chambers will conduct the trial to determine the suspect's culpability in accordance with the approved international cybercrime treaty. The trial chambers will

---

1049 Art 18 of the Rome Statute of the International Criminal Court.

1050 This aspect of issuing investigative steps to the Prosecutor may rarely be necessary where the ICCC works closely with the cybercrime division of INTERPOL.

1051 http://www.icc-cpi.int/en_menus/icc/structure%20of%20the%20court/chambers/pre%20trial%20division/Pages/pre%20trial%20division.aspx (Date of use: 16 August 2014).

1052 http://www.icc-cpi.int/en_menus/icc/structure%20of%20the%20court/chambers/pre%20trial%20division/Pages/pre%20trial%20division.aspx (Date of use: 16 August 2014).

apply all the rules of procedure to ensure a fair trial in determining the guilt or innocence of the suspect.

The appeal chambers as proposed will be the core of the ICCC. Appeals against the judgments of national courts on transnational cybercrime will be in the ICCC appeal chambers. Appeals can be brought on grounds of fairness of the trial, reliability of the proceedings, procedural error, error of facts or law, admission of wrong evidence, severity of sentence, final judgement of the national court or trial chambers and other legal grounds for quashing a conviction or acquittal.[1053] It is proposed that, since the appellate division is the major aspect of the ICCC, and the trial division will receive lesser charges to try, more judges should be appointed to the appeal chambers.

The Prosecutor[1054] will determine whether a case will be sent to the trial court of the ICCC where the national court of a member-state does not possess the requisite capacity to effectively conduct the specific IT criminal proceedings of a transnational nature, or will determine if the case is sent to the Appellate division whether the crime is transnational and has been determined by the national court of a member-state, albeit with some dissatisfaction by either party to the proceedings. The Prosecutor will also prosecute persons on behalf of the complaining government and victim of the criminal act. It is also submitted that member-states upon application to the ICCC can nominate an individual to prosecute a suspect on behalf of the nation state or victim.[1055]

The Registry will perform the administrative and non-judicial aspects that will ensure the smooth running of the court. It is submitted that the various heads of the organs of the

---

1053 http://www.icc-cpi.int/en_menus/icc/structure%20of%20the%20court/chambers/pre%20trial%20division/Pages/pre%20trial%20division.aspx (Date of use: 16 August 2014).

1054 The role of the Prosecutor of the ICC is to determine the cases that will be opened for investigation, investigate such cases and prosecute the perpetrators of such acts that border on war crimes, genocide and crimes against humanity. See http://www.icc-cpi.int/en_menus/icc/structure%20of%20the%20court/office%20of%20the%20prosecutor/faq/Pages/faq.aspx (Date of use: 16 August 2014). However, the role of the Prosecutor under the ICCC will be rather minimal since the investigation work is carried out by the law enforcement agency and in line with this research –INTERPOL does the investigation.

1055 The nominated Prosecutor, however, will perform his duty under the supervision of the ICCC Prosecutor.

ICCC – Chambers, Prosecutor and Registry – can be deputies of the heads of the organs in the larger ICC since the ICCC will be a subsidiary of the ICC.

A major benefit of the judicial system proposed above is that judges of the ICCC, both at its trial section and the main appeal section, will be versed in IT crime issues. The appellate nature of the ICCC will enable the ICCC and the international community keep tabs on how developing countries and other countries are doing in terms of the prevention, investigation and prosecution of cybercrime. For example, when matters are sent to the appellate chambers of the ICCC from the national court of a member-state, the proceedings of the events in the lower (national) court are sent to the appellate court, where the appellate court reviews the events to establish whether injustice has been occasioned or not. When the appellate chamber reviews the events at the lower/national court and finds that the law enforcement investigations was shoddy, that the system of crime prevention in the said member-state is inadequate or the prosecution performed a lax job, these inadequacies of the member-state will be seen during the review of the case and will be made open through the judgment of the appellate chambers of the ICCC. This will compel the law enforcement bodies of member-states (especially developing countries) to take the necessary steps to adopt and apply internationally-acceptable standards in combating the menace of cybercrime, since such negative *obiter dictum*/reports will be available to the international community with the possibility of sanctions.

Another benefit of the proposed judicial system is that it provides a way round the problems posed by jurisdictions and sovereignty, as highlighted earlier. Also allowing the national courts to try the case (except for cases where it is expedient that the ICCC tries the matter in the first instance) will reduce the cost of criminal defence to the suspect.[1056]

[1056] For example, obtaining a legal practitioner to represent an accused person in an international court will be more expensive for the accused person than where the case is tried in a national court.

The selection/appointment of judges and other officials of the ICCC from across various countries, especially developing countries, will enhance the involvement of developing countries in the fight against cybercrime. This is because an appointee from a developing country is like a representative of the country and will try his best to pass across the international best practices to his home-country.

INTERPOL, as proposed earlier, can directly send cases to the ICCC trial chambers through the office of the Prosecutor, and the Prosecutor, in bringing the charge before the trial chambers, must consider whether the national courts of member-states that should exercise jurisdiction do not possess the requisite capacity to effectively conduct the specific IT criminal proceedings of a transnational nature.

The rules of the ICCC will emanate from the existing rules of the ICC and only minimal modifications will be necessary to accommodate the emergence of the ICCC.

However, it is important to note that for the ICC to create a cybercrime division, the Rome Statue establishing the jurisdiction of the ICC has to be amended and expanded to include cyber-criminal offences.[1057]

CONCLUSION

In conclusion, this chapter observes that most cyber-criminal activities are transnational in nature and, therefore, mainly focuses on cross-border IT crimes. The chapter also highlights the procedural difficulties that plague the investigation, prosecution and eventual prevention of IT crime with the existence of jurisdictional boundaries and sovereignty of nations. As already posited, the ubiquitous nature of the internet and the cross-border nature of most IT crimes presupposes that any investigative and prosecutorial effort that will effectively tackle e-crime will be a global one with the apt participation of both developed and developing countries. The chapter examined the

[1057] The Rome Statute grants the ICC jurisdiction to try four core international crimes, namely, genocide, crimes against humanity, crimes of aggression and war crimes. See art 5(1) of the Rome Statute of the ICC.

existing efforts of developed countries to circumvent the limiting effects of jurisdiction and the sovereignty of nations, in bringing offenders to justice. Unfortunately, because of a lack of commitment of some nations, a lack of skills of some nations and the overt connivance of some nations, these efforts have failed to provide the desired result, thus thwarting efforts to bring offenders to justice.

This chapter has proffered several actions that should be embarked upon by the international community with the participation of developed, developing and underdeveloped countries that will aid the investigation, prosecution and eventual prevention of cross-border cybercrime.

The chapter has shown that the re-organisation of the duties of INTERPOL in the manner suggested, to include the policing and investigation of transnational cyber-criminal activities, will engender the participation of developing countries in tackling IT crime while scaling the hurdles posed by the jurisdiction and sovereignty of nations.

The chapter has also shown that an integral part of any legal effort to tackle cybercrime must include the emergence of a judicial system where offenders can be effectively tried. Kofi Annan aptly pointed out that "in the prospect of an international criminal court lies the promise of universal justice".[1058] The chapter has also illustrated that such a judicial body will engender the participation of developing countries in the process, and its appellate nature will ensure that the national courts of developing countries effectively play their role in ensuring that their government agencies properly play their roles in the fight against cybercrime.

It therefore is imperative that nations, regional bodies and the UN come together to make the necessary amendments, legislations/treaties and structural changes in creating the emergence of a modified INTERPOL and International Criminal Court.

1058 Butler AH "The growing support for universal jurisdiction in national legislation" in Macedo S (ed) *Universal jurisdiction: National courts and the prosecution of serious crimes under international law* (University of Pennsylvania Press Philadelphia 2004) 67-76.

These necessary changes will involve the use of the five steps, as enumerated in chapter 3 section 3.4. of this research, namely, identifying the key players; identifying the various sub-players; establishing effective networking; developing a feasible timeframe; and deliberation and reconciliation at the UN level, to achieve these changes.

For a better synergy in tackling the menace of cybercrime, it is submitted that every country that subscribes to the universal cybercrime legislation should also be part of the online global uniform law enforcement agency and the international cyber-criminal court.

It is also imperative that states that refuse to be part of these innovative amendments should receive some level of sanctions to compel their acquiescence. Also, such parties should be made to face some isolation and non-cooperation from other states when such state or its nationals become a victim of trans-border cybercrime. These sanctions are necessary because states that refuse to be part of these innovations will invariably provide a safe haven for IT crime offenders.

The succeeding chapter of this research – chapter 5 will dwell on how to enlist the active support and participation of developing countries in addressing the menace of cybercrime. The chapter will consider the socio-economic factors that cause or exacerbate the apathy of developing countries in addressing electronic crime.
The chapter will proffer various socio-economic strategies that may be employed to get developing countries to join its counterparts from developed countries in taking proactive steps in fighting e-crime.

CHAPTER 5

ENLISTING THE SUPPORT OF DEVELOPING COUNTRIES IN FIGHTING CYBERCRIME: A SOCIO-ECONOMIC APPROACH TO ACHIEVING SAME

INTRODUCTION

The challenges that hamper any meaningful quest to adequately address the dangers of cybercrime are daunting as they affect nations, companies and individuals. Developing countries seem to be weighed down by several factors that compound their apathy in taking adequate steps in effectively tackling cybercrime. Unfortunately, since cybercrime is a ubiquitous phenomenon transcending national boundaries, the indifference of developing countries in taking appropriate measures in fighting e-crime will negatively impact on the efforts of developed countries in addressing the issue. Therefore, it is imperative that the support and active participation of the governments, companies or institutions and individuals in developing countries be obtained in order to complement the efforts of developed countries in effectively tackling internet crime. Unlike most trans-border criminal activities, developed countries can fashion out methods to stop the offending criminal act from physically crossing its borders into its jurisdiction.[1059] Unfortunately, the situation is different in the case of e-crime, which requires no human carrier to pass the offending act through a nation's physical borders. Developed countries cannot play the ostrich pretending that e-crime is the problem of developing countries, or a problem they can solve without the active participation of developing countries.

[1059] For example, drugs, weapons and other illegal commodities that can be physically perceived by the five human senses can be stopped at a nation's border.

Getting a sovereign nation that has not made e-crime its priority to embark on decisive steps that will augment the efforts of progressive developed nations (in this instance, nations that are taking adequate steps to address e-crime) will involve much persuasion and socio-economic pressure on the part of the sovereign nation to take the cue of the progressive nations.

This chapter posits that there are various socio-economic factors that elicit the apathy of developing countries in addressing electronic crime. The chapter will point out some of these socio-economic factors[1060] that exacerbate the apathy of developing countries in lending their active and effective support in addressing internet crime. The chapter will proffer steps that should be taken by developed countries to assist in dealing with these socio-economic factors and the steps that should be taken by developing countries alike**.**

This chapter proposes that through certain socio-economic initiatives, developed countries can drive developing countries into taking some concrete steps that will tackle IT crime. These socio-economic initiatives can elicit at least an expected minimum standard or requirement from the developing countries. These minimum standards include establishing up-to-date cybercrime legislation; modern technologically-compliant law enforcement initiatives; contemporary technological resources; capacity building for law enforcement agencies; and judicial bodies. These persuasions may involve the use of civil societies, corporate bodies, public institution and the like. The chapter examines various socio-economic steps that should be embarked upon to enlist the support of developing countries in fighting cybercrime.

5.1. SOCIO-ECONOMIC FACTORS THAT CAUSE THE APATHY OF DEVELOPING COUNTRIES IN ADDRESSING E-CRIME

[1060] Some factors have already been dealt with in previous chapters of this research. The previously highlighted challenges will just be identified in this chapter without placing much emphasis on them.

Various theories on crime posit different factors that propel deviant behaviour in individuals. According to these theorists, these factors[1061] influence personal beliefs, needs, desires, and strategies of behaviour which eventually determine the choices that individuals make to either stay on the right or wrong side of the law.[1062] Certain societal influences determine behavioural customs, values attached to material goods, perception of the cost and benefits of an action, and the strength of self-control to resist the alluring benefits of illegality.[1063] In trying to identify the foundation behind deviant behaviour in individuals, scholars have propounded several theories such as the rational choice theory;[1064] the social disorganisation theory;[1065] the social learning theory;[1066] the social control theory;[1067] the labelling theory;[1068] the strain theory;[1069] and

---

1061 These factors are culturally and socio-economically determined.

1062 Schiller J "Crime and criminality" http://www.des.ucdavis.edu/faculty/Richerson/BooksOnline/He16-95.pdf (Date of use: 11 January 2015).

1063 Schiller http://www.des.ucdavis.edu/faculty/Richerson/BooksOnline/He16-95.pdf (Date of use: 11 January 2015).

1064 The rational choice theory proposes that individual actions are propelled by self-interest which causes the individual to make decisions to commit an offence after weighing the rewards of the illegality with the potential risks, punishments and chances of getting caught. See Briggs S "Important theories in criminology: why people commit crime" http://www.dummies.com/how-to/content/important-theories-in-criminology-why-people-commi.html (Date of use: 11 January 2015).

1065 The social disorganisation theory posits that the environment (social structures) determines the individual's behavioural choices. Crime becomes more prevalent in economically-disadvantaged societies, thus reducing the capacity or enthusiasm of community inhabitants to implement effective social control. See http://law.jrank.org/pages/818/Crime-Causation-Sociological-Theories-Social-disorganization-theory.html (Date of use: 11 January 2015). See also Briggs http://www.dummies.com/how-to/content/important-theories-in-criminology-why-people-commi.html (Date of use: 11 January 2015).

1066 Social learning theory propounds that an individual's association will determine the individual's drive to commit crime and develop his skills in effecting his criminal activity. See Briggs http://www.dummies.com/how-to/content/important-theories-in-criminology-why-people-commi.html (Date of use: 11 January 2015).

1067 Social control theory stipulates that the bonds that individuals form through people, values and institutions (eg schools, families and religious institutions) restrain them when tempted to commit a crime. Thus, individuals would commit a crime when there is a breakdown in these societal bonds. See Pratt TC, Gau JM and Franklin TW *Key ideas in criminology and criminal justice* (Sage Publications California 2010) 55-67. See also Briggs http://www.dummies.com/how-to/content/important-theories-in-criminology-why-people-commi.html (Date of use: 11 January 2015).

1068 Labelling theory presupposes that conforming persons and people in power (such as judges, politicians, the police) label certain acts as crimes and persons who engage in such activities as criminals. These labels take away certain benefits and opportunities of the offender and affect the self images, reputation or self-rejection of the offender, who eventually continues on the deviant path as a result of the label. See Crossman A "Labelling theory' http://sociology.about.com/od/L_Index/g/Labeling-Theory.htm (Date of use: 11 January 2015).

biology or genetics[1070] as determinant for deviant behaviour. These theories all point to the fact that certain cultural and socio-economic factors underlie the individual's flair for certain criminal activities. The lure of certain offences becomes more appealing and generally acceptable or condoned within economically-disadvantaged societies as in most developing countries, especially when the crime does not physically hurt members of the individual's immediate community or state as in the case of most online crimes.[1071] The economically-disadvantaged society eventually adapts to the custom on the grounds that many of its members are involved in these criminal activities which give the society some benefits, thereby eroding the level of unacceptability of such crimes and eventually crippling the justice system to tackle the crimes. For example, the piracy in Somalia has been reported as having brought some local governance and economic stability to the war-torn and economically-disadvantaged nation, and members of the society support the illegal acts.[1072] This has become the case of e-crime where several socio-economic factors have fuelled the apathy of developing countries in taken effective steps in tackling online crime. In fact, the strain theory aptly captures the situation in developing countries where success is mostly measured by a person's wealth and the failures of the aspiring individual propels him to take illegitimate steps in attaining success.[1073] Corruption, illegality and crimes such as online crime become an acceptable way of life in the society once it reaches the desired success

---

1069 Strain theory propounds that when individuals fail to attain their goals and aspirations through society's approved legitimate means, these failures evoke negative emotions (eg anger and frustration) and the creation of certain pressure on the individual to attain success through other means. Crime sometimes provides a corrective response to the strain put on the individual by the failure. See Agnew R "Strain theories" in Parrillo VN (ed) *Encyclopaedia of social problems* (Sage Publications California 2008) 904-906.

1070 Scholars also propose that genetics, hereditary traits, mental illness and the individual's human make up contribute to reasons why an individual commits certain offences. For example, certain types of crimes are more frequent among certain groups or races, so that sometimes it becomes a stereotype for that race. See Briggs http://www.dummies.com/how-to/content/important-theories-in-criminology-why-people-commi.html (Date of use: 11 January 2015).

1071 For example, Nigerian 419 or advance fee fraud are usually targeted towards foreigners who eventually part with their savings and once the perpetrators spend the money, in most Nigerian societies the individual in fact is praised for his ingenuity.

1072 Laurie D "Report argues Somali piracy benefits, stabilizes economy" http://www.voanews.com/content/report-argues-somali-piracy-benefits-stabilizes-economy-137287138/150635.html (Date of use: 12 January 2015).

1073 Omotor DG "Socio-economic determinants of crime in Nigeria" (2009) *Pakistan Journal of Social Sciences* 54-59.

and does not overtly hurt neighbours, causing society's judicial system to be indifferent to certain criminal activities.

Some socio-economic factors that exacerbate the apathy of developing countries in addressing online crime will be examined below.

5.1.1. POVERTY

Most scholars posit that crime has an intimate connection to poverty.[1074] In fact, Aristotle opined that "poverty is the parent of revolution and crime".[1075] Some scholars posit that every human has the propensity to commit evil. However, the effects of poverty such as hunger, a lack of health care, a lack of basic amenities and opportunities to eventual success, push most offending individuals to the wall and their only reaction is to seek a way of escape which the prospects of crime presents.[1076] An individual's basic desire to survive and lead a life with some level of dignity can make crime seem a more practical path to lead. Online crime is an example of an escape route from poverty and will easily be justified since it is mostly non-violent and the perpetrator's targets are mainly foreigners or corporations. For example, online fraudsters at times target wealthy individuals, foreigners, corporations or institutions as these are viewed as the cause of their predicaments.[1077]

In societies where poverty is prevalent as in developing countries, the perpetrator justifies the act mostly on the grounds that he is only seeking an escape from poverty. The other members of society find it easier to condone the act where they are not the

---

1074 Marinez JL *The link between poverty and crime: Utilizing Ruby Payne's framework of poverty* (MSc dissertation, Texas State University 2013) 2. See also Ward M "Poverty and crime" http://www.nationaldialoguenetwork.org/poverty-and-crime/ (Date of use: 17 January 2015).

1075 Spiegel HW (ed) *The growth of economic thought* (Duke University Press Durham 1991) 23-46.

1076 http://www.shareyouressays.com/84485/short-essay-on-poverty-and-crime (Date of use: 17 January 2015).

1077 Unsuccessful people find a way of exonerating themselves from taking the blame for their failures. They thus blame every other person such as foreigners, rich corporations and individuals without looking inwards for the cause of their failures. They therefore seek ways to justify the harm they inflict on these perceived enemies.

main target of the crime and the crime mostly does not involve violence.[1078] This is typical of e-crime and engenders apathy in addressing the issues. The fact that most people in the developing society who have escaped poverty may have done so through illegitimate means can make them relate with what the poor are experiencing and will condone to some level the illegal activities of the poor once the activity does not harm him or his interests.[1079] This further increases the level of apathy in tackling digital crime.

5.1.2. INEQUALITY

Social inequality manifests in various spheres such as differences in wages and income; power; and general conditions of living, thereby creating social groups within a society and creating disparate opportunities or rewards for the varying social strata.[1080] Scholars opine that these inequalities increase social divisions, status insecurity and competition between the various social classes.[1081] Inequalities also expose persons that are low on the social ladder to the impiety of the powers of the persons on the upper echelon of the social strata.[1082] Some scholars posit that the government unfortunately takes care of the group with the greater influence (the upper class), thereby creating conflict between the government that is trying to subdue the powerless and the powerless who are trying to get themselves into a position of great influence

---

1078 Most online crimes are economic crimes. See Waghorne M "Cybercrime: the scourge of the digital economy" http://www.information-age.com/technology/security/123458137/cybercrime-scourge-digital-economy (Date of use: 17 January 2015).

1079 Most leaders of developing countries acquire their enormous wealth through corrupt practices and thus condone corruption simply because they are not directly affected by these corrupt practices.

1080 Karsedt S "Inequality, power and morals: Criminality of elites and their impact in society" http://www.afp.gov.au/media-centre/publications/platypus/previous-editions/1998/march-1998/inequality.aspx (Date of use: 17 January 2015).

1081 Pickett K "Reducing inequality: An essential step for development and well-being" http://www.progressiveeconomy.eu/content/reducing-inequality-essential-step-development-and-en (Date of use: 17 January 2015).

1082 Pickett http://www.progressiveeconomy.eu/content/reducing-inequality-essential-step-development-and-en (Date of use: 17 January 2015).

and power.[1083] Crime, therefore, presents the individual at the lower rung of the social ladder with an avenue to escape the attendant disadvantages of the lower rung.

Unfortunately, in most developing countries the governments usually are compelled to take adequate steps in addressing a crime and protecting the group with the greater influence where the members of the upper class become mostly affected by the crime in question. This makes the government apathetic to crimes that normally do not affect the group with greater influence.[1084] For example, in Nigeria the government and law enforcement agencies never took the issue of kidnapping serious when it was confined to the south-south region of Nigeria and foreign expatriates usually were the target.[1085] When there was a dearth of expatriates and the menace spread to other parts of Nigeria, the upper class (especially politicians) took appropriate steps because they had become targets of the crime.[1086]

In some instances where the powerful (for example legislators, politicians and judges) take steps to subject the powerless into obedience, the steps may not yield perfect results as some members of the lower rung on the social ladder (for instance, low-cadre law enforcement agencies or the police) will be instrumental in any meaningful implementation of the policies of the powerful. For example, when the legislature criminalises an act, the implementation and investigations may be frustrated by the police who are sympathetic to the plight of the perpetrator. Also, certain members of the upper class that are not affected by the criminal activities (as in the case of online

1083 Gilbert K and Sookram S "The socio-economic determinants of violent crime in Jamaica" www.sta.uwi.edu/conferences/09/salises/documents/K%20Gilbert.pdf (Date of use: 17 January 2015).

1084 Most online crimes emanating from most developing countries are usually targeted at foreigners. See Garson P "Cybercriminals find wonderland in developing countries" https://www.opendemocracy.net/opensecurity/philippa-garson/cybercriminals-find-wonderland-in-developing-countries (Date of use: 20 January 2015).

1085 http://www.scholarsworks.com/origin-problem-curb-kidnapping-problem-nigeria/#sthash.8dYOjJfQ.dpbs (Date of use: 20 January 2015). See also Adibe J "Pervasive kidnapping in Nigeria: Symptom of a failing state?" http://www.hollerafrica.com/showArticle.php?artId=304&catId=&page=1 (Date of use: 20 January 2015).

1086 Odiegwu M "Fighting kidnappers with death sentence" http://www.punchng.com/politics/fighting-kidnappers-with-death-sentence/ (Date of use: 20 January 2015). See also Agbaje O "Kidnappers to target politicians – Ozekhome" http://sunnewsonline.com/new/?p=38186 (Date of use: 20 January 2015).

crime) will be apathetic to the criminal activity or may be apathetic simply because they used to be victims of the inequality.

5.1.3. CULTURAL INDICES[1087]

Communication and interactions within primary groups in a society create the learning process where knowledge about certain criminal behaviour sometimes is acquired.[1088] These interactions, when fused with motives, emotions, drive and impulses, propel the offender to decide whether the consequences of his action outweigh the likely benefits of the criminal act.[1089] This is because human needs, desires and values can be satisfied either through criminal or legitimate means, and an individual's interaction contributes to the option he follows.[1090] When certain misbehaviour becomes part of the cultural proclivities in a society, the fact that economic and political pressure and processes[1091] compel the government to outlaw the offence does not cure the apathy of the members of society and that of the enforcers of the judicial system. Fighting those culturally-permitted crimes becomes difficult. A culture of crime can be developed over a period and, although outlawed, will not receive a high level of enthusiasm to tackle it because it has been entrenched into the system as part of the cultural awareness of the community. For example, in Nigeria bribery is so common that for an individual to be motivated to perform his duty he must be given money.[1092] Bribery, although

---

1087 Culture is a factor that determines social development and therefore can be classified as part of some socio-economic dynamics that determines government or national inclinations and policies. See Tylus K "Culture as a factor of social and economic development - the Polish experience" http://www.poieinkaiprattein.org/economy/culture-and-economy/culture-as-a-factor-of-social-and-economic-development---the-polish-experience-by-karolina-tylus/ (Date of use: 20 January 2015).

1088 Matsueda RL "Social structure, culture, and crime: Assessing Kornhauser's challenge to criminology" in Cullen FT *et al Challenging criminological theory: The legacy of Ruth RosnerKornhauser* (Routledge Publishers New York 2015) 117-143.

1089 Matsueda *Social structure* 124.

1090 Matsueda *Social structure* 135.

1091 Scholars have posited that many societies achieve certain levels of social order from political, economic and organisational processes and not from values, cultural or moral consensus. See Alexander JC "Analytic debates: Understanding the relative autonomy of culture" in Alexander JC and Seidman S (eds) *Culture and society: Contemporary debates* (Cambridge University Press 1990) 1-66.

1092 Okoye SE "How to tackle corruption effectively in Nigeria" http://www.gamji.com/article4000/NEWS4930.htm (Date of use: 29 January 2015).

outlawed[1093] in Nigeria, has become part of Nigerian culture and has acquired another euphemism, PR,[1094] that investigating or prosecution bribery is met with so much apathy.[1095]

5.1.4. ABSENCE OF EFFECTIVE REWARD OR PUNISHMENT SYSTEM

The presence of a proficient reward system will encourage citizens to stay on the side of the law while an effective punishment system will deter individuals from engaging in criminal acts. Control theorists posit that crime is a common human instinct as it is easier to cater for human desires through illegitimate activities than through legitimate means.[1096] For them, people drawn to the allure of crime are only discouraged by the controls and restraints put in place in society to deter such criminal instincts.[1097] Controlling crime through a system that rewards or punishes offenders is a major key in addressing crime. Unfortunately, a major feature in most developing countries is the inability to punish deviant behaviour and to even reward or celebrate such deviant behaviour, while leaving good behaviour uncelebrated.[1098] For example, individuals who steal large sums of money in Nigeria use the judicial system to protect themselves from prosecution, and society ends up celebrating them.[1099] A system that fails to adequately punish offenders encourages the increase in crime and the apathy towards doing the right thing will wane daily. The absence of appropriate rewards and punishment in a society creates apathy in tackling such crime since addressing it is futile when offenders are not punished and law-abiding citizens equally are not rewarded. It is simply a societal misnomer.

1093 Sec 98 Nigerian Criminal Code Act, Laws of the Federation 2004.

1094 PR is the short form of Public Relations.

1095 http://sheltersuites.net/why-are-hotels-in-nigeria-so-expensive/ (Date of use: 29 January 2015).

1096 Pratt TC, Gau JM and Franklin TW (eds) *Key ideas in criminology and criminal justice* (Sage Publications Los Angeles 2011) 55- 69.

1097 Pratt, Gau and Franklin *Key ideas* 58.

1098 Suleiman S "Nigeria: Where thieves are rewarded" http://nigerianstalk.org/2014/01/15/nigeria-where-thieves-are-rewarded-salisu-suleiman/ (Date of use: 31 May 2015).

1099 Suleiman http://nigerianstalk.org/2014/01/15/nigeria-where-thieves-are-rewarded-salisu-suleiman/ (Date of use: 31 May 2015).

5.2. SOCIO-ECONOMIC STEPS THAT WILL ELICIT THE PARTICIPATION OF DEVELOPING COUNTRIES IN FIGHTING CYBERCRIME

Fighting certain criminal activities will not be overtly effective by placing reliance only on legislative initiatives and the extant judicial system within a national precinct. This is because a government may take some legislative measures and yet exude much apathy in tackling the crime.[1100] In fact, the UN pointed out that it is easier to amend or update a law than to transform people's practices and beliefs.[1101] Matsueda points out that most societies achieve strong social order through economic, political and organisational processes and not necessarily through value consensus.[1102] This implies that where values do not propel lawful actions, power brokers and determinants of economic and organisational indices can propel lawful actions. For example, the use of economic sanctions, trans-border data restrictions and other socio-economic methods can be used as a tool to propel nations without adequate IT crime prevention mechanisms to take decisive steps in addressing electronic crime. Socio-economic factors that plague the smooth operation of any crime-fighting mechanism must be addressed for an up-to-date legislative initiative and a technological-compliant law enforcement system to work. The preceding portion of this chapter has highlighted certain socio-economic factors that aggravate the indifference of most developing countries in taking concrete steps that will augment the efforts of developed countries to tackle digital crime. It is evident that these socio-economic factors cannot be tackled solely by those developing countries that are currently being plagued by such issues. It is clear that external help from developed countries will be necessary; after all, the developed countries are negatively affected by the outcome of the apathy. Thus, it will be imperative that developed countries evolve some socio-economic strategies to help persuade developing countries to take comprehensive and concrete steps in dealing with online crime. These steps will propel developing countries to put in adequate

1100 These legislative steps may be propelled by political pressures from developed countries or simply because developing nations decide to be enthused by the bandwagon effect in keeping with the trend in developed countries just because the developed country criminalised the activity.

1101 https://www.unodc.org/documents/justice-and-prison-reform/Handbook_on_Effective_police_responses_to_violence_against_women_English.pdf (Date of use: 31 May 2015).

1102 Matsueda *Social structure* 119.

legislative measures, effective and technologically-complaint law enforcement mechanisms and adequate capacity for investigators, prosecutors and the judiciary.

Some relevant socio-economic strategies that should be employed by developed countries to help cure the apathy of developing countries in addressing online crime will be examined below.

5.2.1. RESTRICTIONS ON TRANS-BORDER DATA FLOW

The central feature of the internet and globalisation is the flow of data without being deterred by jurisdiction. The gains in global communication enables data to be transferred faster across climes and stored indefinitely, greatly increasing the volume of trans-border flows.[1103] International trade and multinational enterprises now rely heavily on the seamless flow of information across companies, institutions, and geographical boundaries.[1104] Government institutions and various establishments also rely on data across national precincts to conduct their affairs. Education, health care, financial services and human resources are beneficiaries of the advantages of cross-border data transfer.[1105] Banks with a presence in several countries rely on trans-border data to improve its decision making, improve customer experience, develop new products and market their products.[1106] For example, banks such as the Dutch Bank with a workforce of over 75,000 personnel serving over 48 million clients spread across more than 40 countries will rely heavily on trans-border data flows for its operations.[1107] Developed countries previously had restricted the transfer of data to nations without adequate data protection as a measure in protecting its citizens.

The need to promote economic growth and yet protect individuals from falling victim to certain trans-border crimes has compelled several nations and regions to find a balance

1103 https://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00548.html (Date of use: 6 March 2015).
1104 https://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00548.html (Date of use: 6 March 2015).
1105 https://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00548.html (Date of use: 6 March 2015).
1106 Castro D and McQuinn A "Cross-border data flows enable growth in all industries" http://www2.itif.org/2015-cross-border-data-flows.pdf (Date of use: 17 May 2015).
1107 Castro and McQuinn http://www2.itif.org/2015-cross-border-data-flows.pdf (Date of use: 17 May 2015).

between the two. For example, the US Chamber of Commerce posits that businesses use cross-border data to trim down costs, promote economic growth, improve efficiency, prevent fraud, making it imperative that rules that promote the unimpeded flow of data, be put into place.[1108] On the other hand, most developed countries consider data protection as a fundamental human right and a vital aspect of the rule of law that must be respected within the information society.[1109] Therefore, these countries or their regional bodies came up with certain rules or guidelines to create a balance between data protection as a fundamental human right and promoting unimpeded flow of data.

It is submitted that cross-border restrictions can be relied upon as a form of sanction or socio-economic tool that will compel nations adversely affected by trans-border data restrictions to take proper steps to address IT crime. Thus, countries without up-to-date cybercrime legislations, technologically compliant law enforcement agencies and contemporary investigative equipments can have necessary trans-border data restricted from reaching those countries (although with some exceptions) as a socio-economic tool in ensuring compliance. Cross-border data restrictions to jurisdictions that have not set up the minimum standard required to address electronic crime will compel stakeholders in such jurisdictions to take adequate steps in joining the fight against IT crime. This is because unimpeded and unregulated trans-border data flow to and from countries without adequate electronic crime protection simply exposes various parties to varying degrees of IT crime.

In proposing the imposition of certain cross-border data restrictions as a measure to compel developing countries to take adequate steps in addressing IT crime, it is submitted that taking a cue from the extant rules created by developed countries (especially the Organisation for Economic Co-operation and Development (OECD)) on trans-border data flows would be necessary. The OECD principles on trans-border data

---

1108 https://www.uschamber.com/issue-brief/safeguard-cross-border-data-flows (Date of use: 17 May 2015).

1109 Mutai M "Trans-border data flow: Its advantages and disadvantages" https://www.mu.ac.ke/informationscience/index.php/research-publications/staff-research-and-publication-2/category/16-miriam-mutai?download=57:advantages-and-disadvantages-of-trans-border-dataflow (Date of use: 15 March 2015).

flows would be used as a model in proposing certain cross-border data restrictions under this chapter.

The efforts of several sovereign nations to ensure data protection created uneven data protection policies and became a huge hindrance to a seamless cross-border data flow, prompting several international or regional bodies to take steps to balance data protection with effective free flow of data.[1110]

These bodies, such as the OECD, have proposed steps to ensure the harmonisation of national laws and the creation of strict trans-border data legal systems amongst member-states and to ensure free trans-border data flow while restricting data transfers to third countries.[1111] The OECD[1112] thus established certain principles or guidelines to govern trans-border data flow. The community posits that amongst several types of data, personal data[1113] is the most vital data worth protecting. In protecting personal data, nations were thus obligated to ensure that the following principles were observed by data controllers while processing personal data.[1114] These principles or safeguards are:

- **Collection limitation principle**

  This makes it mandatory that the collection of personal data must have a limit, and that the data must be obtained through fair and lawful means.[1115] The

---

1110 Mutai https://www.mu.ac.ke/informationscience/index.php/research-publications/staff-research-and-publication-2/category/16-miriam-mutai?download=57:advantages-and-disadvantages-of-trans-border-dataflow (Date of use: 15 March 2015).

1111 Mutai https://www.mu.ac.ke/informationscience/index.php/research-publications/staff-research-and-publication-2/category/16-miriam-mutai?download=57:advantages-and-disadvantages-of-trans-border-dataflow (Date of use: 15 March 2015).

1112 This portion of the research will concentrate on the OECD principles of trans-border data flow since the OECD is the foremost global body dealing with trans-border data flow.

1113 Personal data relates to any data on a natural person which can make the individual identifiable from that data or when put together with other data. See sec 1 of the United Kingdom Data Protection Act of 1998.

1114 Clarke R "The OECD data protection guidelines: A template for evaluating information privacy law and proposals for information privacy law" http://www.rogerclarke.com/DV/PaperOECD.html (Date of use: 17 March 2015).

1115 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Date of use: 17 March 2015).

principle also stipulates that in apposite situations, personal data must be collected with the knowledge and permission of the data subject.[1116]

- **Data quality**

  The guideline mandates nations to ensure that personal data that are collected are relevant for the purpose it is sought to be used.[1117] The principle also stipulates that the data collected are exact, complete and kept current.[1118]

- **Purpose specification principle**

  This entails that prior to the collection of personal data, the purpose for such collection should be specified and any further use of such data must be limited to the already specified purpose.[1119]

- **Use limitation principles**

  This stipulates that except with the consent of the data subject or as allowed by the law, personal data should not be revealed, offered to, made accessible or used for other purposes other than the purpose specified to be used for.[1120]

- **Security safeguards principles**

  This principle requires data controllers to provide reasonable security measures to protect personal data from loss, destruction, alteration, use or disclosure.[1121]

1116 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Date of use: 17 March 2015).

1117 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Date of use: 17 March 2015).

1118 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Date of use: 17 March 2015).

1119 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Date of use: 17 March 2015).

1120 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Date of use: 17 March 2015).

- **Openness**

  The openness principle entails that a general policy about openness of personal data be maintained.[1122] Thus data controllers are expected to provide clear and concise statements on their policies in relation to personal data.[1123] The identity of data controllers and purpose of the data collected are required to be provided to the data subjects.[1124]

- **Individual participation principle**

  This principle gives data subjects the right to establish what information is held about them and to have inaccurate data rectified or completely erased.[1125]

- **Accountability principle**

  This principle requires that data controllers are accountable for complying with these guidelines and measures on data protection.[1126]

The driving force behind these rules is to ensure the safe and free flow of trans-border data among member countries.[1127] The guidelines, however, allow countries to restrict the flow of data to another member country where the latter does not substantially

---

1121. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Date of use: 17 March 2015).

1122 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Date of use: 17 March 2015).

1123 Terwange C "Is a global data protection regulatory model possible?" in Gutwirth S *et al* (eds) *Reinventing data protection* (Springer SBM Heidelberg 2009) 175-190.

1124 Terwange *Is a global data protection regulatory model possible?* 186.

1125 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Date of use: 17 March 2015).

1126 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Date of use: 17 March 2015).

1127 Part 3 secs 15-18 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Date of use: 17 March 2015).

observe and comply with the trans-border data transfer principles.[1128] The guidelines further permit member nations to impose some trans-border data restrictions with respect to certain classes of personal data where the country's privacy laws stipulate some regulations on such data and the member country does not provide equivalent protection.[1129] Trans-border transfers to third countries are only encouraged where the third country has adequate data protection laws.[1130] The advantage of these safeguards is that they attempt to create a balance between the need for free flow of cross-border data while ensuring that individuals and their data are protected from crime. These guidelines and safeguards, however, only relate to personal data and not to every facet of data breach or cybercrime.

The ubiquitous nature of the internet causes both developed and developing countries to rely on data that emanate and terminate from and on either sides of the divide. As earlier on highlighted in previous chapters,[1131] most developed countries have taken adequate steps in preventing and prosecuting cybercrime within their national boundaries. These preventive measures range from adequate cybercrime legislative initiatives, adequate law enforcement mechanisms, adequate capacity and funding for law enforcement agencies, advanced technological capacity, training and education for law enforcement agents. These steps, although impressive, are not so effective and foolproof, because various data from developed countries flow into developing countries that lack adequate cybercrime preventive schemes and *vice versa*. These nations with adequate cybercrime preventive schemes remain susceptible to harmful cyber activities emanating from jurisdictions with few or no cybercrime preventive mechanisms. It is submitted that certain levels of cross-border data restrictions may be employed to play

---

1128 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Date of use: 17 March 2015).

1129 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Date of use: 17 March 2015).

1130 Art 25 European Union Directive on Data protection (Directive 95/46/EC).

1131 Chs 2 and 3 of this research has highlighted several impressive steps embarked on by most developed countries in relation to adequate cybercrime legislation, law enforcement initiatives, law enforcement agency staff capacity or resources, technological capacity, adequate training/education and adequate funding of law enforcement agencies.

an important role and to a large extent compel developing countries to take adequate steps to address cybercrime. This will act as an important way of propelling developing countries that lag behind in taking adequate steps to outlaw, prevent and prosecute cybercrime. It is submitted that the essence of this cross-border data restriction is to put companies and various agencies in a country with inadequate cybercrime preventive measures under some disadvantage that will propel them to lobby its government to put in adequate cybercrime preventive measures. This is because when companies and agencies that rely on cross-border data for their ventures have certain vital data withheld from them solely because the instant business jurisdiction does not have adequate minimum cybercrime preventive standards, they will take all necessary steps to compel the government to adequately address cybercrime. This will also protect nationals and businesses in jurisdictions with proper cybercrime preventive measures from being prone to and unprotected from cyber criminals in jurisdictions with inadequate proper cybercrime preventive measures. Where the company, institution or agency is unable to conduct its business in the jurisdiction because of data restrictions, they will either coerce or lobby[1132] the government to set up adequate measures or they may be forced to close down their businesses which will affect the economy of the state. The companies, agencies and establishments that are affected by this cross-border data transfer restrictions may also metamorphose into interest or pressure groups that will persuade the governments of developing countries to take concrete steps to address internet crime. As Sutton points out, policy-making processes are influenced by interest groups that apply power and authority over policy making and influence every stage of the policy process.[1133] Thus, the proposed cross-border data transfer restrictions protect the consumer from being exposed to certain levels of internet crime

---

1132 Lobbying involves the persuasion of government policy makers to make policies in line with the lobbyists' positions. This could be achieved through studying and analysing extant legislations and regulatory policies; monitoring and reporting policy developments; attending legislative and regulatory agency's hearings; collaborating with other interest groups on similar issues; and educating government officials and other policy makers on the essence of the desired change which the lobbyists are pushing for. See http://grprofessionals.org/about-lobbying/what-is-lobbying/ (Date of use: 21 March 2015).

1133 Sutton R *The policy process: An overview* (Overseas Development Institute working paper) (Chameleon Press London 1999) 22-29.

and, on the other hand, it becomes an instrument that will compel companies and agencies affected to pressurise the government to properly address cybercrime.

These eight trans-border data flow principles or safeguards as enumerated above, although currently applied to personal data protection, can also be applied to other genres of data and cybercrime generally. Thus, countries with adequate cybercrime protection can ensure that these data protection principles are observed or data will be restricted from getting to such non-complaint jurisdictions. It is proposed that in the same way as data protection rules protect only personal data, not all genres of data should be restricted in the case of IT crime from being transferred across national boundaries.

As submitted, a major way of compelling developing countries that do not have adequate IT crime preventive measures to actively join the fight against internet crime is through the imposition of certain trans-border data transfer restrictions. It is submitted that it will be ideal to restrict two types of data from being transferred to countries without adequate cybercrime protection. These forms of data include:

- **Pecuniary or fiscal data**

  The prevalent forms of cybercrime are financial in nature and intended by the perpetrator to assist him in attaining some economic gain.[1134] Most financial data can still be classified as personal data.[1135] Apart from economic cyber-criminal activities targeted at individuals by tricking the victim into parting with money or financial details, companies that store financial data or details are main targets of most cyber-criminal activities.[1136] For example, Sony had its PlayStation network hacked by criminals who intended to obtain consumer data, especially their

---

1134 Ashford W "Financial services sector attracts most cyber crime, says PwC study" http://www.computerweekly.com/news/2240215532/Financial-services-sector-attract-most-cyber-crime-says-PwC-study (Date of use: 21 March 2015).

1135 For example, credit card details, bank account details, etc.

1136 Bartlett D "Talking points – Cyber crime: A growing threat to global companies" http://rsmi.com/publications/talking-points/691-talking-points-cyber-crime-a-growing-threat-to-global-companies.html (Date of use: 21 March 2015).

financial data.[1137] BBC reported that in 2014, 43 per cent of companies around the world reported that consumer data had been stolen.[1138] It becomes imperative that financial data be restricted from trans-border transfers from countries with adequate cybercrime safeguards to countries without adequate cybercrime preventive measures.

This fiscal data, therefore, can encompass an individual, institution or establishment's monetary or financial details.[1139] It also encompasses any information containing any financial detail which includes documentations on revenues, cost and charges for services, profits, operating income, financial performance data and the like.[1140] For example, tampering with a company's financial or revenue details can bankrupt the company or cover the tracks of individuals who siphon and steal the company's funds. This form of data will provide individuals, institutions and corporate bodies with the necessary protection unlike situations where only personal data is protected.[1141] Thus, the data subject can be an identifiable individual, corporate entity or government institution.

- **Personal data**

  Another prevalent form of data susceptible to abuse and compromise, and a target of cyber criminals are individuals' personal data. As elucidated by the OECD, these relate to any information or data relating to a data subject – an identified or identifiable individual.[1142] The protection of this form of data has

---

1137 In 2011 Sony admitted that the credit card details of its users may have been compromised. See Thomson I "Sony admits huge data leak after PlayStation network and Qriocity attacks" http://www.v3.co.uk/v3-uk/news/2046030/sony-admits-leak-playstation-network-qriocity-attacks (Date of use: 29 March 2015).

1138 Hubbard K "Protect your financial data from cyber criminals" http://www.bbc.com/capital/story/20141007-avoid-cyber-crime-in-90-seconds (Date of use: 30 March 2015).

1139 For example, debit and credit card details, bank or other monetary account details, etc.

1140 http://www.merriam-webster.com/dictionary/fiscal (Date of use: 30 March 2015).

1141 Extant data protection laws that protect only personal data protects human beings as data subjects more than institutions.

1142 Fuster GG *The emergence of personal data protection as a fundamental right of the EU* (Springer 2014) 75-108.

been classified as a fundamental human right that every individual deserves to have protected.[1143] Most cyber-criminal activities are perpetrated through the use or acquisition of individuals' personal data. For example, an individual's name, address, credit card information, date of birth, nationality number, mother's maiden name, and so forth, are valuable information that can be used to perpetrate several forms of cyber-criminal activities.[1144]

It is submitted that just as the OECD allowed for some exceptions in its bid to create a balance between the protection of an individual's privacy and the free flow of trans-border data transfer, it is also imperative that some exceptions be allowed under the data restrictions as suggested in this chapter. It is submitted that in order not to completely stifle essential trans-border data flow relating to fiscal or personal data, trans-border data flow to non-compliant states will be permitted when, just as the exceptions in data protection directive –

- the consent of the data subject has been given for the intended trans-border transfer;[1145]
- the intended data is essential to the performance of a contract or pre-contractual measures between a data subject and controller in response to data subject's request;[1146]
- the intended data transfer is critical to the conclusion or performance of a contract between the data controller and a third party for and in the interest of the data subject;[1147]
- public interest or the establishment, application and defence of legal claims make it crucial to have the data transferred;[1148]

1143 Fuster *personal data protection* 104.

1144 Paganini P "The value of personal data in the criminal underground" http://securityaffairs.co/wordpress/33431/cyber-crime/personal-data-criminal-underground.html (Date of use: 1 April 2015).

1145 Art 26(1) EU Data Protection Directive 95/46/EC.

1146 Art 26(1) EU Data Protection Directive 95/46/EC.

1147 Art 26(1) EU Data Protection Directive 95/46/EC.

1148 Art 26(1) EU Data Protection Directive 95/46/EC.

- the trans-border data transfer is crucial to the protection and advancement of the critical interests of the data subject;[1149]
- the data to be transferred is acquired from a public register or document as allowed by the laws.[1150]

It must be pointed out that in applying these exceptions for the protection of IT crime in relation to fiscal and personal data restrictions, these rules or exceptions will also apply to companies or juristic persons that acquiesce to the exceptions. Thus, the term data subject will refer and apply to both individuals and corporate bodies.

It is further submitted that the emergence of these principles or safeguards should be championed by the UN. As earlier on pointed out in chapter 3 of this research, the UN will be well suited to bring into existence a global trans-border restrictive regime to ensure the emergence of these principles and safeguards. The UN through the method highlighted in chapter 3[1151] of this research can adopt the eight principles on trans-border data flow to provide for the restriction of data to states without the minimum standards of cybercrime prevention, investigation and protection. This restrictive regime will then apply to almost all the countries of the world who are members of the UN.

The principles or safeguards must ensure:

- trans-border data restrictions to countries without adequate IT crime protection and prevention except where the data subject acquiesces under the afore-mentioned exceptions;[1152]
- uninterrupted trans-border data flows between nations with up-to-date cybercrime fighting mechanisms;[1153]

1149 Art 26(1) EU Data Protection Directive 95/46/EC.

1150 Art 26(1) EU Data Protection Directive 95/46/EC.

1151 These steps include Identifying the key players, identifying the various sub-players, establishing effective networking, developing feasible timeframe and deliberations or reconciliations at the UN level. These steps were properly enunciated in ch 3 of this research.

1152 Hamelink CJ "Communication rights and the European Information Society" in Servaes J (ed) *The European Information Society: A reality check* (Intellect Bristol 2003) 121-147.

1153 Hamelink *Communication rights* 135.

- eliciting significant commitment from nations to abide by the core principles of data protection and cybercrime prevention.[1154]

The emergence of these trans-border restrictions and the involvement of the UN in the establishment of these trans-border safeguards restrictions must be accompanied by a harmonised legislative initiative and minimum standards expected of countries with respect to legislation, capacity building and up-to-date investigative equipment. A country found to be lacking these minimum standards of good practice should have data restricted from being transferred into such jurisdiction as a form of sanction.

5.2.2. DIPLOMATIC TOOLS

Another socio-economic approach to getting developing nations to take active steps in addressing cybercrime is through the employment of various diplomatic tools by developed countries. These tools may be used to persuade these developing countries to set up the minimum requisite standards that would provide the right environment that can properly address IT crime.[1155] These tools may be employed one after the other until the desired change is achieved. Some of the necessary diplomatic tools include:

- **Coercive diplomacy**[1156]

  The threat of the application of force on developing countries for not taking adequate steps to address IT crime can be employed by developed countries. Developed countries have the requisite demeanour to instil compliance in recalcitrant developing countries when threat of force is used. Sun Tzu posits that success in battle is not measured by the number of battles won but by the

---

1154 Hamelink *Communication rights* 135.

1155 These minimum standards include establishing up-to-date cybercrime legislation, modern technologically compliant law enforcement initiatives, contemporary technological resources, capacity building for law enforcement agencies and judicial bodies.

1156 Coercive diplomacy has been defined as a diplomatic tactic which relies on the threat of force rather than the actual use of force to influence and propel a state to undertake some policies. George AL *Forceful persuasion: Coercive diplomacy as an alternative to war* (United States Institute of Peace Washington DC 1991) 3-14.

ability to seize one's enemy without even fighting.[1157] The threat of sanctions, economic sanctions, and expulsion from international organisations may be used to coerce developing countries into taking adequate steps that will address IT crime.

- **Financial aid**

  These are normally given to help the recipient of aid with certain conditions attached to the aid in order to compel the recipient to comply with certain international norms.[1158] The conditions attached to the aid can be employed by developed countries as a means of compelling the receiving developing country to address IT crime within its jurisdiction. For example, in 2011 the United States allocated $647.7 million in financial aid to Nigeria.[1159] In line with the conditions attached to some aid, the UK and US announced that aids will be withdrawn from developing countries that do not promote gay and lesbian rights, and further announced that more strings will be attached to foreign aid.[1160]

  On the other hand, sustained and consistent domestic pressure on governments will eventually compel the government and law enforcement bodies to take positive steps to address the ills in society. Thus, another method of getting the government of developing countries to fight cybercrime will be the consistent provision of financial aid to civil societies or domestic pressure groups. This is so because civil societies as non-profit making ventures can only sustain their pressure on the government when properly funded. The absence of funding will cause pressure groups to abandon their mission while soliciting funds, which

---

1157 Schettino I "Is coercive diplomacy a viable means to achieve political objectives?" http://www.e-ir.info/2009/06/29/is-coercive-diplomacy-a-viable-means-to-achieve-political-objectives/ (Date of use: 3 April 2015).

1158 Developing countries most often are recipients of financial aid from developed countries.

1159 Wingfield B "Making sense of US foreign aid to Egypt and elsewhere" http://www.forbes.com/sites/brianwingfield/2011/01/29/making-sense-of-u-s-foreign-aid-to-egypt-and-elsewhere/ (Date of use: 3 April 2015).

1160 Richardson H "Aid – More strings attached?" http://www.una.org.uk/content/aid-more-strings-attached (Date of use: 3 April 2015).

invariably makes them unable to mount the necessary pressure on government and its agencies to do the right thing.[1161]

- **Sanctions**

  Countries are pressurised into changing or adopting prevalent international norms when faced with various levels of sanctions.[1162] These sanctions can range from travel bans, embargoes, bans on cash transfers or trans-border data flow restrictions, as proposed in this chapter.[1163] It is submitted that the imposition of various sanctions on the government of developing countries with respect to their willingness to fight electronic crime will dissipate the apathy normally exhibited by most developing countries in relation to IT crime.

  Sanctions that will ensure the participation of developing countries in the fight against IT crime will not be limited to the government. Private institutions, public institutions and government agencies must be recipients of the sanctions in order to achieve the desired results. For example, sanctions on a private sector-driven economy may not propel a government burdened with sanctions once the economy is not affected by the sanction.

These diplomatic tools are not foolproof and do not always elicit compliance with the international norm which they try to enforce. These tools often do not affect the targeted government, but mostly inflict pain on the poor in society and derogate individuals' human rights. For example, Smith points out that sanctions are destructive to the targeted societies, widen the existing conflict, and sometimes prolong the conflict.[1164] For instance, the sanctions imposed on Iraq between 1991 and 2001 contributed to the

---

1161 Musser R "The two main challenges facing African civil society organisations" http://www.cipe.org/blog/2014/08/15/the-two-main-challenges-facing-african-civil-society-organizations/#.VR82SMl0cdk (Date of use: 4 April 2015).

1162 Kolodkin B "What are sanctions" http://usforeignpolicy.about.com/od/introtoforeignpolicy/a/what-are-sanctions.htm (Date of use: 4 April 2015).

1163 Kolodkin http://usforeignpolicy.about.com/od/introtoforeignpolicy/a/what-are-sanctions.htm (Date of use: 4 April 2015).

1164 Shane Smith M "Sanctions: Diplomatic tool, or warfare by other means?" http://www.beyondintractability.org/essay/sanctions (Date of use: 4 April 2015).

deaths of hundreds of thousands of children.[1165] These attendant destructions unfortunately weaken the necessary political support that would have made the sanction effective, such as in the case of Iraq where international support for the sanctions waned.[1166] Coercive diplomacy sometimes is risky and the coercing power can be challenged.[1167] The recipients of financial aid may call the bluff of the nation imposing the condition to the financial aid, thereby refusing the aid and the conditionality attached.[1168]

It is submitted, however, that for developed countries to ensure that the apathy of developing countries in the fight against cybercrime is dissipated, and that the developing countries take adequate steps to address IT crime, certain steps must be taken. These steps will enhance the possibility and effectiveness of the diplomatic approach that will yield the desired result. These steps include:

a. Multilateral coordination and collaboration

First, there must be multilateral coordination and adequate international cooperation.[1169] Where diplomatic tools are applied unilaterally by a single country, the developing country against which the tool is used can rely on the support of other international governments and will not feel the impact of the diplomatic tool.[1170] This will make such corrective measure ineffective. For example, where the United States alone imposes a tough condition on the financial aid aimed for Nigeria, the financial aid can easily be declined and the condition jettisoned when other developed countries are ready to give same aid without conditions. Also, sanctions such as trade embargoes will not have the

---

1165 Shane Smith http://www.beyondintractability.org/essay/sanctions (Date of use: 4 April 2015). See also Sadiq S and Tiller S "The debate over UN sanctions" http://www.pbs.org/frontlineworld/stories/iraq/sanctions.html (Date of use: 4 April 2015).

1166 Shane Smith http://www.beyondintractability.org/essay/sanctions (Date of use: 4 April 2015). See also Sadiq and Tiller http://www.pbs.org/frontlineworld/stories/iraq/sanctions.html (Date of use: 4 April 2015).

1167 Schettino http://www.e-ir.info/2009/06/29/is-coercive-diplomacy-a-viable-means-to-achieve-political-objectives/ (Date of use: 3 April 2015).

1168 For example, when the US and UK governments threatened to cease financial aid to developing countries that do not protect anti-gay rights, the Nigerian government called their bluff and instead passed the Anti-Gay Bill into law. See Richardson http://www.una.org.uk/content/aid-more-strings-attached (Date of use: 4 April 2015).

1169 Shane Smith http://www.beyondintractability.org/essay/sanctions (Date of use: 4 April 2015).

1170 Shane Smith http://www.beyondintractability.org/essay/sanctions (Date of use: 4 April 2015).

desired effect when other developed countries are ready to provide the requisite trade partnership.

b. Domestic opposition and pressure

The efforts of the international community will not be effective without a solid domestic pressure in the developing country. Diplomatic tools are more efficient when targeted governments and their leaders face domestic instability.[1171] For example, the apartheid regime in South Africa buckled under international pressure and sustained domestic agitations.[1172] Smith points out that the presence of domestic pressure would lessen the proclivity of the leader to play the nationalist card or to rally and organise internal support to fight or cushion the effect of the external diplomatic tool.[1173] Thus, in the case of corrective measures in relation to taking adequate steps to address IT crime, the international community must enter into an alliance or sponsor local pressure groups that will sustain the opposition against the existing government posture on cybercrime while agitating that it must be properly addressed.

c. More of incentives

The use of incentives should be employed more than any other diplomatic tool and should be used alongside any diplomatic tool being employed. Baldwin points out that the use of threats sends a message of aggression, anxiety, apprehension and bitterness while the use of incentives sends a message of hope, mutual cooperation and care.[1174] Thus, the chances of making the developing countries dispel their apathy towards IT crime would be increased through the use of incentives. Smith opines that the use of incentives and other diplomatic tools such as sanction will divide the country's domestic support for objectionable government policies.[1175] This is because the use of sanctions on certain sectors in a society and the use of incentives on other

---

1171 Shane Smith http://www.beyondintractability.org/essay/sanctions (Date of use: 4 April 2015).
1172 Shane Smith http://www.beyondintractability.org/essay/sanctions (Date of use: 4 April 2015).
1173 Shane Smith http://www.beyondintractability.org/essay/sanctions (Date of use: 4 April 2015).
1174 Baldwin DA "Power of positive sanctions" http://www.princeton.edu/~dbaldwin/selected%20articles/Baldwin%20(1971)%20The%20Power%20of%20Positive%20Sanctions.pdf (Date of use: 4 April 2015). See also Shane Smith http://www.beyondintractability.org/essay/sanctions (Date of use: 4 April 2015).
1175 Shane Smith http://www.beyondintractability.org/essay/sanctions (Date of use: 4 April 2015).

sectors of society would lessen the government's ability to rally support for its abhorrent policies and increase the support for change since some benefits are offered to certain sectors if the government cooperates with the international community.[1176]

5.2.3. EDUCATION, PUBLIC AWARENESS AND BEHAVIOURAL REORIENTATION

A nation's apathy towards addressing certain criminal activities may stem from the level of awareness of its citizens to the existence of such crime. It can also stem from the cultural and/or behavioural inclinations of the society. Thus, certain societies do not regard some crimes as being wrong or inimical, and the drive to curb such crimes is met with serious apathy. On the other hand, the absence of awareness of the citizenry to the level of the existence of the crime and its harmful nature can increase the indifference of the society to such crime.[1177] For example, in Nigeria the only form of cybercrime that most people are aware of is online fraud,[1178] while nationals hardly know anything about the existence of other IT crimes, such as denial of service attack except for those who perpetrate the attack and those at whom the attacks are targeted.[1179] Furthermore, the absence of awareness on how certain crimes can be tackled or on the preparedness of law enforcement agencies to tackle such crimes also raises the level of apathy within society to deal with such crime.[1180] Matsueda agrees with Sutherland that deviant behaviour is learnt through communication and contact with primary groups in a society.[1181] Therefore, any form of re-orientation would come from a well-articulated mode of education and awareness on the need for a shift from the current state of apathy to a new state of conscious effort in addressing crime. The apathy towards cybercrime in developing countries is largely due to the low level of awareness and the behavioural societal inclination towards IT crime. According to Foldvary, most

---

1176 Shane Smith http://www.beyondintractability.org/essay/sanctions (Date of use: 4 April 2015).

1177 Johnstone G *Restorative justice: Ideas, values, debates* (Routledge New York 2011) 72-93.

1178 Or advanced fee fraud, also known as 419.

1179 http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02 (Date of use: 31 May 2015).

1180 http://www.justice.gov/archive/crs/pubs/principlesofgoodpolicingfinal092003.pdf (Date of use: 31 May 2015).

1181 Matsueda *Social structure* 124.

individuals are apathetic to a social problem simply because they are uninformed.[1182] The nations with apathy have not yet come to terms with the nature, level and amount of devastation occasioned by the evils of IT crime on society. The majority of reported incidents of cyber-criminal activities are the ones that take place mainly in developed countries.[1183]

Promoting a culture, society or government that is not apathetic to the troubles created by IT crime will entail substantial reorientation or education. On the one hand, there must be an increase in education on the risks and level of damage that cybercrime causes society. This education may be championed by developed countries with the help and participation of interest groups in the target developing nation. This form of constant education will attract the attention, and seep into the consciousness of private individuals, private and public institutions, government agencies and personnel. Awareness of the devastating effects of IT crime will compel private individuals and institutions to exert serious pressure on their governments to take definite steps in addressing cybercrime, thus breaking the apathy of individuals and government to the menace of e-crime. This constant education will also attract the attention of government agencies, politicians and government policy makers who are daily confronted with the dangers of cybercrime to society. Constant public awareness will dissipate the level of apathy exhibited by most developing nations in addressing IT crime.

Thus, another way of addressing the apathy of developing countries towards cybercrime will be to address the prevailing moral climate and attitude towards crime among the nationals through the promotion of public values.[1184] The public must be made aware of the causes and effects of IT crime, the key factors in crime prevention,[1185] the extent of

---

1182 Foldvary FE "Ignorance, apathy, and greed" http://starbase.airweb.net/lifestyle/ignorance_apathy.html (Date of use: 31 May 2015).

1183 Gann T "McAfee executive on measuring the cost of cybercrime: Why it matters" http://www.hstoday.us/columns/critical-issues-in-national-cybersecurity/blog/mcafee-executive-on-measuring-the-cost-of-cybercrime-why-it-matters/c79246f8b6f0cf029edd2ff79348e349.html (Date of use: 18 April 2015).

1184 http://www.gov.za/documents/national-crime-prevention-strategy-summary#P3 (Date of use: 18 April 2015).

1185 http://www.gov.za/documents/national-crime-prevention-strategy-summary#P3 (Date of use: 18 April 2015).

government involvement in the IT crime prevention and prosecution, and the level of damage occasioned by e-crime.[1186] This will raise the national consciousness of the citizenry on the spate of cybercrime and reduce the apathy of all stakeholders in the fight against IT crime.

These levels of awareness can be achieved through formal school-based education since the school provides the right forum for the impartation of responsible, right attitudes and values.[1187] Public information campaigns formulated in ways that can be easily understood by the target audience (nationals and governments of developing countries) in appropriate languages can also be employed in creating the relevant public awareness.[1188] The radio, newspapers and various media outlets can be employed in these awareness campaigns. National, regional and local stakeholder workshops would provide the forum for discussion of the issues surrounding the crime with relevant suggestions on how to address the threat.[1189] Information empowering citizens to monitor and question government responses and activities in relation to their readiness to combat cybercrime can also be made available to nationals and local stakeholders. Investigative journalism and information by the media and other independent sources can be sponsored and promoted.[1190] Other public awareness initiatives can also be employed to achieve the desired effect of dissipating the apathy characterising the attitude of most developing countries towards IT crime.

These campaigns and public awareness initiatives can be introduced and driven by international agencies and governments who are desirous of ensuring that the apathy of developing countries abates. Private organisations that are concerned about the menace of cybercrime can also lead the drive for public awareness. This is so because leaving public awareness to government agencies that are already apathetic to the

---

1186 Burns RG, Whitworth KH and Thompson CY "Assessing law enforcement preparedness to address internet fraud" (2004) *Journal of Criminal Justice* 477-493.

1187 Burns, Whitworth and Thompson 2004 *Journal CJ* 487.

1188 http://www.unodc.org/documents/human-trafficking/Toolkit-files/08-58296_tool_9-8.pdf (Date of use: 18 April 2015).

1189 Langseth P "Global programme against corruption" http://www.unodc.org/pdf/crime/gpacpublications/cicp2.pdf (Date of use: 18 April 2015).

1190 Langseth http://www.unodc.org/pdf/crime/gpacpublications/cicp2.pdf (Date of use: 18 April 2015).

menace of cybercrime will not achieve the desired result. The government and its agencies are also primary targets of the education. When left to the government and its agencies, they are likely to stifle every effort to raise the level of IT crime awareness because, as established in previous chapters of this research,[1191] most governments enjoy the proceeds of cybercrime and actually encourage it.[1192]

5.2.4. PRESSURE GROUPS AND CIVIL SOCIETIES

These groups influence government decision-making processes and policies, affect national consciousness and orientation, and act as watchdogs in ensuring that governments and its agencies abide by various international standards in providing for the nation's citizenry. Government policies normally are borne out of the will of the political class and thus geared towards goals that enhance the position of the ruling class or seem to protect the overt interest of the populace.[1193] Pressure groups and civil societies exert pressure and draw the attention of government and individuals to certain areas of societal problems that needs to be addressed.[1194]

Developed countries can sponsor the emergence of pressure groups across developing countries that would pressurise their government to take adequate steps in addressing cybercrime.

These pressure groups can employ direct personal communication with policy makers through the use of lobby groups and the presentation of research results at legislative

---

1191 Ch 2 of this research showed that certain countries either benefit from the proceeds of IT crime or do not regard the prevention of cybercrime as a priority.

1192 For example, countries can encourage hacking for espionage purposes.

1193 Larok A "Different approaches, same goal? Civil society and the fight against corruption in Uganda" http://www.actionaid.org/sites/files/actionaid/different_approaches_same_goal_civil_society_and_corruption.pdf (Date of use: 18 April 2015).

1194 Larok http://www.actionaid.org/sites/files/actionaid/different_approaches_same_goal_civil_society_and_corruption.pdf (Date of use: 18 April 2015).

hearings.[1195] They can also employ various indirect contact techniques through the use of media campaigns, public opinions, protests, strikes, demonstrations, petitions and civil disobediences.[1196]

In providing and sponsoring efficient pressure or interest groups by developed countries, the organisational structure of the group must be properly positioned to ensure the efficiency and potency of the message being propagated by the group. This is so because most individuals behind pressure groups in developing countries are driven by selfish gain with the intent to help the individuals behind the pressure groups gain entrance into the political class.[1197] Thus, the IT crime pressure group can be structured as "Specialised research and advocacy groups",[1198] where they are an effective research or policy advocacy group, with easy access to state policy makers and donor bodies.[1199] These specialised research and advocacy groups can act as consultants to the government and also participate in drafting major policy documents.[1200] These pressure groups can also be structured as Networks and Coalitions[1201] to campaign for and mount pressure on the government to address IT crime.[1202] The success of these pressure or interest groups greatly depends on its organisational structures. However, for these groups to be effective, they should have understood the need for effective cybercrime prevention and fighting machinery to be erected within the system.

Developed countries that engineer the formation and running of these pressure groups must ensure that these pressure groups will receive constant support to shield them from certain factors that plague pressure groups in developing countries. The issues

---

1195 Okeke VOS "Pressure groups and policy process in Nigeria: A case of fourth republic" (2014) *Global Advanced Research Journal of Social Science* 15-24.

1196 Okeke *Pressure groups* 2014 *Global ARJSS* 18.

1197 Abimbola A "Pressure groups and the democratic processin Nigeria (1979-1993)" (2002) *Nordic Journal of African Studies* 38-47.

1198 Okeke *Pressure groups* 2014 *Global ARJSS* 17.

1199 Okeke *Pressure groups* 2014 *Global ARJSS* 17.

1200 Okeke *Pressure groups* 2014 *Global ARJSS* 17.

1201 Okeke *Pressure groups* 2014 *Global ARJSS* 17.

1202 Okeke *Pressure groups* 2014 *Global ARJSS* 17.

that plague most pressure groups in developing countries and which must constantly be addressed include:

- **Intimidation and violence against pressure groups and its officers**

  The governments of most developing countries are intolerant of any group that promotes a divergent opinion that seems inimical to the interests of the government. Thus, intimidation, threats and violence may be unleashed on non-conforming interest groups.[1203] This challenge may be faced by interest groups seeking to promote the active involvement of developing countries in the fight against cybercrime. Unfortunately the discouraging attitudes of security agencies to the rule of law and their constant flagrant abuse of existing judicial systems further reinforce the challenges that may be faced by internet groups.[1204]

- **Delay in the administration of justice and the difficulty in sensitisation**

  The delay in the dispensation of justice creates distrust in the ability of the government to ensure that the rule of law is hallowed and the rights of citizens protected.[1205] This posture makes it difficult for the citizens to assimilate future clamour for change, since the change in government policies end up yielding no benefit to the citizen and at best protects the elite.

- **Illiteracy and communication obstacles**

  A major strategy employed by pressure and interest groups is the creation of awareness and sensitisation of the public to the existence of an ill in society and the steps necessary to combat this.[1206] The literacy level of the populace will to a large extent determine the impact of any public sensitisation. Unfortunately most developing countries have a higher illiteracy level.[1207] For example, most

---

1203 Nzarga FD "Appraisal of human rights non governmental organisations (NGOs) in Nigeria" (2014) *Journal of Law, Policy and Globalisation* 148-151.

1204 Nzarga *Appraisal* 2014 *Journal LPG* 148.

1205 Nzarga *Appraisal* 2014 *Journal LPG* 149.

1206 Nzarga *Appraisal* 2014 *Journal LPG* 150-151.

1207 Adepoju P "Illiteracy, causes, effects and solutions" http://iluvjetnoise.blogspot.com/2012/08/illiteracy-causes-effects-solutions.html (Date of use: 16 April 2015).

businessmen in Nigeria are not computer literate and even though they rely to some extent on the internet for international business transactions, they mostly rely on other persons such as cyber cafe owners for such online business transactions.[1208] This communication gap creates a barrier to any meaningful impact by pressure and interest groups.

- **Absence of adequate funding**

  The creation of awareness, the lobbying of policy makers and the institution of court actions to propel governments to take proactive steps and many other strategies that will be employed by interest groups all require substantial funding to carry out such campaigns.[1209] Since the populace and the government or policy makers are the targets of interest groups, such groups are rarely funded by their national governments.[1210] It is submitted that since developed countries will benefit from the impact of these pressure groups in developing countries, companies, donor agencies and governments of developed countries should contribute immensely to the funding of these interest groups.

- **Corruption and personalisation of interest groups**

  The promotion of interest groups is viewed in most developing countries as a money-making avenue.[1211] Thus, most interest groups are personalised and controlled by individuals who may have registered the group for their personal and selfish gain in order to solicit funds from foreign donors and to siphon same.[1212] As a result of the selfish motives behind the promotion and emergence of such interest groups, the funds meant for the groups are diverted and the group easily winds up.[1213] The personalisation of such groups will lead to its early

---

1208 Okoli F "Starting a computer business centre in Nigeria" http://www.makemoneynigeria.net/cgi-bin/page.pl?b=small-business&bn=4&m=3 (Date of use: 16 April 2015).

1209 Nzarga *Appraisal* 2014 *Journal LPG* 151.

1210 Nzarga *Appraisal* 2014 *Journal LPG* 151-152.

1211 Nzarga *Appraisal* 2014 *Journal LPG* 151-152.

1212 Ofosu-Appiah B "Making NGO's more effective and responsive in a globalised world" https://www.globalpolicy.org/component/content/article/177/31636.html (Date of use: 17 May 2015).

1213 Nzarga *Appraisal* 2014 *Journal LPG* 151.

demise if the sole owners of the group die or become indisposed to continue with the operation of the group.[1214] This selfish structure greatly hampers the sphere of influence and activities of these interest groups within developing countries.[1215]

It is therefore submitted that placing reliance on pressure groups by developed countries in compelling developing countries to take steps in actively participating in the fight against IT crime is a veritable step in achieving the desired result.

5.2.5. ALLEVIATION OF POVERTY, INEQUALITY AND SOCIAL EXCLUSION

According to conflict theorists, criminal activities are motivated by the operation of social and economic factors.[1216] They posit that different groups with different values and concerns make up society and, unfortunately, the government takes care of the group with the greater influence which are those with money and power.[1217] The attention given to the group with greater influence creates some conflict between the government that tries to subdue the powerless and the powerless trying to get into positions of influence.[1218] Also, most societal economics are skewed to encourage the uneven distribution of income and income-generating capabilities, thus compelling individuals to seek to break away from the economic cadre they have found themselves in, in order not to be at the receiving end of the brunt of the upper class. The poor are socially excluded and marginalised from the opportunities and rights readily made available to the rich or upper class.[1219] These conflicts and class inequalities fuel the desire for crime. The individual, who sees a number of the members of the upper class engaging in illegality, opts to take some illegitimate steps to get out of his economic inequality.

1214 Nzarga *Appraisal* 2014 *Journal LPG* 151.

1215 Nzarga *Appraisal* 2014 *Journal LPG* 151.

1216 Gilbert and Sookram www.sta.uwi.edu/conferences/09/salises/documents/K%20Gilbert.pdf (Date of use: 17 January 2015).

1217 Gilbert and Sookram www.sta.uwi.edu/conferences/09/salises/documents/K%20Gilbert.pdf (Date of use: 17 January 2015).

1218 Gilbert and Sookram www.sta.uwi.edu/conferences/09/salises/documents/K%20Gilbert.pdf (Date of use: 17 January 2015).

1219 These rights and opportunities may include housing, security, employment, due process, health care, democratic participation, the rule of law, social, economic and cultural life. Klasen S "Social exclusion, children, and education: Conceptual andmeasurement issues" http://www.oecd.org/edu/school/1855901.pdf (Date of use: 17 May 2015).

Thus, the gap between the rich and the poor must be addressed if crime is to be tackled effectively.

Most developing countries fall under the class of non-egalitarian societies where equal opportunities are rare and inequality rates are higher.[1220] These inequalities are characterised by differences in power, income, wealth distribution and general conditions of living between the different social classes.[1221] According to Karsedt, in non-egalitarian societies social mobility is severely inhibited, elites are recruited from the upper social strata, and they exert influence on various government institutions.[1222] The elites in such societies view themselves as above the law, repress various state control mechanisms through the suppression of public opinion and influence on the judicial system and are not challenged.[1223] Karsedt further opines that inequality makes the elite less susceptible to social control, deterrence or shaming by public opinion, thus making room for higher levels of elite crimes, even cybercrime.[1224] This further increases the resolve of deviant members of the lower class to aspire to join the elites through any means, including cybercrime. This attendant migration will help the perpetrator to escape the inequality faced by the lower class while attaining all the benefits and protection the elites possess, even protection from criminal prosecution.

Therefore, the use of force, legislation and other state control will not be effective unless poverty is addressed and inequality is reduced to the barest minimum where differences in economic strata do not determine how the rule of law applies to different individuals. Until inequality is addressed and every class given its due opportunities, crime, including electronic crime, will be seen as a faster way for class migration.

1220 Young-Mok K "Inequality-how to address Piketty on the global level" https://www.devex.com/news/inequality-how-to-address-piketty-on-the-global-level-84077 (Date of use: 17 May 2015).

1221 Karsedt S "Inequality, power and morals: Criminality of elites and their impact in society" http://www.afp.gov.au/media-centre/publications/platypus/previous-editions/1998/march-1998/inequality.aspx (Date of use: 17 May 2015).

1222 Karsedt http://www.afp.gov.au/media-centre/publications/platypus/previous-editions/1998/march-1998/inequality.aspx (Date of use: 17 May 2015).

1223 Karsedt http://www.afp.gov.au/media-centre/publications/platypus/previous-editions/1998/march-1998/inequality.aspx (Date of use: 17 May 2015).

1224 Karsedt http://www.afp.gov.au/media-centre/publications/platypus/previous-editions/1998/march-1998/inequality.aspx (Date of use: 17 May 2015).

Developed countries can help alleviate the poverty and inequality in developing nations through the provision and promotion of various economic growth indices in the target developing nation. These poverty and inequality reduction indices are factors that can draw out an appreciable number of individuals below the poverty lines, reduce the poverty levels and ultimately reduce the incidence of crime in the jurisdiction of a developing country. Some of these indices include:

- **Education**

  Scholars believe that there is a nexus between poverty reduction and education.[1225] Scholars posit that education provides its recipients with essential critical skills and these skills provide the key to the recipients' ability to provide for themselves and their families.[1226] It also provides more employment opportunities, job security, decent wages and good working conditions for educated individuals.[1227] This eventually contributes to viable economic growth, and encourages good governance, policies and transparency.[1228]

- **Economic growth**

  Poverty and social inequality are reduced when a nation's economy grows. This is so because economic growth sees the birth of better opportunities, wealth creation, employment and the provision of basic amenities of life, impacting positively on the poverty levels in a nation. Developed countries can encourage economic growth through various means such as strengthening trade links between the developed and the developing country,[1229] and encouraging its

---

1225 Ukwaeze ER and Nwosu EO "Does higher education reduce poverty among youths in Nigeria?" (2014) *Asian Economic and Financial Review* 1-19.

1226 Omoniyi MBI "The role of education in poverty alleviation and economic development: A theoretical perspective and counselling implications" (2013) *British Journal of Arts and Social Sciences* 176-185.

1227 http://www.globalpartnership.org/education (Date of use: 17 July 2015).

1228 http://www.globalpartnership.org/education (Date of use: 17 July 2015).

1229 Lilley P and Basnett Y "10 ways the new EU trade chief can help reduce poverty in developing countries" https://www.devex.com/news/10-ways-the-new-eu-trade-chief-can-help-reduce-poverty-in-developing-countries-84458 (Date of use: 17 July 2015).

private firms to embark on multinational investment in the developing country.[1230] Economic growth will provide an escape from poverty and social inequality.

- **Empowerment and strengthening of institutions**

  The institutions that determine the smooth running of a system determines the opportunities and economic balance experienced by various individuals. For example, the judicial system contributes to the level of human rights protection while the security bodies ensure the existence of the rule of law and public safety. Without these institutions, there will be anarchy, the poor will be vulnerable and discriminated against, market conditions will worsen and only the strong will survive and become wealthy.[1231] Developed countries can encourage, facilitate and compel the strengthening of institutions. They can also ensure that the poor are empowered while ensuring that administrative, political, formal and informal institutions work in favour of the poor.

  Aristotle once posited that poverty is the parent of crime.[1232] An individual's sense of morality is often eroded when faced with deprivation and poverty. It therefore behoves developed countries to take every necessary step to help developing countries curtail poverty as a tool in slowing down the increase of IT crime.

CONCLUSION

This chapter has shown that crime is a creation of several biological, ecological, socio-economic and other micro-level factors that influence people's desires and affect their

---

1230 Pfeffermann G "Poverty reduction in developing countries: The role of private enterprise" http://www.imf.org/external/pubs/ft/fandd/2001/06/pfefferm.htm#author (Date of use: 17 July 2015).

1231 Yanagihara T "Approach to poverty reduction in developing countries and Japan's contribution" http://jica-ri.jica.go.jp/IFIC_and_JBICI-Studies/english/publications/reports/study/topical/articles/pdf/articles_02.pdf (Date of use: 17 July 2015).

1232 Omotor DG "Socio-economic determinants of crime in Nigeria" (2009) *Pakistan Journal of Social Sciences* 54-59.

decision-making processes.[1233] The chapter has also shown that nations and individuals are largely apathetic to certain social ills as they are uninformed or plagued by a number of socio-economic problems such as poverty and the like. The chapter has attempted to highlight certain socio-economic factors that exacerbate the apathy of developing countries in addressing the cybercrime. The chapter has shown that socio-economic factors that lead to crime are not addressed solely by legislative fiats but by employing the use of certain socio-economic measures with a synergy of individuals, private companies, government institutions and international organs.

It is submitted that the employment of the afore-mentioned socio-economic measures by developed countries would help lead developing countries to

a. pursue the eradication of cybercrime safe havens;[1234]
b. cooperate in the investigation and prosecution of cyber-criminals;[1235]
c. ensure the proper training of law enforcement agencies in tackling cybercrime;[1236]
d. take adequate steps to create public awareness amongst its citizenry on steps to prevent and combat cybercrime.[1237]

The next chapter – chapter 6, will examine the various existing internet governance and regulatory structures and also try to find out the level of involvement of developing countries therein. The chapter will also examine how the abysmal involvement or otherwise of developing countries contributes to their apathy towards participating actively in tackling cybercrime. The chapter will seek to find out the factors that draw developing countries away from being part of the decision-making processes that determine and govern the internet. The chapter will make a case for the active

1233 Schiller J "Crime and criminality" http://www.des.ucdavis.edu/faculty/Richerson/BooksOnline/He16-95.pdf (Date of use: 17 July 2015).
1234 Li X "International actions against cybercrime: Networking legal systems in the networked crime scene" http://www.webology.org/2007/v4n3/a45.html (Date of use: 17 July 2015).
1235 Li http://www.webology.org/2007/v4n3/a45.html (Date of use: 17 July 2015).
1236 Li http://www.webology.org/2007/v4n3/a45.html (Date of use: 17 July 2015).
1237 Li http://www.webology.org/2007/v4n3/a45.html (Date of use: 17 July 2015).

participation of developing at all levels of the various internet governance schemes in order to ensure that developing countries are part of the internet regulatory schemes and invariably become more active and effective in the fight against cybercrime.

The chapter will further make a case for the emergence of a uniform internet regulatory body that will ensure compliance with the uniform cybercrime legislation and the participation of developing countries in the said regulatory body.

CHAPTER 6

INTERNET GOVERNANCE AND REGULATION: A CASE FOR AN EFFICIENT REGULATORY STRUCTURE AND THE INVOLVEMENT OF DEVELOPING COUNTRIES IN SAME

INTRODUCTION

The administration, organisation and structure of any entity affect the level of involvement or apathy that may be exuded by a class of its stakeholders. The involvement of policy makers, civil societies, all cadres of stakeholders, governments of developed and developing countries are critical to the successful curbing of the menace of cybercrime. Cyberspace has several bodies that formulate policies regulating this ubiquitous sphere. The policies of these internet governance bodies affect both developed and developing countries. Unfortunately, there is a high level of apathy among developing countries as it relates to participation in the existing internet governance bodies.[1238] This apathy on the part of developing countries in participating in the activities of these internet governance bodies invariably affects the readiness and interest of developing countries in actively joining the fight against cybercrime. Any drive to get developing nations involved in the fight against cybercrime will not be comprehensive without the active participation of developing countries in internet policy

---

[1238] Internet governance bodies refer to the various institutions that administer, manage and set policies and principles that regulate accepted behaviour within cyberspace. See Souter D "Phase 2 report: Mapping the information and participation practice of internet governance entities" http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 20 September 2015).

formulation and internet governance.[1239] All the lofty ideas proffered in previous chapters, such as a global judicial system, will not materialise without an active all-inclusive internet governing system.

It will be difficult to enlist the participation of developing countries in the fight against cybercrime when stakeholders from developing countries are excluded or feel excluded from existing internet governance bodies. It is submitted that the seeming apathy of developing nations would be greatly cured when they become part of the policy-making process and administration of the internet. This is so because individuals and institutions from developing countries that participate in the policy-making process of various internet governance forums will ensure that their nations participate in all facets of activities relating to cyberspace.

It must be pointed out that the level of participation that is likely to yield results is not merely membership or simple attendance of meetings, but rather active participants in the entire decision-making process. This will include identifying issues, conducting policy research, creating positions, assembling coalitions, bargaining with other stakeholders and being part of the various decision-making hierarchies.[1240]

This chapter analyses the presence and activities of various internet governance bodies. The chapter analyses the organisational structure of some main internet governance bodies in relation to developing countries. The chapter also identifies the absence of developing countries in participating in these various internet governing groups as a factor in the apathy of developing countries towards fighting cybercrime. The involvement of developing countries in these internet governance bodies relates to active participation and active involvement in the internal management of these bodies. How involved are developing countries in both? The chapter further attempts to

---

1239 Sadowsky G, Zambrano R and Dandjinou P "Internet governance: A discussion document" http://www.internetsociety.org/sites/default/files/internet%20Governance%20A%20Discussion%20Document%20%28George%20Sadowsky%29.pdf (Date of use: 20 September 2015).

1240 Maclean D *et al* "Strengthening developing country participation in international ICT decision making" http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 20 September 2015).

establish the factors behind this apathy and proffers some solutions. The chapter identifies the need for the emergence of a uniform internet regulatory body with oversight functions over the other existing internet governance bodies which will eventually ensure compliance with the already-proposed uniform cybercrime legislation. However, the chapter will not analyse all the internet governance bodies nor will it highlight every aspect of their administration. The chapter will examine a number of the existing internet governance bodies with a view to finding out the level of participation by developing countries.

6.1. CURRENT STATE OF INTERNET GOVERNANCE

It is established that the same way crimes plague the real world they also plague the virtual world, since the same persons susceptible to perpetuating evil in the real world also utilise the cyberspace for their nefarious activities. The effects of online activities are felt in the real world, thus making it imperative that some regulation be put in place to ensure that some form of order is maintained in the online world.

Several noble ideas, proffered by various scholars to create some form of order and crime-free cyberspace cannot be achieved without a proper regulatory structure that will ensure the internet architecture, technical standards and norms that will promote law and order on the internet. For example, this research has advocated the emergence of cyber courts, proper international policing and the like as a panacea to the menace that plagues cyberspace. The benefits of these institutions cannot be properly harnessed without an efficient internet governance mechanism that carries both developed and developing countries along. All the lofty ideas proffered in previous chapters will not materialise without a harmonised internet governing system with some uniformity in operation and the active participation of developing countries.

The extent of government intervention on internet regulation ends up dominating the physical realms alone and is fragmented along legal jurisdictions and boundaries. Thus,

to several scholars self-regulation provides the answer to a global, cross-border regulatory scheme that is guided by the architecture and code of the internet.[1241]

6.1.1. SELF-REGULATION AND ITS DESIRABILITY

The early stages of the commercialisation of the internet and the desire for technological neutrality made internet self-regulation desirable in order to encourage its growth.[1242] The proponents of liberalism were more inclined to allow the internet to be regulated by market forces and the industry. This is because liberal thoughts were sceptical of government interventions in cyberspace and viewed self-regulation as the enlightened approach to regulation.[1243] For example, the Bill Clinton administration of the United States pushed for the self-regulation of the internet under the guiding principles that, amongst other factors,[1244] (a) the internet should be market-driven with the private sector leading;[1245] (b) governments should refrain from imposing unnecessary regulations;[1246] and (c) government interventions should ensure only competition, transparency, fraud prevention, the protection of intellectual property and the facilitation of dispute resolution.[1247]

The early insistence of the United States that the internet should be self-regulated was welcomed by other nations and was further reinforced by the idea that cyberspace differed from the physical realms and the reach of national governments.[1248] The early reliance on self-regulation for the internet accentuates the benefits of such a self-regulatory scheme. For example, self-regulation proponents argue that the less formal

---

1241 Price ME and Verhulst SG *Self-regulation and the internet* (Kluwer Hague 2005) 1-27.

1242 Price and Verhulst *Self regulation* 4.

1243 Ang PH "Self-regulation after WGIG" http://www.wgig.org/docs/book/Peng_Hwa_Ang%20.pdf (Date of use: 20 September 2015).

1244 Macintosh KL "How to encourage global electronic commerce: The case for private currencies on the internet" (1998) *Harvard Journal of Law and Technology* 739-740. See also http://clinton4.nara.gov/WH/New/Commerce/summary.html (Date of use: 20 September 2015).

1245 Macintosh 1998 *Harvard JLT* 739. See also http://clinton4.nara.gov/WH/New/Commerce/summary.html (Date of use: 20 September 2015).

9 Macintosh global electronic commerce 1998 *Harvard JLT* 739.

1247 Macintosh global electronic commerce 1998 *Harvard JLT* 739.

1248 Johnson DR and Post DG "Law and borders: The rise of law in cyberspace" (1996) *Stanford Law Review* 1378-1379.

process of self regulation provides the internet with more flexibility that will not stifle innovation or limit consumer choices.[1249] It is also argued that the internet industry, being a technical enterprise, when self-regulated will provide the best form of quality control and will be better equipped to identify low standards which will guarantee quality.[1250] It is further argued that since the industry will bear the cost of regulation, the industry will come up with incentives to lower the cost of compliance and enforcement, thus making self-regulation desirable.[1251]

Unfortunately, self-regulation also has its shortcomings. For example, antagonists argue that self-regulation always promotes the interests of the self-regulator who will never work against its interests.[1252] The challenges of jurisdiction pose an obstacle to an effective self-regulatory scheme. It has also been pointed out that self-regulation thrives where the "self-regulators are few in number and cohesive".[1253] Scholars further point out that self-regulation creates a dearth of incentives that will enable the enforcement of standards, since the self-regulators are few and carry on without government intervention.[1254]

Evidently, the internet has several aspects that cannot currently be addressed by self-regulation alone. From the technical aspects, architecture and code of the internet, to various internet contents, public policy issues, copyright infringements and cybercrime activities, the results of behaviour and interactions on cyberspace do not differ from those of the real world. Price *et al* points out, that self-regulatory agencies are saddled with the duty of defining industry morality and bringing industry values and principles to public notice.[1255] However, they further point out that experience has shown that self-regulation alone does not produce the desired result in relation to internet and media-

1249 Ang PH "The role of self-regulation of privacy and the internet" (2001) *Journal of Interactive Advertising* 1-9.
1250 Ang 2001 *Journal IA* 5.
1251 Ang 2001 *Journal IA* 5.
1252 Ang 2001 *Journal IA* 5.
1253 Ang 2001 *Journal IA* 5**.**
1254 Ang 2001 *Journal IA* 5.
1255 Price and Verhulst *Self regulation* 4-6.

related content regulation, but rather that multiple modes of governance need to be applied.[1256]

Even though self-regulatory schemes can impose sanctions on certain issues governing the internet's architecture and certain technical aspects, issues revolving around IT crime cannot be addressed by self-regulation alone. For example, computer fraud cannot adequately be addressed by self-regulation since perpetrators can only be punished through a state's criminal system. It becomes imperative that the emergence of some legal codes and sanctions be enacted to ensure order within the virtual world. These laws can only be made by governments, and its sanctions implemented through the states' legal institutions.

6.1.2. INTERNET GOVERNANCE INSTITUTIONS AND THE INVOLVEMENT OF DEVELOPING NATIONS

The world has moved on from the earlier proposition that self-regulation alone is the key to the proper administration of the internet. This is because self-regulation alone would have been ideal where the entire administration of the internet is only technical in nature.[1257] Fortunately, cyberspace administration would include managing the technical coordination aspects or bodies, standards, regulatory or development aspects and public policy aspects.[1258]

In order to administer the various aspects in cyberspace, several models of internet governance have emerged, with their proponents recommending the reliance on one or more models of internet governance as an effective tool in the proper management of the virtual world. For example, Solum highlights five forms of internet governance and argues that the current internet governance schemes are a hybrid of the various existing

1256 Price and Verhulst *Self regulation* 4-6.
1257 Malcolm J *Multi-stakeholder governance and the internet governance forum* (Terminus Press Perth 2008) 29-91.
1258 Malcolm *Multi stakeholder* 29-91.

internet governance models.[1259] According to Solum, internet governance may be modelled on the understanding that the internet is a self-regulating realm or on the understanding that the internet transcends national precincts which can be governed by transnational cooperative bodies or international organisations based on treaties between states.[1260] He posited that it can also be modelled to be controlled by codes and architecture where regulatory decisions are made by protocols and software, or it can be modelled with the notion that national governments will determine internet governance through legal regulation.[1261] He further pointed out that internet governance can be determined and driven by market forces and economics.[1262]

The Working Group on Internet Governance (WGIG) also identified five models of internet governance[1263] and classified these as non-government models,[1264] development assistance models,[1265] standard development models,[1266] treaty-making models[1267] and policy coordination models.[1268]

The varying taxonomies on the models of internet governance underscore the importance of internet governance and the approach adopted by various stakeholders

---

1259 Solum LB "Models of internet governance" in Bygrave LA and Bing J (eds) *Internet governance: Infrastructure and institutions* (Oxford University Press Oxford 2009) 48-91.

1260 Solum *Models* 56-87.

1261 Solum *Models* 56-87.

1262 Solum *Models* 56-87.

1263 http://www.wgig.org/docs/WGIGpaperStakeholders.pdf (Date of use: 26 September 2015).

1264 This model of internet governance employs non-governmental organisations and private organisations to oversee the management of certain internet functions such as ICANN; http://www.wgig.org/docs/WGIGpaperStakeholders.pdf (Date of use: 26 September 2015).

1265 This internet governance mechanism focuses on the provision of assistance to developing countries on certain areas of concern; http://www.wgig.org/docs/WGIGpaperStakeholders.pdf (Date of use: 26 September 2015).

1266 This internet governance model refers to intergovernmental organisations that establish norms and standards but which do not create any obligations on nations or subject to ratification such as the ITU; http://www.wgig.org/docs/WGIGpaperStakeholders.pdf (Date of use: 26 September 2015).

1267 This model refers to intergovernmental arrangements that establish norms and standards that are subject to national ratification, create obligations under national and international laws and are either enforced though international dispute resolution mechanisms or do not include a binding dispute resolution mechanism; http://www.wgig.org/docs/WGIGpaperStakeholders.pdf (Date of use: 26 September 2015).

1268 This refers to intergovernmental mechanisms that do not create norms or standards but coordinate national policies and policy direction to international organisations; http://www.wgig.org/docs/WGIGpaperStakeholders.pdf (Date of use: 26 September 2015).

would mould the character of internet governance schemes that determine how internet is ultimately regulated and the extent of stakeholder participation. For example, where market forces alone drive the decisions regulating internet governance, the extent of inputs by states and their legal systems may dwindle once the market forces of the nation have nothing to do with the internet.

It is submitted that internet governance based on the fusion of all the various internet governance models but chiefly propelled by Solum's second model of internet governance seems more apposite considering the fact that internet crimes are ubiquitous and are felt in the offline world and have to be punished or sanctioned by states' judicial or criminal systems. Thus, internet governance are chiefly modelled on the understanding that "internet governance inherently transcends national borders and hence that the most appropriate institutions are transnational quasi-private cooperatives or international organisations based on treaty arrangements between national governments" is appropriate.[1269] The most suitable kind of governance model has to be global, multi-sectoral, accommodating a wide variety of participants from all categories of stakeholders and democratic institutions.[1270]

It is obvious that the current ubiquitous nature of the internet makes it impossible for a single organisation to adequately handle and coordinate the various aspects of the internet. This is because the various internet architectures, protocols, communication infrastructure, public policy issues and contents are manned by different organisations in various jurisdictions and various real-time laws. Thus, there are several international, regional, national, inter-governmental, governmental and non-governmental entities that deal with internet governance.

1269 Solum *Models* 56-57.

1270 Baird Z and Verhulst S "A new model for global internet governance" http://www.markle.org/sites/default/files/ahs_global_internet_gov.pdf (Date of use: 17 September 2016).

This chapter will therefore take a narrower perspective and focus on the existing internet governance bodies, the extent of involvement of developing countries in them and ways of getting developing countries to participate in these bodies.

In looking at the various internet governance institutions, the pertinent question behind the analysis will be the involvement of developing countries in the administration of the various bodies. Clearly, this research cannot analyse every internet governance entity but will examine a few internet governance institutions or bodies, which will give an idea as to the extent of the participation of developing countries. Some of these entities include the Internet Corporation for Assigned Names and Numbers (ICANN); the International Telecommunication Union (ITU); the Internet Engineering Task Force (IETF); the Internet Governance Forum (IGF); the Internet Society (ISOC); the World Wide Web Consortium (W3C), and the Number Resource Organisation (NRO).

6.1.2.1. INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS

The Internet Corporation for Assigned Names and Numbers (ICANN) is the foremost internet management, non-profit corporation saddled with the responsibility of coordinating the domain name system, allocating internet protocol (IP) addresses, managing root server systems, managing top-level domain names and assigning protocol identifiers.[1271] These responsibilities entail that ICANN will approve and license companies to operate as primary registrars of top-level domain names (TLDs) and also make decisions on the addition or otherwise of new TLDs to the root system.[1272] They further entail that ICANN will coordinate a uniform domain name dispute resolution policy (UDRP) and also coordinate the various technical parameters revolving around its responsibilities.[1273]

1271 https://www.icann.org/resources/pages/welcome-2012-02-25-en (Date of use: 26 September 2015).

1272 Haqqani AB (ed) *The role of information and communication technologies in global development* (United Nations Publications New York 2005) 3-18.

1273 Haqqani *global development* 7-8.

The management of the domain name system is integral to the functioning of user-friendly computing because humans are spared the agony of remembering IP addresses and instead rely on domain names for easy internet navigation.[1274] These technical decisions taken by ICANN invariably shape the functioning of websites, determine domain names and who owns them, and stipulate how disputes over trade-marked domain names are resolved.[1275] These decisions also determines the amount of data on domain name owners that can be publicly accessed, stipulate how domain names can be reallocated and general determination of technical parameters for the coordination of the domain name system.[1276] The domain name system is the nucleus and backbone of the internet, and ICANN is at its centre.[1277] The role of ICANN makes policy development relating to its immediate duties and the internet, in general, a major aspect of its functions.[1278]

The initial idea behind ICANN was the technical management of the domain name system. However, its technical decisions have many public policy implications. For example, the decision of ICANN in relation to the uniqueness of name spaces would expand to public policy issues such as intellectual property and content regulation which will apply to all servers within the name space.[1279] Again, the creation of the Uniform Domain Resolution Policy (UDRP) to resolve disputes arising from registration and use

---

1274 Every computer on the internet has an internet protocol (IP) address which is made up of a string of numbers, for example 192.0.37.165 which is like the computer's address. The domain name provides the computer with an identifiable name with which the computer or network can be located. The system thus transfers the domain name into the relevant IP address. For example, Amazon.com can easily be located than relying on a set of numbers. Brain M and Crawford S "How domain name servers work" http://computer.howstuffworks.com/dns.htm (Date of use: 26 September 2015).

1275 Haqqani *global development* 7-8.

1276 Haqqani *global development* 8. See also Schweighofer E "Roles and perspectives of ICANN" in Benedek W, Bauer V and Kettemann MC (eds) *Internet governance and the information society: Global perspectives and European dimensions* (Eleven International Publishing Utrech 2008) 79-90. See also https://www.arin.net/participate/governance/icann.html (Date of use: 03 October 2015).

1277 Wu C and Irwin JD *Introduction to computer networks and cybersecurity* (CRC Press New York 2013) 95-97.

1278 Haqqani *global development* 7-8.

1279 Klein H "ICANN and internet governance: Leveraging technical coordination to realize global public policy" http://indiana.edu/~tisj/readers/full-text/18-3%20Klein.pdf (Date of use: 28 September 2015).

of domain names, using the dispute resolution providers[1280] approved by ICANN, expands into public policy frontiers.[1281]

The "technical" decisions of ICANN are essential and invariably affect both developing and developed countries.

ICANN though a non-governmental organisation is structured to accommodate input from various stakeholders. ICANN's board of directors is its primary decision-making organ.[1282] To maintain its multi-stakeholder's approach in administering the domain name system, two directors each are selected from the Address Supporting Organisation,[1283] Country Code Supporting Organisation[1284] and Generic Names Supporting Organisation[1285] respectively.[1286] The board also includes a president who is an *ex officio* director, and the bylaws further mandate the nominating committee to select eight other board members.[1287] In order to ensure wide international representation on the board, the bylaws stipulate an aggregate balance and diversity in the geographical distribution of board membership in addition to diversity in skills, culture, experience, and perspective.[1288] Thus, the bylaws provide for proportional

---

1280 These dispute resolution providers include the Asian Domain Name Dispute Resolution Centre; the National Arbitration Forum; the Czech Arbitration Court; the WIPO Arbitration and Mediation Centre; and the Arab Centre for Domain Name Dispute Resolution (ACDR); https://www.icann.org/resources/pages/providers-6d-2012-02-25-en (Date of use: 28 September 2015).

1281 Blackman K "The uniform domain name dispute resolution policy: A cheaper way to hijack domain names and suppress critics" (2001) *Harvard Journal of Law and Technology* 223-230.

1282 Art 2 sec 1 Bylaws for Internet Corporation for Assigned Names and Numbers (ICANN).

1283 The Address Supporting Organisation reviews and develops recommendations on IP address policies and in conjunction with the Regional internet Registries (RIR), advises the ICANN Board on issues surrounding number resource allocation policy; https://aso.icann.org/documents/memorandums-of-understanding/memorandum-of-understanding/ (Date of use: 05 October 2015).

1284 The Country Code Supporting Organisation provides the platform for the development and recommendation of policies to ICANN in relation to country code top-level domain (ccTLD) http://ccnso.icann.org/about (Date of use: 05 October 2015).

1285 The Generic Names Supporting Organisation formulate policies for generic Top-Level Domains (gTLD). These generic Top-Level Domains are not linked to specific countries, for example .com and .org. http://www.balancingact-africa.com/news/telecoms_en/7072/icann-asks-for-more-african-input-in-generic-names-supporting-organisation (Date of use: 5 October 2015).

1286 Art 6 sec 2 Bylaws for Internet Corporation for Assigned Names and Numbers (ICANN).

1287 Art 6 sec 2 Bylaws for Internet Corporation for Assigned Names and Numbers (ICANN).

1288 Art 6 sec 2(2) Bylaws for Internet Corporation for Assigned Names and Numbers (ICANN).)

representation of the five geographic regions[1289] with at least one director from each region. No single region can have more than five directors on the board.[1290]

In order to encourage input from various internet stakeholders, governments are represented in the Government Advisory Committee (GAC)[1291] while internet users and the general public are represented through the At-Large Committee (ALAC).[1292] These bodies are only advisory bodies. In addition, ICANN also has the Root Server System Advisory Committee, the Security and Stability Advisory Committee and the Technical Liaison Group as advisory bodies.[1293]

ICANN's decisions affect both developed and developing countries and are important to both divides.[1294] However, developing countries will be disposed to clamouring for better inclusion of developing countries in the administration of ICANN when they perceive the importance of ICANN to the developing nations. The decisions of ICANN are of serious relevance to developing nations.

First, the role played by ICANN in country-level domain names makes ICANN relevant to both developed and developing countries and of greater concern to developing nations.[1295] For example, country code domain names are delegated or re-delegated by a synergy of the requestor,[1296] relevant stakeholders,[1297] proposed manager,[1298]

1289 For purposes of proper representation, ICANN provides for five regions: Europe; Asia/Australia/Pacific; Latin America/Caribbean islands; Africa; and North America. See art 6 sec 5 Bylaws for Internet Corporation for Assigned Names and Numbers (ICANN).

1290 Art 6 sec 5 Bylaws for Internet Corporation for Assigned Names and Numbers (ICANN).

1291 Chango M "Accountability in private global governance: ICANN and civil society" in Scholte JA (ed) *Building global democracy? Civil society and accountable global governance* (Cambridge University Press Cambridge 2011) 267-287.

1292 Schweighofer *ICANN* 79-90.

1293 Schweighofer *ICANN* 83.

1294 Haqqani *global development* 7.

1295 Haqqani *global development* 7.

1296 The requestor is usually the proposed manager and the entity that initiates the process for a formal delegation of the country code domain name; https://www.icann.org/en/system/files/files/drd-ui-09sep13-en.pdf (Date of use: 10 October 2015).

1297 The relevant stakeholders are the parties that will benefit when the country code domain becomes operational. Their opinions are sought and are relevant in order to assess the public interest aspects of the request for the country code domain name; https://www.icann.org/en/system/files/files/drd-ui-09sep13-en.pdf (Date of use: 10 October 2015).

government,[1299] the US Department of Commerce,[1300] Verisign[1301] and ICANN.[1302] ICANN plays the most important role in any request for country code domain names and is chiefly involved in the receipt, verification and processing of the request.[1303] In processing the request for a country code domain name, the inclusion of the two-letter country code[1304] in the ISO list is of great importance.[1305] Even though the ISO list is created and maintained by the International Standards Organisation (ISO), ICANN's policy requires that ICANN reacts to the said list in the allocation of Country-Code Top-Level Domains (CCTLDs)[1306]

Second, the role played by ICANN in maintaining intellectual property rights and several dispute resolutions through ICANN's Uniform Dispute Resolution Policy (UDRP) causes ICANN and its administration to be of serious importance to the developing world.[1307] Conflicts and disputes around domain names pose a grave danger to the effective management of the domain name system where it is not properly managed or settled, and hamper fair participation in a global economy.[1308] ICANN's UDRP presents an efficient platform for developing nations to properly resolve intellectual property infringements in relation to the domain name system without recourse to a cumbersome

---

1298 The proposed manager is the entity that seeks to have the responsibility of a country code domain delegated to it. This entity upon approval becomes a trustee for the domain name; https://www.icann.org/en/system/files/files/drd-ui-09sep13-en.pdf (Date of use: 10 October 2015).

1299 The government of the jurisdiction or country whose name is sought to be used as the country code is consulted to either support or object to the emergence of the requested country code. This is because the country code represents the name of a country or territory and thus the government becomes a major stakeholder domain name; https://www.icann.org/en/system/files/files/drd-ui-09sep13-en.pdf (Date of use: 10 October 2015).

1300 The US Department for Commerce as the Root Zone Administrator verifies the procedures followed in authorising the request for the country code domain name; https://www.icann.org/en/system/files/files/drd-ui-09sep13-en.pdf (Date of use: 10 October 2015).

1301 Verisign is the root zone maintainer and receives requests processed by ICANN and implements the changes in the root zone necessary for the delegated domain name; https://www.icann.org/en/system/files/files/drd-ui-09sep13-en.pdf (Date of use: 10 October 2015).

1302 https://www.icann.org/en/system/files/files/drd-ui-09sep13-en.pdf (Date of use: 10 October 2015).

1303 https://www.icann.org/en/system/files/files/drd-ui-09sep13-en.pdf (Date of use: 10 October 2015). See also Haqqani *global development* 9.

1304 For example, .ng for the Nigerian country code; .za for the South African country code or .in for the Indian country code.

1305 Haqqani *global development* 9.

1306 Haqqani *global development* 7-14.

1307 Haqqani *global development* 7-14.

1308 Haqqani *global development* 7-14.

legal battle within the jurisdiction and judicial system of developed countries which may be unfavourable to claims from other jurisdictions.[1309]

Third, the security of the domain name system and ICANN's measures to provide adequate security make it imperative that the activities of ICANN are important to developing countries.[1310] The current spate of cyber-attacks and possible e-terrorism makes the security of the Domain name system imperative. ICANN's decisions in relation to the security of the DNS are more vital for the developing world because, while a minor attack on the developed countries might slow down traffic, the same attack on a developing country may completely cripple communications systems in the developing country.[1311] This is because the communication systems gateways and bandwidths in most developing countries are insufficient and scarce. Thus, ICANN's stance in considering an increase in widely-distributed root servers and investing in other emerging technologies to enhance the security of the Domain Name System (DNS) is important to developing countries.[1312]

ICANN's involvement in country-level domain names further underscores the importance of ICANN to the developing countries. This is so because country-level domain names establish the online identity of a state, and this makes ICANN's involvement in the administration of the CCTLDs of great benefit to developing countries.[1313]

It is also imperative to point out that the ability of e-commerce to stimulate development in developing countries makes ICANN and its decisions of significant relevance to developing countries.[1314]

1309 Haqqani *global development* 7-14.
1310 Haqqani *global development* 7-14.
1311 Haqqani *global development 7-14.*
1312 Haqqani *global development* 7-14.
1313 Haqqani *global development* 7-14.
1314 Haqqani *global development* 7-14.

ICANN has been taking steps to accommodate and ensure the participation of developing countries by making certain that some form of regional equity is prevalent in its activities. In ensuring regional equity and the participation of developing nations, ICANN's bylaws stipulates that each region[1315] produces a director on its board in order to promote diversity in culture, skills, experience, location and perception.[1316] The various councils and arms within ICANN are structured to encourage diversity and to encourage participation by all internet users.[1317]

ICANN's policy of rotating the locations of its meetings around various nations of the world also seeks to increase the participation of developing countries in its activities.[1318] For example, the ICANN 42 meeting (held from 23 to 28 October 2011) took place in Dakar, Senegal, while the ICANN 47 meeting (held from 14 to 18 July 2013) took place in Durban, South Africa.[1319] This is so because travel expenses and the denial of right of entry into developed countries would create a barrier to the level of participation for national of developing countries where the ICANN meetings are held in developed countries alone. Furthermore, ICANN is tinkering with the idea of convening a summit on developing countries to discuss the prospects of better participation of developing countries in the affairs of ICANN.[1320] The body embarked on a number of initiatives to facilitate multi-stakeholder participation, such as the Government Advisory Committee (GAC) with about 130 governments participating in the committee.[1321] ICANN has also created several fellowship programmes, partaken in regional meetings, increased

---

1315 ICANN's rules recognise Europe; Asia/Australia/Pacific; Latin America/Caribbean islands; Africa; and North America as its regional categorisation in order to ensure global participation in its affairs. See art VI sec 5 Bylaws for Internet Corporation for Assigned Names and Numbers (ICANN).

1316 Art VI sec 2(2) Bylaws for Internet Corporation for Assigned Names and Numbers (ICANN).

1317 Franda M *Governing the internet: The emergence of an international regime* (Lynne Riener Publishers Boulder 2001) 43-82.

1318 Dzidonu C and Quayor NN "Broadening and enhancing the capacity of developing countries to effectively participate in the global ICT policy fora and the ICT for Development (ICTfDev) Process" http://research.policyarchive.org/15545.pdf (Date of use: 8 November 2015).

1319 https://meetings.icann.org/en/calendar (Date of use: 8 November 2015).

1320 https://community.icann.org/download/attachments/5996930/AFRALO%20AfrICANN%20-%20Singapore%20.pdf?version=1&modificationDate=1373407641000&api=v2 (Date of use: 15 November 2015).

1321 Hickson N "ICANN response to internet governance consultation" https://ec.europa.eu/digital-agenda/en/content/icann-response-internet-governance-consultation (Date of use: 15 November 2015).

interpretation services and ensured the accessibility of translated materials that will enhance the participation of developing countries in the activities of ICANN.[1322]

However, several pundits still posit that the participation of developing countries in ICANN remains discouraging.[1323] In fact, the prevailing belief is that ICANN's activities and programmes do not reflect the needs and interests of developing countries in relation to the interests and needs of developed countries.[1324] For example, the high cost of travel makes it difficult for the average participant from a developing country to attend ICANN's public meetings that take place outside the participant's country of residence.[1325] Most ICANN meetings still take place in developed countries. The Markle Foundation also pointed out that most of ICANN's secretariat staff are from developed countries, even though there is some level of diversity among ICANN's organisational units.[1326] Furthermore, in 2014, while reporting on underserved regions with respect to domain names, ICANN observed that the majority of its accredited Registrars were located in developed countries.[1327]

A study by the Commonwealth Telecommunications Organisation and Panos London revealed that, although developing countries are represented in most intergovernmental internet governance organisations (such as the ITU), developing countries were under-represented in technical, standard-setting bodies and non-traditional decision-making

---

1322 https://www.icann.org/public-comments/dns-underserved-2014-05-14-en (Date of use: 24 November 2015).

1323 Touray KS "I had a dream: ICANN has 2 billion reasons to support developing countries" http://www.circleid.com/posts/20130901_icann_has_2_billion_reasons_to_support_developing_countries/ (Date of use: 24 November 2015).

1324 Rawal R "Danger mouse? The growing threat of cyberterrorism" in Nixon PG and Koutrakou VN (eds) *E-government in Europe: Re-booting the state* (Routledge Publications New York 2007) 54.

1325 The major determinant of a developing country is the level of its average income of its residents. Most residents of developing countries earn less than $1,000 per month and therefore can hardly afford to afford the basic necessities of life. See Cunningham M "Economic inequality: Differences in developed and developing nations" http://study.com/academy/lesson/economic-inequality-differences-in-developed-and-developing-nations.html (Date of use: 27 November 2015).

1326 Haqqani *global development* 3-18. See also https://www.icann.org/community/explore?profile_search[badge_filters][]=staff_badge (Date of use: 28 November 2015).

1327 https://www.icann.org/public-comments/dns-underserved-2014-05-14-en (Date of use: 28 November 2015) ICANN observed that out of the 1010 accredited registrars, seven were located in Africa while 14 were located in the Middle East.

arms.[1328] The study further established that developing countries were virtually unrepresented in market-driven internet governance decisions due to its low capacity.[1329] It will be difficult for a participant from a developing country to actively contribute to any policy-making process dominated by stakeholders from developed countries.

6.1.2.2. INTERNATIONAL TELECOMMUNICATION UNION

The International Telecommunication Union (ITU) is an agency of the UN with the mandate of fostering the growth of information and communication technology, and to coordinate the operation of telecommunication networks around the world.[1330] The Telecommunication Standardisation sector (ITU-T)[1331] of the ITU is a standard-setting body saddled with coordinating and developing standards for all facets of telecommunications infrastructures on a global basis, which includes the defining tariffs and including wireless, fibre optics, satellite and the like.[1332] The mandate of the ITU-T saddles the body with the coordination of telecommunications infrastructure which is the internet's major platform for its operation.[1333] This makes the ITU-T a major internet governance determinant since its policies and standard also shape the internet.

1328 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 20 September 2015).

1329 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 20 September 2015).

1330 https://www.unngls.org/index.php/engage-with-the-un/un-civil-society-contact-points/120-the-international-telecommunication-union-itu (Date of use: 23 December 2015).

1331 The other sectors are the radio communication (ITU-R) and the telecommunication development (ITU-D). The various ITU sectors were created to ensure that global standards that facilitate interoperability of communications systems around the world are set. They also ensure that programmes designed to improve capacity-building and telecommunication infrastructure are implemented. They also help achieve consensus on the operation and management procedures that will guide wireless services around the globe; https://www.unngls.org/index.php/engage-with-the-un/un-civil-society-contact-points/120-the-international-telecommunication-union-itu (Date of use: 23 December 2015).

1332 Hassan A "Internet governance: Strengths and weaknesses from a business perspective" in Drake WJ (ed) *Reforming internet governance: Perspectives from Working Group on Internet Governance (WGIG)* (United Nations New York 2005) 117-128.

1333 Souter D "Phase 2 report: Mapping the information and participation practice of internet governance entities" http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 24 December 2015).

The ITU as a major player in infrastructure management and standard-setting has been adjudged as the only international organisation that can make binding decisions on issues bordering on internet governance.[1334] The nature of the ITU-T, being a sector of the ITU (an agency of the UN), makes its policies and standards bear some formal international obligation to be adopted by member states.[1335]

Full membership of the ITU-T is reserved for governments of member-states.[1336] Associate or sector membership, on the other hand, is open to businesses, academia and other telecommunications organisations subject to the approval of the national governments.[1337] Associate members are entitled to participate in the technical work of a particular area of interest within the ITU-T scope of activities, while the sector members can participate in all ITU-T's technical work.[1338] Unfortunately, neither sector nor associate membership entitles such cadres of participants to a role in management decision making.[1339] Voting power resides with the member-states, while the major work of ITU-T is carried out by the associate and sector members.[1340] ITU-T's standardisation work is carried out by the technical study groups drawn from ITU-T members with the responsibility of developing recommendations or standards that will govern the various fields of international telecommunication, including internet governance.[1341] These study

---

1334 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 24 December 2015).

1335 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 24 December 2015).

1336 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 24 December 2015).

1337 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 24 December 2015).

1338 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 24 December 2015).

1339 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 24 December 2015).

1340 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 24 December 2015).

1341 http://groups.itu.int/itu-t/StudyGroups.aspx (Date of use: 25 December 2015).

groups are made up of experts in telecommunication from across various parts of the world. The Telecommunication Standardisation Bureau (TSB) as the executive arm of ITU-T provides daily management, secretarial support and coordination of the work of the various sectors.[1342] The ITU-T's top-level decision making is vested in the World Telecommunication Standardisation Conferences, convened every four years, to approve, modify or reject proposed draft recommendations or standards.[1343]

The composition of the various arms and cadres of the ITU-T as an agency of the UN provides some opportunity for the input of developing countries in its decision making, voting and management. For example, Maclean points out that almost all developing countries are members of the ITU and are represented by their countries' telecommunication administrations.[1344] The study groups are open to representatives of various member-states and anyone who wishes to register as an associate or sector member or from the academia, business associations, intergovernmental bodies, and so forth.[1345]

The activities of the ITU-T benefit the developing countries significantly. Through its Bridging the Standardisation Gap programme, the ITU-T pushes for an increased participation of developing countries in the standardisation process which will enable developing countries to experience some economic benefits that follow technological development.[1346] The ITU-T's standardisation work helps reduce the digital divide between developed countries and developing countries through its efforts in increasing the capabilities of the national standards of the developing countries.[1347] This increases the opportunities of developing countries for more economic growth and technological

---

1342 http://www.itu.int/en/ITU-T/info/tsb/Pages/geninfo.aspx (Date of use: 25 December 2015).

1343 Jakobs K *Standardisation processes in IT: Impact, problems and benefits of user participation* (Vieweg Lengerich 2000) 61-64.

1344 Maclean D "International Telecommunications Union (ITU)" https://www.giswatch.org/sites/default/files/gisw_itu_0.pdf (Date of use: 25 December 2015).

1345 http://www.itu.int/en/ITU-T/membership/Pages/Members.aspx (Date of use: 25 December 2015).

1346 Mauree V "ICT standardisation capabilities of developing countries: Bridging the standardisation gap" https://www.itu.int/dms_pub/itu-t/oth/0B/1F/T0B1F0000013301PDFE.pdf (Date of use: 25 December 2015).

1347 United States Congressional Serial Set, Serial No 15006, Senate Treaty Documents No 9-12 (United States Government Printing Office Washington 2006) 333-335.

innovation.[1348] ITU-T efforts in setting standards that will ensure the interoperability of equipments between ICT networks and devices mean a lot to the developing world, which may have been totally annihilated from the developed world or exposed to extremely expensive interoperability.[1349]

The ITU-T as an arm of the ITU (an agency of the UN) has its roots in the formal intergovernmental UN approach which is augmented by the additional input of regional and national telecommunications regulators and players, academia and business entities drawn from both developed and developing nations. This creates some room for the participation and representation of developing nations in formulating standardisation policies. Like most international bodies, the ITU Charter also enjoins the body to take steps to draw developing countries into its activities.[1350] For example, article 15 (205C) of the Convention of the International Telecommunication Union mandates the director of the Telecommunication Standardisation Bureau to "provide assistance to developing countries in the preparatory work for world standardisation assemblies, particularly with regard to matters of a priority nature for those countries".[1351] The ITU's stance of reaching its decisions through consensus[1352] is a measure that protects developing countries that usually do not have the capacity to push through their ideas or interests. The reliance on advanced remote participation in ITU-T meetings saves travel costs, especially for those in developing countries.[1353] ITU-T's multilingual staff across 12 offices worldwide provide some window of opportunity for developing nations to be part of the activities of ITU-T.[1354]

As part of the ITU-T's efforts to accommodate and ensure the participation of developing countries in ITU-T's activities, the Convention of the International

---

1348 United States Congressional Serial Set, Serial No 15006, Senate Treaty Documents No 9-12 (United States Government Printing Office Washington 2006) 333-335.

1349 http://www.itu.int/en/ITU-T/about/Pages/default.aspx (Date of use: 26 December 2015).

1350 http://www.itu.int/net/wsis/docs/geneva/official/dop.html (Date of use: 26 December 2015).

1351 Constitution of the International Telecommunication Union, 1992.

1352 Hill R *The new international telecommunication regulations and the internet: A commentary and legislative history* (Springer Heidelberg 2014) 19.

1353 http://www.itu.int/en/ITU-T/membership/Pages/default.aspx (Date of use: 26 December 2015).

1354 http://www.itu.int/en/ITU-T/membership/Pages/default.aspx (Date of use: 26 December 2015).

Telecommunication Union stipulates that in appointing the Chairpersons and Vice-Chairpersons of each study group, competence, equitable geographical distribution and the need to promote more efficient participation by developing countries must be given particular consideration.[1355] The management teams of most study groups have a mix of experts from developed and developing countries. For example, Study Group 11 has a Vice-Chairperson from Ghana although the other 11 members of the team are from developed countries.[1356] Of the 13 members of the Study Group 2 management team, four Vice-Chairpersons are from developing countries.[1357]

Study groups as the pivotal centre of ITU-T activities have been modelled to accommodate the input from developing countries through the creation of regional study groups.[1358] Regional study groups have been created in Africa, the Americas, Arab and Asia and Pacific to bring the participation of various nations in ITU-T activities closer to home.[1359]

The desire for enhanced participation by developing countries has also led to the use of various electronic platforms such as e-meetings, remote participation and the like to conduct meetings in real time.[1360]

The lofty strides of the ITU-T as a sector or study group-driven arm of ITU, to accommodate and encourage the participation of developing countries in it activities, are largely hindered by the lack of technical and financial capabilities.[1361] Membership

---

1355 Art 20 (242) Convention of the International Telecommunication Union.

1356 http://www.itu.int/en/ITU-T/studygroups/2013-2016/11/Pages/mgmt.aspx (Date of use: 18 September 2016).

1357 http://www.itu.int/en/ITU-T/studygroups/2013-2016/11/Pages/mgmt.aspx (Date of use: 18 September 2016).

1358 The creation of Regional Study Groups was enacted by Resolution 54 of the World Telecommunication Standardization Assembly. http://www.itu.int/en/ITU-T/regional-groups/Pages/default.aspx (Date of use: 28 December 2015).

1359 http://www.itu.int/en/ITU-T/regional-groups/Pages/default.aspx.

1360 http://www.itu.int/en/events/Pages/Calendar-Events.aspx?sector=ITU-T (Date of use: 28 December 2015).

1361 Calandro E, Gillwald A and Zingales N "Mapping multistakeholderism in internet governance: Implications for Africa" http://www.researchictafrica.net/docs/Mapping%20multistakeholderism%20in%20internet%20governance%20draft%20final%2004082013.pdf (Date of use: 28 December 2015).

of the ITU-T comes with a fee and the major hallmark of a developing country is the level of poverty of its citizens.[1362] For example, the annual fee for sector members is 31,800 CHF while the annual fee for associate members is 10,600 CHF and the annual fee for members from the academia is 3,975 CHF.[1363] Currently, the number of companies and other participants from developing countries that are ITU-T sector members is abysmal and discouraging.[1364] Out of the 197 sector members, 157 are from developed countries with only a few from developing countries trailing behind.[1365] Also, the study groups that are at the centre of ITU-T standards development are restricted to full and sector members and then associates get access to one study group they have paid to join, while the academia get access to all study groups at a fee.[1366] There is no room for the public and non-members to make inputs, and this further reduces the chances of developing countries to participate in ITU-T standards development.[1367]

6.1.2.3. INTERNET ENGINEERING TASK FORCE

The Internet Engineering Task Force (IETF) is another informal standard-setting body which is a key internet governance entity.[1368] The platform brings together researchers, vendors, network designers, ICT operators and other interested individuals who are

---

1362 http://www.itu.int/en/ITU-T/membership/Pages/Categories-and-Fees.aspx (Date of use: 23 October 2016).

1363 Although organisations and persons from some low-income and developing countries benefit from some discount. For example, sector members from low-income countries are allowed to pay an annual fee as low as 3,975 CHF while the Academia allow its members from developing countries to pay 1,987 CHF; http://www.itu.int/en/ITU-T/membership/Pages/Categories-and-Fees.aspx (Date of use: 23 October 2016).

1364 https://www.itu.int/online/mm/scripts/mm.list?_search=ITU-T&_languageid=1&_foto=y (Date of use: 28 December 2015).

1365 https://www.itu.int/online/mm/scripts/gensel11 (Date of use: 19 September 2016).

1366 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 24 December 2015). See also http://www.itu.int/en/ITU-T/membership/Pages/default.aspx (Date of use: 26 December 2015).

1367 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 24 December 2015).

1368 Alvestrand H "A mission statement for the IETF" https://www.ietf.org/rfc/rfc3935.txt (Date of use: 2 January 2016.

concerned with the seamless functioning of the internet and its architecture.[1369] The IETF thus aims at producing relevant technical and engineering documents that will include protocol standards, best current practices and the like, which will influence internet design and management, and develop new internet standard specifications.[1370]

Membership of this internet governance entity is open to any individual (rather than institutions, governments or companies) interested in participating in IETF activities at no cost, and this provides additional motivation for citizens of developing countries to participate in this forum.[1371] The absence of an organisational structure[1372] removes certain restrictions that characterise organisations with hierarchical structures that can shut out certain class of participants who do not as yet occupy the top echelon in decision making. IETF technical work is organised into several areas[1373] and done through the body's working groups (WG) via mailing lists, reducing the requirement to travel outside the participant's domicile for participation in IETF activities.[1374]

The IETF's activities are managed and coordinated by the Internet Engineering Steering Group (IESG), which steers the eight IETF core areas of the working groups.[1375] The IESG is saddled with the responsibility of approving internet standards and overseeing the internet standards process for such approval.[1376] The IESG is made up of the IETF Chairperson and two area directors, each representing the eight IEFT core work areas.[1377] Souter points out that IETF is more concerned with its outputs than with

---

1369 Alvestrand https://www.ietf.org/rfc/rfc3935.txt (Date of use: 2 January 2016.

1370 Alvestrand https://www.ietf.org/rfc/rfc3935.txt (Date of use: 2 January 2016.

1371 https://www.ietf.org/newcomers.html (Date of use: 2 January 2016).

1372 https://www.ietf.org/newcomers.html (Date of use: 2 January 2016).

1373 IETF's work areas revolve around Routing (RTG), Applications (APP), Real-time Applications and Infrastructure (RAI), Internet (INT), Security (SEC), Transport (TSV), Operations and Management (OPS), and General. See Melnikov A, Saint-Andre P and Nottingham M "Recent collaboration between W3C and IETF" http://www.w3.org/2010/11/TPAC/W3C-IETF-Collaboration.pdf (Date of use: 2 January 2016).

1374 https://www.ietf.org/list/ (Date of use: 2 January 2016).

1375 https://www.ietf.org/list/ (Date of use: 2 January 2016).

1376 https://www.ietf.org/list/ (Date of use: 2 January 2016).

1377 Galvin J "IAB and IESG selection, confirmation, and recall process: Operation of the nominating and recall committees" https://www.ietf.org/rfc/rfc2727.txt (Date of use: 2 January 2016).

administration and, thus, does not have an analogous management structure.[1378] Thus, IETF's secretariat is outsourced to a United States-based company, Association Management Solution.[1379]

The IETF, being an expert offshoot of the internet society, has its main driving force in the IESG. The structure of the IETF allows the participation of individuals that are interested in its activities without the payment of any fees or formal membership.[1380] This clearly removes many barriers to the participation of residents of developing countries. The IETF creates a multi-stakeholder approach to its participation and clamours for diversity in its participation.[1381] The main reliance on mailing lists as an effective mode of work and of communication with members of the IETF and IESG will encourage the participation of members of developing countries who ordinarily would be deterred by the cost of international travel.

Unfortunately, the participation of developing countries in IETF is rather discouraging.[1382] For example, Baryun, in a memo while discussing the issue of diversity in 2014, pointed out that there was only one participant from a developing country.[1383] The IESG has not felt the impact and input of the developing world either as its Chairperson or area directors.[1384] This may stem from the fact that the IETF community consists mainly of elites from the technical world.[1385] Also, the IETF's face-

---

1378 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 2 January 2016).

1379 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 2 January 2016).

1380 Doria A "The IETF and the multistakeholder model" https://docs.google.com/document/d/1x-WlVPfk3FZ9NKLeDJuQlk5WqG-HSVmm56c028D3xGg/edit?pref=2&pli=1# (Date of use: 4 January 2016).

1381 Doria https://docs.google.com/document/d/1x-WlVPfk3FZ9NKLeDJuQlk5WqG-HSVmm56c028D3xGg/edit?pref=2&pli=1# (Date of use: 4 January 2016).

1382 http://www.ietf.org/iesg/past-members.html (Date of use: 4 January 2016).

1383 Baryun A "Re: [Diversity] Diversity team wiki (was Re: Questions from USA Today" https://www.ietf.org/mail-archive/web/diversity/current/msg00598.html (Date of use: 4 January 2016).

1384 https://www.ietf.org/iesg/members.html (Date of use: 4 January 2016).

1385 Doria https://docs.google.com/document/d/1x-WlVPfk3FZ9NKLeDJuQlk5WqG-HSVmm56c028D3xGg/edit?pref=2&pli=1# (Date of use: 4 January 2016).

to-face meetings and first-time attendee training which are held three times a year have never been done in a developing country.[1386] The attendant cost of visa applications and travel will discourage most prospective participants that would have been glad to be part of the meetings and training. Arkko in 2013 further pointed out that participation in IETF are meant for persons that are domiciled around certain areas, with developing countries being left out.[1387] Furthermore, the association management solution as the outsourced private company that manages the activities of the IETF has no obligation to ensure diversity but merely to ensure the proper management of IETF's portfolio.[1388]

6.1.2.4. INTERNET GOVERNANCE FORUM

The internet Governance Forum (IGF) is a non-technical body that provides a multi-stakeholder platform for continuous dialogue on policies and directives that would shape the internet.[1389] The platform brings together governments, academics, private and public sectors, civil societies, technical bodies, developed and developing countries on an equal basis to participate in the ongoing internet governance debate.[1390]

The Forum's area of concern transcends issues on the technical fabrics of the internet and also delves into broader subjects such as the protection of children, data protection, cybercrime and the like.[1391] Thus, the Forum, amongst other functions, discusses issues that will foster the development and security of the internet, facilitate the exchange of information while utilising the expertise of the academic, scientific and technical world.[1392] The Forum also facilitates capacity building for developing countries in relation to internet governance, and promotes the participation of nations, especially

---

1386 https://www.ietf.org/meeting/past.html (Date of use: 4 January 2016).

1387 Jari Arkko is the Chairpersom of IETF. See Arkko J "Diversity" https://www.ietf.org/blog/2013/04/diversity/ (Date of use: 4 January 2016).

1388 https://www.amsl.com/index.html (Date of use: 4 January 2016).

1389 Calandro, Gillwald and Zingales http://www.researchictafrica.net/docs/Mapping%20multistakeholderism%20in%20internet%20governance%20draft%20final%2004082013.pdf (Date of use: 28 December 2015).

1390 http://www.intgovforum.org/cms/aboutigf (Date of use: 30 November 2015).

1391 https://www.afnic.fr/medias/documents/afnic-internet-governance-guide-06-2008.pdf (Date of use: 2 December 2015).

1392 http://www.intgovforum.org/cms/aboutigf (Date of use: 30 November 2015).

developing countries, in various existing and emerging internet governance schemes.[1393] The IGF was modelled as a neutral body without any binding or oversight functions to build on existing internet governance bodies, and which is subject to periodic review in order to ascertain the need for its future existence.[1394]

At the inception of the IGF, the then UN Secretary-General established the advisory group which has now metamorphosed into the Multi-stakeholder Advisory Group (MAG), to assist in convening IGF meetings and to advise the Secretary-General on IGF programmes and schedules of meetings.[1395] In order to maintain its multi-stakeholder stance, the MAG is made up of 55 members representing various governments, academic and technical communities, and the private sector and civil society.[1396]

The continuous[1397] operation of IGF is fairly important to developing countries. This is so because the IGF's multi-stakeholder approach provides developing countries with an opportunity of getting its voice heard on internet governance issues which would have been difficult with more technical bodies that require much expertise to be part of. IGF's increased chances of remote participation open up more effective ways of participating in IGF deliberations. This is more acceptable to most residents of developing countries who would have been denied the opportunity of participating through financial constraints and other impeding factors.[1398] IGF's policy of discussing and making recommendations on a wide range of issues mostly benefits developing countries that might have been shut out where only intricate technical internet policies are made. The IGF undertakes a lot of outreach programmes for developing countries, which are poised to draw developing countries out from their current complacency over ICT and its

---

1393 http://www.intgovforum.org/cms/aboutigf (Date of use: 30 November 2015).

1394 Xue H "Multinationals' global governance on the internet" in Rosen J (ed) *Individualism and collectiveness in intellectual property law* (Edward Elgar Cheltenham 2012) 269.

1395 http://www.intgovforum.org/cms/magabout (Date of use: 5 December 2015).

1396 http://www.intgovforum.org/cms/magabout (Date of use: 5 December 2015).

1397 IGF is designed to terminate after every five years subject to approval for its continuous existence where the need for the existence and further discussions on internet related issues is still expedient.

1398 https://www.intgovforum.org/cms/2011/Proposed%20Improvements%20to%20the%20IGF.PDF (Date of use: 6 December 2015).

attendant issues.[1399] The advent of various regional IGFs brings the forum nearer to developing countries and provides a platform for countries in a region to discuss internet-related issues that are relevant to the region, making the continuous existence of the IGF desirable for developing countries.[1400] Developing countries are the major recipients of IGF's outreach programmes and capacity-building schemes on a number of internet governance issues.[1401]

The multi-stakeholder structure of IGF creates substantial room for the participation of the developing world in the discussions and recommendations revolving around issues concerning the cyberspace. The body has no formal membership arrangement and thus is open to any participant, although participants are stakeholders drawn from either civil society, the private sector, government, internet technical or professional community.[1402] Incidentally, a part of the IGF mandate, as encapsulated by paragraph 72 of the Tunis Agenda, makes reference to enhancing the participation of developing countries in various internet governance mechanisms and the activities of IGF.[1403]

The IGF has no apex body but its activities and meetings are organised and reviewed by the Multi-stakeholder Advisory Group that is appointed by the UN Secretary-General. Developing countries have a reasonable number of representatives in the Advisory Group.[1404] Part of IGFs efforts to accommodate and ensure the participation of developing countries in IGF activities has provided developing countries with more opportunities to produce the Chairperson of the Multistakeholder Advisory Group.[1405] Representatives from Brazil, India, Kenya, Azerbaijan, Indonesia and Latvia have been

---

1399 https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c344b (Date of use: 11 December 2015).

1400 Teleanu S "Emerging IG issues from the perspective of regional and national IGF initiatives" https://www.internetsociety.org/blog/2012/11/emerging-ig-issues-perspective-regional-and-national-igf-initiatives (Date of use: 9 December 2015).

1401 http://igcaucus.org/submission-cstd-working-group-improvements-igf (Date of use: 9 December 2015).

1402 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 24 December 2015).

1403 http://www.intgovforum.org/cms/aboutigf (Date of use: 11 December 2015).

1404 http://www.intgovforum.org/cms/component/content/article?id=2102:mag-2015 (Date of use: 12 December 2015).

1405 Malcolm *Multi stakeholder* 356.

Chairpersons of the Multistakeholder Advisory Group in 2007, 2008-2010, 2011, 2012, 2013 and 2014-2015 respectively.[1406] Members of the MAG are also drawn from various nations of the world to represent IGF's multi-stakeholder diversity.[1407]

Several IGF meetings have been held in developing countries. This affords most participants from developing countries the opportunity to attend the IGF meetings, especially meetings held in the participants' region. For example, the first meeting in 2006 was held in Greece, while IGF meetings in 2007 to 2014 were held in Brazil, India, Egypt, Lithuania, Kenya, Azerbaijan, Indonesia and Turkey respectively.[1408]

The desire for enhanced participation of developing countries has led the IGF to provide various platforms for remote participation through its Remote Participation Working Group (RPWG).[1409] The platforms allow participation from various countries via blogs, e-mails, chat rooms, video and audio streaming, webcast and various other means.[1410]

The various regional and national initiatives of the IGF tend to bring participation in IGF closer to developing countries. A number of the regional, national and private stakeholders with common interests hold separate meetings and further participate in inter-regional dialogues at the annual IGF meetings.[1411] For example, there are the African IGF, the Asia Pacific IGF, the Central African IGF, the East African IGF, the Southern African IGF, the Latin American and Caribbean IGF and many other regional IGFs.[1412] There are the Azerbaijan IGF, the Bangladesh IGF, the Côte d'Ivoire IGF, the

---

1406 In 2007, Nitin Desai from India and Hadil da Rocha Vianna from Brazil co-chaired the MAG. In 2008-2010, Nitin Desai served as MAG Chair. In 2011, Alice Munyua from Kenya served as MAG Chair. In 2012, Elimir Valizada of Azerbaijan served as MAG Chair. In 2013, Mr Ashwin Sasongko of Indonesia served as MAG Chair. In 2014-2015, Jānis Kārkliņš served as MAG Chair. http://www.scoop.it/t/governance-by-dr-lendy-spires-foundation?page=4 (Date of use: 12 December 2015).

1407 https://www.intgovforum.org/cms/mag/45-mag-membership (Date of use: 5 November 2016).

1408 http://www.intgovforum.org/cms/athensmeeting (Date of use: 12 December 2015).

1409 http://www.intgovforum.org/cmsold/Contributions2009/Synthesis_Contribution_RPWG.doc (Date of use: 12 December 2015).

1410 http://www.intgovforum.org/cmsold/Contributions2009/Synthesis_Contribution_RPWG.doc (Date of use: 12 December 2015).

1411 http://www.intgovforum.org/cms/igf-initiatives (Date of use: 12 December 2015).

1412 http://www.intgovforum.org/cms/home-36966/77-igf-regional-events/igf-regional-and-national/2160-list-of-national-and-regional-igf-initiatives-2015 (Date of use: 12 December 2015).

Kenya IGF, the Mexico IGF, the Rwanda IGF, the Nigeria IGF and many other national IGF initiatives.[1413] Other interests groups such as the Youth IGF have also set up their own IGF initiatives.[1414]

Developing countries seem to be an integral part of IGF's policies, structures and governance. However, the management and structure and the fact that the body is not a decision-making body that can only make recommendations, makes the involvement or otherwise of developing countries in IGF's structure of little importance when reviewing the involvement of developing countries in internet governance, in particular, and combating cybercrime, in general.

6.1.2.5. THE INTERNET SOCIETY

The Internet Society (ISOC) is an international body that provides the platform for professionals from across various nations, interested in the future of the internet to interact.[1415] The body's mandate revolves around policy discourse, development of standards and approaches to address various internet issues.[1416] The body thus facilitates development of standards, protocols and technical infrastructure of the internet.[1417] It also facilitates capacity building, fosters participation, provides leadership on issues connected to the evolution of the internet and provides an environment for international cooperation.[1418]

In order to maintain an international outlook, ISOC's membership is open to organisations and individuals from across the globe without fees with the exception of those who elect to be sustaining members.[1419] ISOC also provides an institutional home

1413 http://www.intgovforum.org/cms/home-36966/77-igf-regional-events/igf-regional-and-national/2160-list-of-national-and-regional-igf-initiatives-2015 (Date of use: 12 December 2015).
1414 http://www.intgovforum.org/cms/home-36966/77-igf-regional-events/igf-regional-and-national/2160-list-of-national-and-regional-igf-initiatives-2015 (Date of use: 12 December 2015).
1415 https://www.techopedia.com/definition/2432/internet-society-isoc (Date of use: 9 January 2016).
1416 http://www.internetsociety.org/who-we-are/mission (Date of use: 9 January 2016).
1417 http://www.internetsociety.org/who-we-are/mission (Date of use: 9 January 2016).
1418 http://www.internetsociety.org/who-we-are/mission (Date of use: 9 January 2016).
1419 Weber RH *Shaping internet governance: Regulatory challenges* (Springer Heidelberg 2010) 39-72.

for a number of technical groups such as the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB), the Internet Engineering Steering Group (IESG) and the Internet Research Task Force (IRTF).[1420]

ISOC is governed by a board of trustees appointed or elected from the chapters, organisation members, and also from the Internet Engineering Task Force (IETF).[1421] The board of trustees drawn from all the regions of the world can then designate three or more of its members to form an executive committee.[1422] Members of the executive committee are chosen from the board of trustees.[1423] This mode of electing members of the board gives ample opportunity for developing countries to be part of the board.

ISOC's stance in providing a platform of interaction for institutions and individuals interested in cyberspace suits developing countries. The prevalent need of most developing countries is capacity building, and ISOC's capacity building initiatives which is at the core of ISOC's functions is of great importance to developing countries. ISOC's interactive platform provides grants to relevant outreach initiatives that address the educational, societal and humanitarian aspects relating to cyberspace and internet connectivity.[1424] The structure of ISOC that promotes the participation of developing countries through its regional and national chapters provides a platform which spurs developing countries to get involved. These chapters in turn promote educational

1420 Simonelis A "A concise guide to the major internet bodies" http://ubiquity.acm.org/article.cfm?id=1071915 (Date of use: 5 November 2016).
1421 http://www.internetsociety.org/who-we-are/board-trustees (Date of use: 9 January 2016).
1422 Weber *Shaping internet governance* 45-46.
1423 http://www.internetsociety.org/who-we-are/board-trustees/committees (Date of use: 9 January 2016).
1424 http://www.internetsociety.org/what-we-do/grants-awards (Date of use: 7 September 2016).

events,[1425] community programmes,[1426] public policy programmes[1427] and networking events[1428] which developing countries are in dire need of.

The international outlook of ISOC allows the participation of organisations and individuals without fees except for the sustaining members. This removes some financial burden from persons in developing countries who may have refrained from participating because of financial restraints.

Murray points out that ISOC reflects an open and democratic nomenclature and thus allows the creation of national chapters by anyone who wants to form a chapter, once 25 ISOC members can be mustered and a set of local bylaws enacted.[1429] The prominence of the national chapters in ISOC scheme of activities creates a multi-stakeholder platform that encourages diversity in participation.[1430] There are currently 110 active chapters which cut across six continents providing ISOC with various local and regional perspectives on emerging internet issues.[1431] Shears referred to ISOC as a global membership with a local perspective.[1432] Weber opined that the influence of ISOC's regional bureaus, chapters and members enables ISOC to assume the position of a multi-stakeholder internet forum.[1433]

1425 ISOC through its chapters educates members and the public on various internet-related issues; http://www.internetsociety.org/who-we-are/chapters (Date of use: 7 September 2016).

1426 ISOC's community programmes tries to ensure that internet access for economically-disadvantaged communities are attained. http://www.internetsociety.org/who-we-are/chapters (Date of use: 7 September 2016).

1427 ISOC engages policy makers on issues relating to the internet and ensures that those issues are addressed. http://www.internetsociety.org/who-we-are/chapters (Date of use: 7 September 2016).

1428 ISOC networks individuals and institutions interested in internet related issues and provides a platform for interaction. http://www.internetsociety.org/who-we-are/chapters (Date of use: 7 September 2016).

1429 Murray A *The regulation of cyberspace: Control in the online environment* (Routledge-Cavendish New York 2007) 91.

1430 Malcolm *Multi stakeholder* 44.

1431 http://www.internetsociety.org/who-we-are/chapters (Date of use: 11 January 2016).

1432 Shears M "The road to Rio and beyond current status of internet governance discussions" https://www.ripe.net/participate/meetings/roundtable/september-2007/roadtorio.pdf (Date of use: 11 January 2016).

1433 Weber *Shaping internet governance* 46.

The composition of the board of trustees ensures that various nations and regions are represented in the board. For example, the current board of trustees have members from Yemen and Kenya.[1434] Yamout, however, pointed out that just as other internet governance entities, the level of participation of developing nations in ISOC is low and its participation in the decision-making fora is even lower.[1435] Although some members of the board of trustees are from developing countries, the majority of the board members are from developed countries. For example, as many as five board members are from the United States of America.[1436]

6.1.2.6. THE WORLD WIDE WEB CONSORTIUM

The World Wide Web Consortium (W3C) is another standard-setting entity whose mandate revolves generally around the infrastructure, applications and technical development of the internet, and majorly ensuring the growth of the World Wide Web through the development of protocols and guidelines.[1437] The body also engages in the development of software, education, various outreaches, and providing the forum for discussions about the growth of the web.[1438] The membership of W3C is open to organisations, content providers, standard entities, technology products vendors, research laboratories, universities, governments and individuals.[1439]

W3C is jointly overseen by the MIT Computer Science and Artificial Intelligence Laboratory located in the United States of America, Keio University located in Japan, Beihang University located in China, and the European Research Consortium for Informatics and Mathematics located in France.[1440] The W3C also maintains 19 regional

1434 http://www.internetsociety.org/who-we-are/board-trustees (Date of use: 11 January 2016).
1435 Yamout S "Developing nations participation in internet governance" http://www.intgovforum.org/cms/wks2014/index.php/proposal/view_public/103 (Date of use: 11 January 2016).
1436 http://www.internetsociety.org/who-we-are/board-trustees (Date of use: 11 January 2015).
1437 https://www.w3.org/Consortium/mission (Date of use: 17 January 2016).
1438 https://www.w3.org/Consortium/mission (Date of use: 17 January 2016).
1439 https://www.w3.org/Consortium/membership-faq (Date of use: 5 November 2016).
1440 https://www.w3.org/Consortium/facts (Date of use: 17 January 2016).

offices across the world.[1441] This joint agreement, partnership and regional offices attempt to reflect an international stance to the operation of the W3C and increase its geographical base while promoting global participation in its activities.[1442] W3C's activities are governed by the director and CEO with the team of professional staff, the Advisory Committee, the Advisory Board, the Technical Architecture Group (TAG) and the chartered groups.[1443]

The importance of the expertise of W3C to the growth of the internet and the World Wide Web has prompted the need for a global participation in its standard-setting activity. The W3C thus promotes the participation of the individuals and institutions from around the world to be part of its business. In its multi-stakeholder approach, W3C welcomes anybody to participate in its policy discussions and standards development processes although certain areas are restricted to W3C members.[1444] The W3C also employs the input of invited experts to join a working group and W3C staff to fashion out proposals for certain areas or topics of interest.[1445] The participation of these invited experts provides an opportunity for participation from experts outside the W3C body.

However, membership requirements, although transparent, must be reviewed and approved by the W3C upon application.[1446] Unfortunately, there is no final guideline relating to the process of approval or denial of membership to the W3C.[1447] Again, although its membership is open to individuals, the W3C in practice is a conglomerate of businesses and organisations. In fact, the W3C's publication on its membership states: "Our processes are designed for organisational participation and we do not have

---

1441 Bird JA "Addresses of W3C offices" https://www.w3.org/Consortium/Offices/staff (Date of use: 23 January 2016).

1442 Birkenbihl K "Roles of W3C offices" https://www.w3.org/Consortium/Offices/role.html (Date of use: 23 January 2016).

1443 https://www.w3.org/Consortium/facts (Date of use: 23 January 2016).

1444 https://www.w3.org/Consortium/membership-faq#who (Date of use: 23 January 2016).

1445 Nevile CM "World wide web consortium process document" https://www.w3.org/2015/Process-20150901/ (Date of use: 5 November 2016).

1446 Nevile https://www.w3.org/2015/Process-20150901/ (Date of use: 5 November 2016).

1447 Nevile https://www.w3.org/2015/Process-20150901/ (Date of use: 5 November 2016).

the support structure to handle large numbers of individual members".[1448] This hampers the chances of persons from developing countries to participate in W3C activities.

The structure of W3C thus impedes the participation of developing countries in its activities. For example, out of the 410 membership strength of W3C, only a few corporations from developing countries, such as the National Informatics Centre of India, the National Internet Exchange of India, the National Payments Corporation of India and the KIIT College of Engineering Gurgaon, are members of the W3C. W3C staff members are from developed countries,[1449] while most members of the Advisory Committee (the committee that makes final decisions on proposals) have very few members from developing countries since every member organisation appoints a representative to the Advisory Committee.[1450]

6.1.2.7. NUMBER RESOURCE ORGANISATION

The Number Resource Organisation (NRO) is involved in the provision of a harmonised internet number registry scheme and thus contributes to the core internet resources and ensures a secure and stable internet.[1451] The body contributes to policy formations in internet governance and also coordinates the five Regional Internet Registries (RIR) that administer the distribution of internet number resources which include Autonomous System Numbers (ASN) and Internet Protocol (IP) addresses.[1452]

The RIRs, the major nucleus of NRO's business, administers the allocation and registration of internet numbers in each region of the world.[1453] These regional bodies thus represent the various diverse internet stakeholders and present a multi-stakeholder approach in the distribution of internet number resources.

1448 https://www.w3.org/Consortium/membership-faq (Date of use: 23 January 2016).
1449 https://www.w3.org/People/ (Date of use: 23 January 2016).
1450 Nevile https://www.w3.org/2015/Process-20150901/ (Date of use: 5 November 2016).
1451 https://www.nro.net/ (Date of use: 30 January 2016).
1452 http://www.internetsociety.org/deploy360/resources/number-resource-organization/ (Date of use: 30 January 2016).
1453 https://www.nro.net/about-the-nro/regional-internet-registries (Date of use: 30 January 2016).

Membership of the NRO is universal but limited to the RIRs.[1454] Schweighofer points out that the RIRs have many individual members representing various local interests.[1455] Some RIRs restrict their membership to end users or entities that have entered into service agreements with the Registry, while some Registries, in addition to the end users or entities with service agreements, also allow individuals with interest in their activities to participate. For example, to participate as a member of the American Registry for Internet numbers (ARIN), the entity must have a valid registration services agreement for internet number resources, or an individual appointed or elected to the board of trustees.[1456] On the other hand, for the Internet Numbers Registry for Africa (AFRINIC), a legal person who meets the criteria for internet number resource and signs the registration service agreement, an individual or organisation with an interest in number resources management and any director who is a member can participate as a member.[1457] The RIR, however, encourage more multi-stakeholder input into its activities and policy development through the use of RIR communities made up of internet service providers, governments at various levels, universities, private and public corporations, civil societies and the like.[1458] The RIR's policy-making processes are thus designed to allow any interested person (member or non-member) to participate in the process.[1459] There are no restrictions or requirements on who may propose or amend a policy.[1460] For example, the American Registry for Internet numbers (ARIN) states clearly that any interested party is encouraged to participate in its policy development.[1461]

The NRO Executive Council, Number Council and the Secretariat make up the organisational structure of the NRO and these are drawn from the five Regional Internet

1454 Barret A "NRO-NC / ASO-AC Address Council Report" https://internetsummitafrica.org/images/AIS14_slides/Alan_Barrett-nro-nc.afrinic20_201406.pdf (Date of use: 30 January 2016).
1455 Schweighofer *ICANN* 88.
1456 https://www.arin.net/about_us/membership/overview.html (Date of use: 30 January 2016).
1457 http://afrinic.net/en/about-us/our-members (Date of use: 30 January 2016).
1458 https://www.nro.net/about-the-nro/regional-internet-registries (Date of use: 30 January 2016).
1459 https://www.nro.net/about-the-nro/regional-internet-registries (Date of use: 30 January 2016).
1460 https://www.nro.net/about-the-nro/regional-internet-registries (Date of use: 30 January 2016).
1461 https://www.arin.net/participate/how_to_participate.html (Date of use: 30 January 2016).

Registries (RIRs).[1462] This ensures adequate representation from various regions of the world. For example, three members of each RIR are appointed into the Number Council of the NRO.[1463] The Executive Council is made up of the Chief Executive of each RIR and the positions within the Executive Council rotate annually.[1464]

The RIRs as representatives of entities and interested individuals in each region naturally has the majority of its members, staff, board of directors and other keys functionaries drawn from those regions. For example, the AFRINIC, which serves Africa and the Indian ocean, has members of its board of directors drawn from Nigeria, Tanzania, Mauritius, Egypt, the DRC, South Africa and Niger.[1465] The RIR structure presents a veritable opportunity and platform for the participation of individuals from both developed and developing countries. The NRO being a consortium of RIRs and having its members and functionaries drawn from the five RIRs also presents a veritable opportunity and platform for the participation of individuals from both developed and developing countries.

It must be pointed out that in 2015, out of 30,584 members of RIRs, Reseaux IP Europeens (RIPE), which serves the European, Middle East and Central Asia, had the highest number of members (11,305 members) while the Internet Numbers Registry for Africa (AFRINIC), which serves Africa and the Indian ocean, has the lowest number of members (1,153 members).[1466] The APNIC, the Asia Pacific Network Information Centre (APNIC) which serves the Asia Pacific region had 8,730 members; the American Registry for Internet numbers (ARIN) which serves Canada, the United States, North Atlantic and some Caribbean Islands, has 5,075 members, while the Latin American and Caribbean Internet Addresses Registry (LACNIC) which serves the Latin American and the Carribbean regions has 4,321 members.[1467] This shows that the regions with

1462 https://www.nro.net/about-the-nro (Date of use: 30 January 2016).
1463 https://www.nro.net/about-the-nro/the-nro-number-council (Date of use: 30 January 2016).
1464 https://www.nro.net/about-the-nro (Date of use: 30 January 2016).
1465 https://www.afrinic.net/en/about-us/our-structure/bod (Date of use: 30 January 2016).
1466 https://www.nro.net/about-the-nro/nro-faq (Date of use: 30 January 2016).
1467 https://www.nro.net/about-the-nro/nro-faq (Date of use: 30 January 2016).

more developing nations, as in Africa, have a lower level of participation with respect to membership.

6.2. EXTENT OF PARTICIPATION OF DEVELOPING COUNTRIES IN INTERNET GOVERNANCE

The core interest of various internet governance entities revolve around specific areas of internet regulation, governance or provision and thus are mostly representative bodies of groups with common interests in those areas. For example, the NRO and RIR deal with address resources while IETF deals with technical and infrastructural development of the internet. Thus internet governance bodies end up encouraging the participation and membership of bodies and individuals with expertise in the entity's interest area. The insistence on specialisation may well explain one of the major reasons why developing countries that are still grappling with capacity building lag behind in their participation within these internet governance entities. It is fairly obvious that the level of participation of most developing countries constrained by limited resources is largely dependent on the availability of points of participation and how accessible and straightforward those points are.[1468] Bodies that do not disparage contributions from those with less expertise and allow contributions from outside its community will receive the patronage of most developing countries.[1469]

In order to appreciate the extent of the participation of developing countries in internet governance and regulation in its various forums, it will be pertinent that the level of participation of various nations be grouped under some taxonomy. Thus, the extent of

---

1468 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 15 May 2016).

1469 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 15 May 2016).

participation in the various internet governance bodies can be categorised into three tiers which include:[1470]

(i) formal participation ensuing from some form of membership;
(ii) representation of members in the decision making processes of the various entities;
(iii) the extent of input from non-members in the decision making process.

6.2.1. FORMAL PARTICIPATION BASED ON MEMBERSHIP

Various internet governance entities allow some form of membership to individuals and organisations, which will allow access to participation in its activities.[1471] However, most internet governance entities, in creating a multi-stakeholder platform that would allow for broader participation, allow non-members with common interests to participate in its activities.[1472] From the foregoing analysis of the afore-mentioned internet governance entities, membership arrangements between various internet governance entities vary. For example, membership of ITU-T and W3C is practically restricted to organisations, governments and official bodies.[1473] Membership into the RIRs is open to organisations in the region that require address space from the RIR.[1474] For some RIRs such as the ARIN, address space users are automatic members while some other RIRs such as the

1470 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 15 May 2016).

1471 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 15 May 2016).

1472 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 15 May 2016).

1473 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 15 May 2016).

1474 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 15 May 2016).

RIPE-NCC, membership is optional.[1475] For ISOC, its membership is open to organisations and individuals without a fee or upon payment of a fee for those who want to participate in the elections.[1476] The IETF and IGF have no membership arrangement. The IETF is open to any individual or organisation intending to participate in its activities, thus making the IETF rely on the use of volunteers instead of representatives.[1477] The IGF structure allows a multi-stakeholder platform which is open to governments, the private sector, civil society and internet technical or professional community.[1478] For ICANN as a corporation with a complex membership structure, the body has various subsidiary bodies representing various communities with an interest in ICANN's work. These range from technical agencies such as the Address Supporting Organisation, Country Code Names Supporting Organisations, Generic Names Supporting Organisations, governments (who can participate through the Governmental Advisory Committee) and individual internet users who are represented through the At Large Structures.[1479]

6.2.2. REPRESENTATION OF MEMBERS IN THE DECISION-MAKING PROCESSES OF THE VARIOUS ENTITIES

The various internet governance entities have created some form of final decision-making arm or apex structure which oversees the entity's affairs. The apex wing of these entities are selected or elected from the various groups, bodies or individuals who participate in the entity's activities and are mainly members of the entity with expertise.

1475 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 15 May 2016).

1476 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 15 May 2016).

1477 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 15 May 2016).

1478 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 24 December 2015).

1479 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 24 December 2015).

For example, each RIR has some form of executive council or board, elected by its members, while the W3C has the Advisory Committee (which is an assembly of W3C members) sitting atop its structure, who then appoints an Advisory Board to provide guidance to the body.[1480] ISOC, for its part, is governed by a board of trustees elected from the various constituencies, organisational and individual members (through its national chapters), and various internet technical bodies which are affiliated to ISOC.[1481] The IETF is coordinated by the Internet Engineering Steering Group, although each working group determines how they function.[1482] ICANN has the board of directors atop its echelon who are selected by its supporting organisations and by a nominating committee saddled with the responsibility of appointing qualified directors from the list of those who wish to be appointed.[1483] IGF's meetings are coordinated with the support of the Multistakeholder Advisory Group appointed by the Secretary-General of the UN, and thus has no formal apex body.[1484]

Souter points out that the institutional authority of these entities are more of a collaborative arm binding the various divisions or levels within each entity, and thus are weaker than other apex structures of institutions outside the existing internet governance bodies whose hierarchical structure highlights a concrete chain of command.[1485] For example, in IETF, the Internet Engineering Steering Group does not determine how the working groups function, while the individual area directors direct the particular areas of activity and none of these top arms have a final say on the working

---

1480 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 24 December 2015).

1481 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 24 December 2015).

1482 Alvestrand H "An IESG charter" https://www.ietf.org/rfc/rfc3710.txt (Date of use: 24 December 2015). See also Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 24 December 2015).

1483 Schweighofer *ICANN* 83.

1484 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 24 December 2015).

1485 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 24 December 2015).

groups.[1486] The Advisory Committee of the W3C does not act as a board of directors and has no decision-making authority but rather an advisory role.[1487] The executive council of the RIRs has a limited role in overseeing the body's policy-making process in relation to IP address allocation and registration which is the core of the body's existence.[1488]

The involvement and level of participation of developing countries in the decision-making arm of the various internet governance entities is abysmal. For example, the members of the W3C advisory board[1489] are drawn from companies such as IBM, Mozilla, Microsoft, NTT Nippon Telegraph and Telephone Corp, Gemalto, Yandex, Apple, the Paciello Group, Google and Alibaba, all headquartered in developed countries.[1490] ISOC has three of its board of trustees from developing countries (Yemen, Sri Lanka and Kenya) while the rest (ten) are from developed countries.[1491] The Internet Engineering Steering Group has its members drawn from various developed countries and companies domiciled in developed countries.[1492] Few members of the Multistakeholder Advisory Group are from developing countries.[1493] Only a few individuals from developing countries are members of the board of directors of ICANN.[1494] In fact, some of the persons from developing countries really have stronger ties to developed countries (and will most likely propagate their interests) such as the

---

1486 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 24 December 2015).

1487 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 24 December 2015).

1488 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 24 December 2015).

1489 https://www.w3.org/2002/ab/ (Date of use: 10 September 2016).

1490 These companies are headquartered in the United States of America, United States of America, United States of America, Japan, The Netherlands, Russia, United States of America, United States of America, United States of America and China respectively.

1491 http://www.internetsociety.org/who-we-are/board-trustees (Date of use: 10 September 2016).

1492 https://www.ietf.org/iesg/members.html (Date of use: 10 September 2016).

1493 http://www.intgovforum.org/cms/mag/45-mag-membership/3030-mag-2016-membership-2 (Date of use: 10 September 2016).

1494 https://www.icann.org/resources/pages/board-of-directors (Date of use: 10 September 2016).

Vice-Chairperson of ICANN's board of directors who is an Egyptian with British citizenship and with a greater part of his working experience in the United Kingdom.[1495]

6.2.3 EXTENT OF INPUT FROM NON-MEMBERS IN THE DECISION-MAKING PROCESS

Most internet governance entities create some form of avenue for non-members who are interested in the activities of the entity to make some input. This is essential as the criteria for membership in most internet governance bodies may be cumbersome or specialised for certain classes of interested persons or institutions to make a useful input. For example, some of the entities (such as the IGF) have created some form of community of interested persons, and through its open consultations solicit their views on some of the entity's areas of interest. Most internet governance entities, such as ICANN and the RIRs, organise public meetings which encourage the input of non-members who attend these. Blogs, websites and other information channels are relied upon by most entities to receive inputs and feedback on their activities. Online mailing lists are also utilised by most entities and made available to both members and the public for their input. These channels provide ample opportunity for non-members to make some input.

However, as pointed out by Souter, participation is not attained by the mere provision of opportunities to the public but diversity of participation is encouraged by the way in which these opportunities are configured.[1496] The attitude of members to newcomers or non-members, the traditions and ethos of the decision-making forum and the availability of remote participation have an effect in propelling better participation than the mere provision of technical opportunities.[1497]

1495 https://www.icann.org/profiles/cherine-chalaby (Date of use: 10 September 2016).

1496 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 13 March 2016).

1497 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 13 March 2016).

It must be pointed out that it is ideal that these internet governance entities should encourage openness, transparency and inclusiveness which will allow non-members to make inputs and add to the entity's policy and decision-making process. This is so because an entity may be transparent in its management and policy making without being accessible to stakeholders that will be affected by the entity's policies.[1498] The ability of each entity to allow inputs from non-members will enhance the chances of stakeholders from developing countries who cannot afford the cost and demands of membership to still participate in the formulation of policies.

However, most internet governance entities already have their core target membership which often excludes institutions and agencies from developing countries.[1499] Giving room for input from non-members in the decision-making process of the various internet governance entities holds some hope for the participation of developing countries in the policy-making formulations of relevant internet governance bodies that affect them.

The benefits of this informal practice can be seen in the philosophy of some afore-mentioned internet governance entities. According to Souter, most internet governance entities, unlike other international agencies, already express a wide space for all-inclusive participation and collaboration.[1500] He further posits that this inclusive participation is an off-shoot of the collaborative nature that characterised internet's early development, where loose associations of volunteers were responsible for the internet's architecture and technical standards.[1501] These internet governance bodies in their statements affirm their willingness to allow broad participation of non-members. For example, ICANN states that it "operates on a multi-stakeholder model that brings all

1498 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 13 March 2016).

1499 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 13 March 2016).

1500 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 13 March 2016).

1501 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 13 March 2016).

interested parties together to discuss policy issues that fall within ICANN's areas of responsibility".[1502] The W3C, in its effort to engage the broader public, states that one of its goals is to "make it extremely easy for individuals (not just organisations) to participate actively in the W3C community".[1503] Furthermore, APNIC (an RIR) states that its policies are developed by its members with the input and collaboration of the wider internet community.[1504]

Unfortunately, what organisations posit as their mission statements and their beliefs are mostly inconsistent with their practice.[1505] For example, although ICANN's meetings are open to the public, most attendees/participants are from developed countries. Hofmann points out that the greater part of attendees at ICANN meetings are related to the internet industry and mainly from OECD countries.[1506] She further points out that individuals and non-commercial internet users do not have an effective voice in relation to ICANN policy issues.[1507] Invariably, ICANN does not make room for all stakeholders to participate in ICANN policy formulation but rather, actual influence on the policy formulation process varies significantly among the various groups within ICANN. Park points out that governments of developing countries rarely attend ICANN meetings except when they are faced with some CCTLD management strain with various non-state actors.[1508]

A South African case study by the University of the Witwatersrand, in analysing the current level of participation in international ICT decision making, found that South Africa participates extensively in the various international ICT decision-making bodies,

---

1502 https://www.icann.org/en/system/files/files/acct-trans-frameworks-principles-17oct07-en.pdf (Date of use: 13 March 2016).

1503 https://www.w3.org/2010/04/w3c-vision-public/wiki/Newstd (Date of use: 1 May 2016).

1504 Malcolm *Multi stakeholder* 307.

1505 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 13 March 2016).

1506 Hofmann J "Internet Corporation for Assigned Names and Numbers (ICANN)" http://www.giswatch.org/sites/default/files/gisw_icann_0.pdf (Date of use: 30 May 2016).

1507 Hofmann http://www.giswatch.org/sites/default/files/gisw_icann_0.pdf (Date of use: 30 May 2016).

1508 Park YJ *The political economy of Country Code Top Level Domains* (ProQuest Ann arbour 2008) 156.

but rather unevenly when compared to developed countries.[1509] The study found that South Africa, although a leader on the African continent, unfortunately tends to follow rather than lead.[1510]

In a nutshell, the extent of input in the decision-making bodies by institutions and agencies from developing countries, whether as members or non-members, is rather appalling. Souter points out that these bodies chiefly encourage persons or institutions that are part of their core communities to participate, allowing those outside the core community some sort of associate membership.[1511] Unfortunately, most developing countries find themselves outside these core communities.

6.3. ENCOURAGING PARTICIPATION OF DEVELOPING COUNTRIES IN INTERNET GOVERNANCE

This research has highlighted the several policy-making organs of some internet governance agencies, and it is obvious that the participation of developing countries in the affairs and decision-making organs of the previously-mentioned internet governance bodies is abysmal. Several factors have been pointed to as the reason behind the apathy of developing countries in participating actively within the ranks of various internet governance agencies. Some of these factors include:

- **Lack of awareness**

  The CTO/Panos study on "Strengthening Developing Country Participation in International ICT Decision-Making" found that a major obstacle to the effective participation and representation of developing countries in the various internet governance agencies is the lack of awareness of policy, policy venues,

---

1509 Gilwald A "Strengthening participation by developing countries in international decision-making: Case study of South Africa" https://www.wits.ac.za/media/migration/files/SACTOP.pdf (Date of use: 4 July 2016).

1510 Gilwald https://www.wits.ac.za/media/migration/files/SACTOP.pdf (Date of use: 4 July 2016).

1511 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 15 May 2016).

governance process and the need to appreciate those governance process.[1512] The study also found that there is a lack of awareness among policy makers of developing countries on the significance of international decisions on the country's national ICT policy framework and regulations.[1513] The study further found that most developing countries lack awareness in relation to the benefits of ICT and the role it plays in development.[1514] However, the lack of awareness in developing countries on the benefits of ICT can be said to be fast disappearing as a result of increased ICT penetration within developing countries although so many grounds are still to be covered.[1515]

- **Lack of technical and policy capacity**

  ICT remains a novel area in most developing countries and emerging issues appear complex as a result of the dearth of persons and institutions with the requisite technical capacity. Emerging ICT issues such as a migration to IP-based networks, e-commerce applications, implementation of future generation mobile communications systems, and protection of intellectual property rights, remain an enigma to several developing countries.[1516]

  Building technical and policy capacity becomes increasingly difficult as it can only be evolved through years of education, sensitisation and work experience in which developing countries rarely invest.[1517] On the other hand, most governments of developing countries rarely recruit seasoned ICT experts and

---

1512 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 23 July 2016).

1513 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 23 July 2016).

1514 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 23 July 2016).

1515 According to Brahima Sanou, the Director of the ITU Telecommunication Development Bureau, 3.2 billion people in 2015 used the internet around the world and 2 billion users were from developing countries. Sanou B "The world in 2015" https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf (Date of use: 23 July 2016).

1516 Achugbue EI and Akporido CE "National information and communication technology policy process in developing countries" in Adomi EE (ed) *Framework for ICT policy: Government, social and legal issues* (IGI Global New York 2011) 218-232.

1517 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 23 July 2016).

also fail to build technical and policy capacity, while the existing ICT experts are mostly attached to the private sector.[1518] The reluctance in attracting ICT experts by governments further compounds the ability of the various nations to adequately participate in international ICT discourse and fora since most internet governance bodies only allow the participation of government stakeholders.[1519]

- **Difficulty in accessing information**

  Another obstacle in the participation of developing countries is the absence of affordable, effortless and timely access to information and analysis about ICT-related issues.[1520] The low degree of internet penetration in developing countries limits its access to information. A large number of persons in developing countries find internet access expensive and can hardly afford paper-based publications.[1521] Maclean *et al* point out that the rapid changes that ICT policy agenda has witnessed across the various internet governance bodies make it difficult for developing countries to keep track with the changes, foresee key events and map out their strategies for successful results.[1522] They further point out that when the rapid change is only an "information overload" for developed countries, these changes amount to "information scarcity" for developing countries because of the state of their access to information.[1523]

- **Financial barriers**

  Economic indices and financial capabilities are an important measuring line in determining the level of development a country has attained. Most developing countries are bedevilled with economic woes and financial constraints leaving

---

1518 Achugbue and Akporido *National information and communication technology* 218-232.

1519 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 23 July 2016).

1520 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 23 July 2016).

1521 Eagle N "How to make the internet free in developing countries" https://techcrunch.com/2015/06/01/how-to-make-the-internet-truly-free-in-developing-countries/ (Date of use: 24 July 2016).

1522 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 24 July 2016).

1523 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 24 July 2016).

most of its citizens living on and below the established poverty lines. The high cost of attending meetings, the cost of accessing appropriate information, the cost of keeping up with the increased number of internet-related meetings and the various cadres of decision or policy-making bodies dissuade persons and institutions in developing countries from participating in internet governance agencies.[1524] Most developing countries still battle to provide their citizens with the basic amenities of life while relegating other aspects that can boost their development to the background.

Conversely, the economic situation and levels of corruption, a common feature of developing countries, make recipients of international fellowships abuse the grants by sponsors, and national governments for political and selfish reasons send persons without requisite ICT knowledge to represent their interests at meetings.[1525] Fellowships and grants for attendance at various internet governance fora end up not reaching the right persons from developing countries who should be attending these meetings.

- **Weaknesses in ICT policy processes**

  General weaknesses in ICT policy processes also act as an obstacle to the participation of developing countries in internet governance.[1526] Most internet governance agencies revolve around the partnership and inputs of various national governments or institutions. However, many developing countries do not possess a national ICT strategy, lack proper political leadership and fail to effectively provide proper synergy between varying government ICT agencies within its clime.[1527] Maclean *et al* found that there was a failure to disseminate information to affected government agencies or other stakeholders in developing

---

1524 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 24 July 2016).

1525 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 24 July 2016).

1526 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 24 July 2016).

1527 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 24 July 2016).

countries about meetings, and a failure to prepare and evolve a national position after consultation with stakeholders prior to meetings.[1528] Maclean *et al* in their study also found that the non-inclusion of qualified technical and policy experts in the national delegation that will participate in the international meetings, and an absence of implementation and accountability mechanisms bedevilled most developing countries.[1529] Again, information on the outcome of international meetings is not relayed to appropriate national stakeholders.[1530]

Maclean *et al* in their study found that at the regional level where developing countries are prevalent, there is the absence of effective preparatory processes and institutions for international meetings and this has hampered the participation of developing countries, especially at this time when policy positions are coordinated at regional levels in order to have a stronger voice at international meetings.[1531]

- **National priorities**

  Another obstacle hampering the participation of developing countries are the priorities of the political class that translate to the national priorities. Most developing countries have their policies and priorities set by the political class who often are not technocrats, and their decisions on issues, whether widely consulted on or not, are forced down the throats of technocrats and other stakeholders.[1532] The apathy of the ruling class rubs off on the stakeholders in the country, especially since most internet governance bodies are represented by

---

1528 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 24 July 2016).

1529 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 24 July 2016).

1530 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 24 July 2016).

1531 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 24 July 2016).

1532 For example, as at 2016, in Nigeria the Minister of Power, Housing and Works is a lawyer with no training or experience in power generation or distribution, housing or road construction and other accompanying responsibilities. See Mohammed Y "Appoint experienced person to head power ministry Ewenla tells Buhari" http://www.pmnewsnigeria.com/2016/04/27/appoint-experienced-person-to-head-power-ministry-ewenla-tells-buhari/ (Date of use: 25 September 2016).

national governments. A major obstacle to the participation of developing countries is the inadequacy of human resources which is exacerbated by the national priorities.[1533] According to Achugbue *et al*, the governments of most developing countries find it difficult to recruit and retain qualified ICT staff.[1534] Providing the basic amenities of shelter, clothing and food still features prominently in the agenda of most developing countries.[1535]

With the various obstacles that affect the readiness of developing countries in participating in the affairs and decision-making processes of the existing internet governance bodies, several pundits have tried to proffer salient steps that internet governance entities should adopt in order to ensure the participation of developing countries. Some of these steps include:

- **Raising policy awareness**

  The levels of awareness in developing countries of the activities of internet governance entities and the need for participation should be increased.[1536] Maclean *et al* proffered that developing a global information resource on ICT policy holds an important key in raising the awareness within national precincts.[1537] This global information resource will provide information on the activities of the various internet governance bodies, provide information on dates and policy venues for the various internet governance activities.[1538] Representatives of the various national governments should be mandated to create an information agency that will transmit information to national stakeholders via all information channels. The representatives of the various

---

1533 Achugbue and Akporido *National information and communication technology* 218-232.

1534 Achugbue and Akporido *National information and communication technology* 218-232.

1535 Most politicians in most developing countries still employ the provisions of basic amenities of life as a tool in winning votes. Unfortunately, most of these promises evaporate after the electioneering campaigns. See Haider S "The politics of providing basic amenities to the urban poor" in Mohanty B (ed) *Urbanisation in developing countries: Basic services and community participation* (Concept Publishing New Delhi 1993) 389-396.

1536 Gilwald https://www.wits.ac.za/media/migration/files/SACTOP.pdf (Date of use: 4 July 2016).

1537 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 23 July 2016).

1538 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 23 July 2016).

governments can be constrained (through treaties or sanctions) to keep on creating awareness of the importance of the internet within their national boundaries, so that the problems created by the lack of awareness of the role the internet and its governing bodies play in development will decrease. The internet, newsletters, annual reports and other information channels can be employed by the central information resource and passed down through the national information agencies for the benefit of national stakeholders, with modifications that will appeal to the locals.

- **Capacity building**

  Building technical and policy capacity in developing countries holds another important key in encouraging the participation of developing countries. The various internet governance fora can break this barrier by establishing standards required of representatives of developing countries with a mandate on the developing country to pass on the acquired skill and capacity to interested institutions. These various for a must embark on continuous education and training since it is apparent that capacity building takes years of education and work experience.[1539] According to Maclean *et al*, the various international ICT fora should also embark on independent technical and policy research, and analysis of pertinent emerging issues.[1540] Internet governance bodies should also encourage the establishment of a global network of constituent regional and national institutes or hubs with the responsibility of conducting research and training on internet policy and regulatory issues.[1541] Also, the establishment of funds that will support this research and training within the peculiarities of various developing countries will positively impact on the decision making of the sponsoring internet governance body.[1542]

1539 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 23 July 2016).

1540 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 23 July 2016).

1541 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 23 July 2016).

1542 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 23 July 2016).

- **Strengthening national policy institutions and repositioning national priorities**

  Strengthening national and regional policy institutions and repositioning national priorities hold a veritable key in encouraging the participation of developing countries in the policy process of various internet governance bodies. This can be achieved by encouraging the involvement of all national stakeholders in national policy-making and strategy formulation.[1543] The promotion of public discussions and debates, the improvement of information flow and policy harmonisation between various government institutions and agencies with ICT responsibilities will also encourage the participation of developing countries.[1544] Experts from the private sector and civil society must be encouraged to participate in the national policy formulation and to be part of the national delegation to the various internet governance decision-making arms.[1545]

  Conversely, the political class should be constantly reminded of the attendant benefits (especially economic benefits) of the internet and need for the country to participate in the internet governance policy-making process. They should also be held accountable (through treaties and sanctions) by the various internet governance bodies to which the country subscribes, for the failure of their country's to evolve a formidable national policy.

  On the regional and sub-regional level, strategy formulation, discussions and debates, information sharing, participation of experts drawn from all facets of stakeholders must be encouraged and facilitated.[1546]

1543 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 23 July 2016).

1544 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 23 July 2016).

1545 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 23 July 2016).

1546 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 23 July 2016).

- **Provision of adequate fiscal support**

  A major feature of most developing countries is the paucity of funds. All the various mechanisms that will encourage the participation of developing countries in actively participating will require funding for such programmes to be sustained. Capacity building, training, dissemination of information, procurement of debates, organisation of policy formulation meetings, and travelling fellowships to get country representatives to attend international policy venues all require funding.[1547]

  The Panos study, however, pointed out that the provision of funding does not eliminate the issues as the ineffective use of resources, more than financial deficiency, creates a paucity of funds.[1548] The various ICT institutions in developing countries must be re-organised to ensure efficiency by properly allocating resources and ensuring that the funds are allocated to sponsor the right experts or persons.[1549] Also, current practices relating to delegate selection, conference preparation, participation and accountability must be reassessed to ensure that financial resources are channelled appropriately to prevent embezzlement or inefficient use of resources.[1550]

- **Participation in international internet governance fora must be prioritised**

  On top of the list of actions that must be embarked upon to encourage the participation of developing countries is the prioritising of the involvement of developing countries. These internet governance bodies must of its own volition facilitate the involvement of developing countries by actively including them in the organisational structure and policy-making processes of these internet

---

1547 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 23 July 2016).

1548 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 23 July 2016).

1549 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 23 July 2016).

1550 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 23 July 2016).

governance bodies.[1551] Hossain suggests that meetings of these internet governance bodies can be held mainly in developing regions, while developing countries may be allocated more seats and positions in these bodies.[1552]

- **All information on each internet governance entity and its activities should be made available to the public**[1553]

- **The standard development and policies of the various internet entities should be inclusive, open and transparent**[1554]

- **Ideas on policy and standards development can be initiated by anyone and participation in the development of the internet should be made open to anyone with a desire to participate irrespective of status**[1555]

- **Ideas, once initiated, belong to the internet entity rather than the initiator or his region**[1556]

  This will help blur the divide between developed countries and developing countries, reduce unnecessary competition that will further scare developing countries and encourage team work amongst them.

1551 Hossain J "View from the desk of the Internet Governance Secretariat" http://www.internetsociety.org/ur/node/380526 (Date of use: 2 August 2016).

1552 Hossain http://www.internetsociety.org/ur/node/380526 (Date of use: 2 August 2016).

1553 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 2 August 2016).

1554 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 2 August 2016).

1555 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 2 August 2016).

1556 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 2 August 2016).

- **Further developments should be collaborative and should take place in meetings that allow participation from any interested party or should take place online to ensure broad participation**[1557]

- **The adoption of novel policies and standards should be borne out of consensus rather than majority decisions**[1558]

  This will enable the input of developing countries to be sought and policy positions explained adequately so that they can key into same. This is so because reliance on consensus decisions will constrain the internet governance driven by developed countries to carry developing countries along on all levels of its activities.

Therefore, in order to improve the participation of developing countries, the levels of awareness in developing countries of the activities of these entities and the need for participation should be increased.[1559] Access to information, improved financial resources, with technical, regulatory and policy capacity must be raised.[1560] These will encourage the participation of developing countries because the absence of these fundamental factors contributes to the lacklustre approach of developing countries in participating in the activities of the various internet governance agencies.

Greater use of and reliance on capacity outside of government, the strengthening of regional interests and leverage on the regional common interest to influence policy or agenda setting, to swing or veto votes and to lobby capacity will improve and rekindle the interest of developing countries in its participation within internet governance agencies.[1561] Other scholars posit that shifting the balance of power through regional

---

1557 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 2 August 2016).

1558 Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/internet_Governance_Report_Souter_May09.pdf (Date of use: 2 August 2016).

1559 Gilwald https://www.wits.ac.za/media/migration/files/SACTOP.pdf (Date of use: 4 July 2016).

1560 Gilwald https://www.wits.ac.za/media/migration/files/SACTOP.pdf (Date of use: 4 July 2016).

1561 Gilwald https://www.wits.ac.za/media/migration/files/SACTOP.pdf (Date of use: 4 July 2016).

co-ordination, caucusing and lobbying, rather than concentrating same at the centre of the internet governance body, would enhance the participation of developing countries.[1562] This is because countries participate more freely and effectively within its regional blocs. On the other hand, regional meetings must be more serious, moving from mere discussion groups to serious working groups aimed at delivering highly-rated inputs on policy and standards development to the international internet governance entity.[1563]

The University of the Witwatersrand case study suggested the enhanced use of e-mailing list that will keep recipients abreast with current discourse on internet governance issues, which will be used as a channel to send out briefing papers on the areas to be discussed at each upcoming event some months prior to the event.[1564] All cadres of stakeholders will be encouraged at various forums to be part of the e-mailing list.[1565] Subscribers to this expanding e-mailing list will have the opportunity of making informed decisions, aligning with similar interest groups and actively participating either directly or indirectly in the decision-making units of the various internet governance groups. More persons will be aware of the issues being considered at these internet governance bodies and will participate in their country's national debate or regional dialogue in order to influence the outcome of the decision at the international internet governance body. Consumer participation in the policy formulation should also be encouraged.[1566]

1562 Gilwald https://www.wits.ac.za/media/migration/files/SACTOP.pdf (Date of use: 4 July 2016).
1563 Gilwald https://www.wits.ac.za/media/migration/files/SACTOP.pdf (Date of use: 4 July 2016).
1564 Gilwald https://www.wits.ac.za/media/migration/files/SACTOP.pdf (Date of use: 4 July 2016).
1565 Gilwald https://www.wits.ac.za/media/migration/files/SACTOP.pdf (Date of use: 4 July 2016).
1566 Gilwald https://www.wits.ac.za/media/migration/files/SACTOP.pdf (Date of use: 4 July 2016).

6.4. THE EMERGENCE OF A UNIFORM REGULATORY INTERNET BODY AS A PANACEA TO ENSURING PARTICIPATION OF DEVELOPING COUNTRIES AND ENSURING COMPLIANCE WITH THE UNIFORM CYBERCRIME LEGISLATION

In previous chapters (chapter 4 section 4.3), this research has advocated the emergence of a uniform cybercrime court with appellate jurisdiction. This research has also posited in chapter 3 section 3.2, that the emergence of uniform and universal cybercrime legislation will lead to a better regulated internet that has the active participation of developing countries. It follows, therefore, that the emergence of a uniform regulatory body under the UN will also augment the efforts of such uniform legislation and cybercrime court while allowing the active participation of developing countries in its decision-making processes, policy and standard-setting processes, the management and administration of the said regulatory body.

This research has pointed out a number of internet governance bodies with their areas of influence and varying mandates such as ICANN, IETF, ITU, IGF and many other bodies. These varying mandates create divergent perspectives on how issues of internet governance will be addressed. For example, IETF has always held its meetings in developed countries, while ICANN most often rotate its meetings to accommodate representatives from developing countries.[1567] These divergent perspectives will invariably create a certain degree of difficulty in harmonising any effort that will effectively address all internet governance issues, especially as it relates to the participation of developing countries. It is therefore submitted that a global supervisory body that will oversee the entire internet governance bodies be evolved to ensure harmony in executing any policy that will enhance the participation of developing countries in combating cybercrime. As advocated earlier, the body should be global, multi-sectoral, allowing a wide variety of participants and democratic. The various suggestions on how to increase the participation of developing countries (such as

[1567] https://www.ietf.org/meeting/past.html (Date of use: 3 August 2016). See also https://meetings.icann.org/en/calendar (Date of use: 3 August 2016).

capacity building, raising policy awareness, and so forth) already proffered will be better coordinated when there is an international body overseeing all the various internet governance agencies. It is normal that where there is no overseeing body, whatever solutions proffered will be handled differently by the various internet governance agencies. For example, some internet governance agencies may prioritise the release of funds to developing countries while another body will make education and policy awareness its top priority.

It is further submitted that this supervisory body be made a subsidiary of the United Nations. In previous chapters where this research suggested the emergence of a uniform cybercrime legislation and cybercrime court, the research submitted that the UN, being the umbrella body to which almost all nations of the earth subscribe, any internet-related issue that stems from a uniformed system should be rooted in and controlled by the UN. The emergence of this supervisory body and the continuous existence of the already-existing internet governance body is imperative because the already existing internet governance has its area of expertise and has over the years made its gains. Scrapping these bodies for just one internet governance body will therefore not be desirable. Thus, creating a body with oversight functions over the various internet governance bodies to ensure some uniformity is desirable. The reliance on the UN becomes more attractive since the internet is ubiquitous and most states, through their government representatives, should participate in internet policy formulation. A supervisory body should not be the major reserve of any national government (such as in ICANN), but should stem from an international body that has all states as its members.

Al-Darrab, suggesting the emergence of a body with oversight functions over other internet governance bodies, posited that since states take part in internet policy setting, having such a body will create some level of confidence amongst states to place more

reliance on the internet and invest in same.[1568] On the other hand, the ubiquitous nature of the internet makes it unfair that a nation alone should oversee certain aspects of the internet. This is because oversight functions are traditionally performed by national governments or intergovernmental agencies.[1569] The overseeing of certain internet governance bodies by a state, as in the case of ICANN being overseen by the United States (via the US Department of Commerce), creates some apathy since the extent of input of other national governments is limited making global legitimacy far-fetched.[1570] As Al-Darrab succinctly put it, "[p]olicy authority for internet-related public policy issues is the sovereign right of states".[1571] Global oversight through an international intergovernmental body will properly address various public policy issues that affect the internet, capacity building in developing countries and coordinate the existing internet governance bodies in their technical and operational functions while establishing global legitimacy and acceptance.[1572] Al-Darrab further posited that there are a number of international public policy issues that are outside the purview of existing internet governance bodies that are not adequately addressed which can only be addressed effectively when there is a global oversight body.[1573]

6.4.1. ESTABLISING THE UNIFORM REGULATORY INTERNET BODY

It is submitted that the uniform regulatory internet body or congress be made a subsidiary of the UN saddled with the responsibility of overseeing the existing internet bodies and ensuring that internet policies are in line with the proposed uniform cybercrime legislation. The congress, being an offshoot of the UN, will have all member states of the UN represented therein. It must be pointed out that the Panos study showed that the clamour for the reliance on intergovernmental bodies in championing

1568 Al-Darrab AA "The need for international internet governance oversight" in Drake WJ (ed) *Reforming internet governance: Perspectives from the working group on internet governance* (United Nations ICT Task Force New York 2005) 175-184.
1569 Al-Darrab *Internet governance oversight* 175-184.
1570 Al-Darrab *Internet governance oversight* 175-184.
1571 Al-Darrab *Internet governance oversight* 175-184.
1572 Al-Darrab *Internet governance oversight* 175-184.
1573 Al-Darrab *Internet governance oversight* 175-184.

internet governance is loudest among developing countries.[1574] For example, India on various occasions has reiterated its preference for a UN-based organisation with a multi-stakeholder stance, to perform the functions of ICANN in relation to internet governance.[1575] This stance was supported by most developing countries and even Russia and China, but opposed by the US, the EU and most developed countries.[1576] This is partially born out of the inability of developing countries to obtain adequate representation within technical and standard-setting internet governance bodies, which is exacerbated by a lack of capacity in developing countries. It therefore is imperative that a UN-driven internet governance mandate is in line with the need to protect developing countries since any form of internet governance structure that will oversee the existing structures (which is mostly technical in nature and which is beyond the capacity of most developing countries) will defeat the purpose of encouraging the participation of developing countries in internet governance.

It is submitted that like other UN bodies, the highest decision-making body will be its general assembly which will be above the hierarchy of the congress.[1577] This general assembly will be saddled with the responsibility of deciding and approving the body's policy thrust, approving its programmes and appointing and approving an executive board. The meeting of the general assembly can take place after every two or three years.

It is further submitted that the suggested executive board will have the powers to give effect to the policy thrust of the general assembly under an efficient structure. This executive board will have the head of the Secretariat as its head and will have representatives of the various regions as its members to ensure the participation of both

---

1574 Maclean *et al* http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 23 July 2016).

1575 Subramanian R "Internet governance: A developing country perspective" (2013) *Communications of the International Information Management Association* 9-10.

1576 Subramanian *Internet governance* 2013 *Communications of the IIMA* 9-10.

1577 For example, UNESCO has its General Conference as its supreme decision making body while the ITU has the Plenipotentiary Conference as its highest decision-making arm. See http://www.mext.go.jp/english/unesco/1304525.htm (Date of use: 14 August 2016). See also Bekkers R *Mobile telecommunications standards: GSM, UMTS, TETRA, and ERMES* (Artech Publications 2001) 125-136.

developed and developing countries in its decision-making process. Each region or continent will produce at least five representatives, with the understanding that both developed countries and developing countries have their representatives from each region that will be members of the executive board. This executive committee will meet more frequently to access the implementation of policies, to make further recommendations to the general assembly and to ensure the smooth operation of the Secretariat. It is submitted that in order to ensure speedy delivery of its mission, the executive board should be saddled with more responsibilities while the general assembly merely steers policy directions. The Secretariat will be run by the head of the executive board for a tenure or tenures with staff in line with the rules and expediency in carrying out the responsibilities of this uniform regulatory internet body. The Secretariat can appoint as members of its staff liaison directors that will liaise with a designated internet governance body. Each liaison director will ensure that policies evolved within the uniform regulatory internet body (as it relates to the expertise of the body) are adopted within the internet governance agency in which it acts.

The essence of this uniform regulatory internet body is to ensure uniformity in giving vent to the already-proposed uniform cybercrime legislation, to ensure the participation of developing countries and to ensure unity of purpose within the diverse internet governance body in guaranteeing that the menace of cybercrime is brought to its barest minimum.

It is also submitted that every policy created by the various internet governance bodies will be made to receive the approval of this uniform regulatory body. In order to ensure that obtaining the approval of the uniform regulatory body does not create bottlenecks and hamper the work of the existing internet governance body, the representatives of the uniform regulatory body may be saddled with the responsibility of approving such policies. They will in turn report to the executive board and general congress on the approval which will be ratified by a simple majority but can be nullified by a two-thirds majority. This will give the representatives more time to function faster and assiduously.

The structure of this body must be organised in such a way as to ensure the participation of developing countries. Thus, it is submitted that the membership of the executive board and the general assembly should not be restricted to government representatives. Rather, civil societies, the private sector and other stakeholders must have their representatives from each region. This is necessary because the apathy exuded by most developing countries is further fuelled by the reluctance of its national governments who most often are bereft of the requisite capacity to participate in internet policy-making bodies.

It is submitted that the global uniform internet regulatory body should create obligations on states which will ensure that regulations by the internet governance bodies that it oversees are implemented by states. This will create some cohesion and harmony in technical standards and norms amongst nations. This is imperative because most of the existing internet governance structure does not create obligations on states to adhere to its recommendations or ratify same. For instance, the ITU technical recommendations are not subject to national ratification and do not create obligations either under the national or international laws.[1578] The use of treaties may be relied upon to ensure participation and harmonisation.

The emergence of this global uniform internet regulatory body will ensure the participation of developing countries within its structure and promote same within all the various internet governance forums.

It is important to note that the governing laws of each internet governance agency must be amended to accommodate the oversight functions of this uniform regulatory internet governance body.

1578 http://www.itu.int/itunews/manager/display.asp?lang=en&year=2005&issue=05&ipage=internet&ext=html (Date of use: 13 November 2016).

CONCLUSION

This chapter posits that the internet has several internet governance bodies that regulate it. The chapter examined a number of internet governance bodies with a view to establishing the level of participation of developing countries. The chapter also points out that developing countries rarely participate at these various points of internet control like their counterparts from developed countries. Unfortunately, the level of participation within these internet control points also determines the general level of participation in addressing cybercrime. The chapter tried to establish some of the factors that drive the apathy of developing countries in participating in the various internet governance agencies. The chapter then proffered several solutions and ideas that will assist in drawing developing countries from the factors that repel them from taking part in the various internet governance bodies.

The chapter has also gone further to posit that the emergence of a uniform internet regulatory body which will oversee the existing internet governance bodies will help increase the participation of developing countries with the internet governance bodies and their participation in fighting cybercrime.

It is imperative that existing internet governance agencies, civil societies, nations, regional internet governance bodies and the United Nations come together to make the necessary amendments, legislations/treaties and structural changes in creating the emergence of a uniform internet regulatory body with oversight functions over existing internet governance bodies.

These necessary changes will involve the use of the five steps, as enumerated in chapter 3 section 3.4. of this research, namely, identifying the key players; identifying the various sub-players; establishing effective networking; developing a feasible timeframe; and deliberation and reconciliation at the United Nations level, to achieve these changes.

Chapter 7 of this research will focus on strengthening international cooperation in order to ensure the participation of both developed and developing countries in effectively tackling online crime. The chapter will examine the various factors that impede international cooperation and will then proffer some solutions that will strengthen international cooperation.

CHAPTER 7

STRENGTHENING INTERNATIONAL COOPERATION: A TRANSNATIONAL PANACEA TO FIGHTING CYBERCRIME

INTRODUCTION

The ubiquitous nature of the internet makes it imperative that any effective effort to address cybercrime will cut across various nations, continents and climes. The preceding chapters in this research have shown that various nations especially developed nations have taken impressive steps in addressing cybercrime. Most countries have amongst other efforts updated their laws, taken steps to prevent the occurrence of a number of cybercrime activities, advanced their technology to tackle e-crime, and increased the capacity of their law enforcement agencies and judicial officers. Yet, the efforts of other countries (especially developing countries) are still abysmal.

Enhanced international cooperation holds the key to a seamless coordination of the lofty ideas and efforts that will combat cybercrime cutting across nations of the world, developed or developing alike. For example, the police will be unable to arrest perpetrators who reside in countries that purposely provide safe havens for cyber-criminals. Again, countries that loathe international cooperation and lack the requisite capacity to tackle e-crime will be a safe haven for cyber-criminals. The proposals (suggested in the preceding chapters of this research) for an international criminal court for cyberspace (ICCC), harmonised legislation and online uniform global law enforcement agency will never come to fruition when efforts to tackle cybercrime remain fragmented alongside national and regional lines. Even when the international criminal

court for cyberspace, harmonised cybercrime legislation and online uniform global law enforcement agency come into being, their activities cannot be coordinated without efficient international cooperation amongst all stakeholders.

This chapter will attempt to unveil a number of factors that hamper international cooperation and therefore highlight the disadvantage of this disunity in effectively fighting cybercrime. The chapter will also attempt to highlight a number of steps that can be adopted by nations in order to strengthen international cooperation which will invariably lead to an effective curbing of the menace of cybercrime.

7.1. THE NEED FOR INTERNATIONAL COOPERATION IN CURBING CYBERCRIME

In combating any criminal offence, a number of factors determine the success of such a venture. Like other criminal activities, detecting and punishing cybercrime will entail having the requisite laws that criminalise such activity, detecting the source of the criminal activity, detecting the individuals behind the activity and their location, prevention (public-private partnerships and awareness creation) and finally setting the law in motion against them.

Attaining the requisite laws that criminalise cyber activities will entail the following:

(a) harmonising national legislative responses to show some uniformity in cybercrime legislation among national and regional jurisdictions.[1579] This is necessary because similar national legislative responses will make addressing cyber-criminal activities easier considering the ubiquitous nature of the internet. In other words, a nation that is in line with the principles on dual criminality[1580] will not be obligated to assist another nation to investigate a cyber-criminal activity

1579 This was addressed extensively in secs 3.2. and 3.4. of ch 3 of this research.

1580 *Dual criminality* requires that an accused be extradited only if the alleged criminal conduct is considered criminal under the laws of both the surrendering and requesting nations. See Doyle C *Extradition to and from the United States* (Nova Science Publishers New York 2008) 7.

emanating from its jurisdiction when the activity is not criminalised in both countries. Any country with outdated cybercrime legislative responses will affect the efforts of other countries.

(b) creating national legislative responses with common taxonomies.[1581] This is necessary because, as shown earlier in chapter three of this research, having a consistent cybercrime taxonomy will ensure adequate crime reporting, collaborative synergy among agencies, knowledge sharing and clear measurement on the impact of cybercrime across jurisdictions in order to take appropriate steps to tackle same. It will also enhance consistent interpretation and consistent best practices among law enforcement agencies irrespective of jurisdictional boundaries or constraints since the consistent classification will highlight the similar characteristics of cybercrime.

(c) evolving harmonised international cybercrime legislation.[1582] Harmonised international cybercrime legislation will address inconsistencies in the criminalisation of offensive conducts, eliminate the emergence of safe havens, and eradicate the gaps in divergent national legislations which criminals exploit to perpetrate their nefarious activities. According to Bande,[1583] uniformity in legislative framework enhances the cooperation of varying jurisdictions in tackling crime, since the principles of reciprocity[1584] and double criminality[1585] are the main pivots driving international cooperation in criminal jurisprudence and extradition of offenders.[1586]

1581 This point was addressed extensively in ch 3 of this research.

1582 This point was also addressed extensively in ch 3 of this research.

1583 Bande LC "The making of cybercrime legislation in Malawi: A comparative analysis of Malawi's proposed cybercrime law against international standards and best practices" https://lirias.kuleuven.be/bitstream/123456789/404618/1/The+Making+of+Cybercrime+Legislation+in+Malawi+Pdf.pdf (Date of use: 12 September 2013).

1584 Ambos K "The International Court and the traditional principles of International cooperation in criminal matters" in Takamaa K and Koskenniemi M (eds) *The Finnish yearbook of international law 1998* (Kluwer Law International 2000) 413-425.

1585 Ambos *Traditional principles* 413-425.

1586 Rezek JF "Reciprocity as a basis of extradition" 1982 *British Yearbook of International Law* 171-203. See also Bande

Detecting the source of the cyber-criminal activity and setting the law in motion against the perpetrator, will amongst other factors, entail the following:

i. technological capacity. This is because cybercrime perpetrated through the internet requires a high level of technological skills for the investigators/law enforcement agencies, prosecutors and the judicial officers who try the offenders. E-crime belongs to the genre of activity that cannot be properly investigated, prosecuted or adjudicated with prevailing traditional means.

ii. human capacity building. The capacity of individuals investigating, prosecuting or adjudicating cybercrime must always be upgraded. This genre of human activity evolves faster than the law. For example, a judicial officer without the requisite information technology knowledge will find the prosecution and intricate IT evidence strange and incomprehensible. Law enforcement agencies require skilled investigators with detective and technical skills (IT software, hardware and forensic tools), prosecutors and adjudicators with the requisite knowledge of cybercrime. As demonstrated earlier in chapter 2 of this research, most developed countries, invest so much in both human and technological resources in order to equip its law enforcement agencies with the requisite capacity to detect, prevent, successfully prosecute and adjudicate over cybercrime. On the other hand, most developing countries lack the human and technological capacity and funding to efficiently investigate and prosecute cybercrime.

A country without the capacity to investigate, prosecute or adjudicate on cybercrime will affect the efforts of nations with the capacity because a sovereign nation with capacity cannot invade another sovereign nation seeking to apprehend or prosecute the perpetrator of a cybercriminal activity within the borders of another nation without the capacity. This leads to safe havens and invariably aids cyber-criminals to go

---

https://lirias.kuleuven.be/bitstream/123456789/404618/1/The+Making+of+Cybercrime+Legislation+in+Malawi+Pdf.pdf (Date of use: 13 September 2013).

unpunished or unapprehended. The principles of sovereignty of nations and the need to protect a country's nationals from foreign aggression will make it difficult to allow a country to conduct its investigation in another country even where the second country seems incapable of detecting online criminal activities within its borders.

Countries rely on a number of traditional methods (with its limitations) such as mutual legal assistance treaties (MLAT), extradition, letters rogatory, and voluntary cooperation between governments and their law enforcement agencies; in investigating and apprehending perpetrators outside their borders.[1587] These traditional methods of cross-border investigations will be greatly hampered where capacity is lacking. For example, extradition requires a judge from the requested country to authorise the request of the requesting country to extradite an individual. For a judge to grant the request for extradition, he must be convinced that a *prima facie* case has been established against the individual sought to be extradited.[1588] Where a judge lacks the capacity to understand the request being made, it will be difficult for that judge to make an order assisting the requesting country.

Cybercrime prevention through public-private partnerships and awareness creation entails the following:

(a) massive funding. The prevention of cybercrime through the creation of awareness requires the involvement of various public and private enterprises. These bodies will embark on the creation of awareness and capacity building in countries that lag behind in respect of information technology. Unfortunately most developing countries are still weighed down by the provision of the basic necessities of life to make the creation of awareness in relation to cybercrime its top priority.

1587 These traditional methods, their current uses and limitations were analysed in ch 4 of this research.

1588 Nicholls C *et al Nicholls, Montgomery, and Knowles on the law of extradition and mutual assistance* (Oxford University Press Oxford 2013) 112.

(b) technological advancement that will help prevent massive incidents of cybercriminal activities within each jurisdictional precinct.

It is submitted that since cybercrime is a ubiquitous phenomenon, whatever posture or method employed in tackling the menace must involve concerted international cooperation cutting across various nations and regions regardless of the socio-economic situation of each country. Developed countries cannot afford to concentrate its efforts within its national or regional boundaries while disregarding developing countries that are still grappling with a heavy socio-economic burden. Thus, efforts in harmonising legislative responses, capacity building, and creation of awareness all require international cooperation. For example, in chapter 2 of this research, it was shown that the technological advancements deployed by developed countries in investigating, prosecuting and adjudicating on cybercrime is quite remarkable. A judge without adequate IT knowledge will find it difficult to properly appreciate an extradition process to a developed country, neither will a police officer bereft of a basic understanding of cybercrime properly assist an investigation from another country. Also, developing countries cannot be left to solely fund their own part of the bargain when they are still beleaguered by such large financial burdens in the provision of their national basic amenities.

In addition, the various proposals made in the preceding chapters of this research in relation to the emergence of a uniform cybercrime legislation,[1589] the International Criminal Court for Cyberspace (ICCC),[1590] and the online uniform global law enforcement agency[1591] cannot be achieved without concerted international cooperation. The emergence of harmonised legislation, the International Criminal Court and uniform police, as highlighted earlier, will make addressing cybercrime easier than the existing methods of addressing cybercrime such as extradition and the like.

1589 This was extensively dealt with in secs 3.2. and 3.4. of ch 3 of this research.
1590 This was extensively dealt with in sec 4.3. of ch 4 of this research.
1591 This was also extensively dealt with in sec. 4.2. of ch 4 of this research.

However, whether the existing state of affairs in respect of addressing the menace of cybercrime is allowed to continue, or whether the world starts to take steps to prepare for uniformity, or whether the world eventually attains uniformity, international cooperation must be a unifying force as various nations of the world are involved in the various stages of such evolutionary trends.

7.2. FACTORS THAT HAMPER INTERNATIONAL COOPERATION

Prior to the overwhelming desire by nations to cooperate, the guiding principle for nations has been espoused in the Westphalian model of international law. This model is to the effect that the world consists of sovereign states without a supreme authority; states settle their differences privately and by force, if necessary; there is minimal cooperation between states although they engage in diplomatic relations, pursue their own national interests over those of others; and barriers to state freedom must be minimised.[1592] These principles have driven a wedge between nations in the desire to cooperate.

However, cooperation between nations has accelerated over time and the increased cross-border interactions propelled by the emergence of information technology make international cooperation inevitable.

Harmonising national and regional efforts to combat a trans-national crime will entail concerted efforts by the various stakeholders/players to evolve the adequate cooperation that will see the efforts come to fruition. Unfortunately, states do not always

---

1592 Held D, McGrew A, Goldblatt D and Perraton J *Global transformations: Politics, economics and culture* (Stanford University Press Stanford 1999) 32-85. The Westphalian model stipulates that "[t]he world consists of, and is divided by, sovereign states which recognize no superior authority … The process of law-making, the settlement of disputes and law enforcement are largely in the hands of individual states. International law is oriented towards the establishment of minimal rules of coexistence; the creation of enduring relationships among states and people is an aim, but only to the extent that it allows national objectives to be met. Responsibility for cross-border wrongful acts is a "private matter" concerning only those affected. All states are equal before the law; legal rules do not take account of asymmetries of power. Differences among states are often settled by force; the principle of effective power holds sway. Virtually no fetters exist to curb the resort to force; international legal standards offer minimal protection. The maximization of impediments to state freedom is the collective priority." See Held *et al Global transformations* 37-38.

cooperate, even where they have common interests.[1593] Although interdependence has increased among nations, cooperation still eludes them.[1594]

However, several factors hamper international cooperation and invariably deflate the efforts of countries to address trans-national crime. Some of these factors include:

a. Enmity, rivalry and divergences between countries[1595]

The concept of sovereignty entails that countries are in control in relation to their domestic matters and this also drives them to advance their interests above those of other nations. This mainly leads to the assertion of superiority above other countries. In asserting this superiority, countries sometimes oppose the views of their perceived rivals even when those views are helpful. For example, Maness *et al* summarised the rivalry between the United States of America and Russia as follows: "It seems that where the United States is involved Russia is there to oppose and *vice versa"*.[1596] Rivalry behaviour stalls international cooperation and hampers meaningful harmonisation of policies.

On the other hand, divergence in opinion and disagreements also affect international cooperation. For example, countries have divergent views on content-related matters in relation to cybercrime. Countries therefore tend to address the attendant problem according to their distinct policies and cultural proclivities. China, for instance, censors politically-sensitive information within its jurisdiction,[1597] while religion is a top priority for countries such as Saudi Arabia.[1598] Singapore, for its part, restricts access to

---

1593 Sterling-Folker J "Neoliberalism" in Dunne T, Kurki M & Smith S (eds*) International relations theories: Discipline* (Oxford University Press Oxford 2010) 114-131.

1594 Sterling-Folker *Neoliberalism* 114-131.

1595 Balzer AJ "International police cooperation: Opportunities and obstacles" in Pagon M (ed) *Policing in Central and Eastern Europe: Comparing firsthand knowledge with experience from the West* (College of Police and Security Studies Ljubljana 1996) 63-74.

1596 Maness RC and Valeriano B (eds) *Russia's coercive diplomacy: Energy, cyber, and maritime policy* (Palgrave Macmillan Publication Hempshire 2015) 45-84.

1597 Drucker S, Gumpert G and Cohen HM "Social media" in Drucker SJ and Gumpert G (eds) *Regulating convergence* (Peter Lang Publishing New York 2010) 80-81.

1598 Saudi Arabia blocks sites offensive to Islam and the government, such as pornographic and gambling sites. Duquenoy P, Jones S and Blundell BG (eds) *Ethical, legal and professional issues in computing* (Middlesex University Press London 2008) 79-95.

pornography,[1599] while in countries such as the United States, freedom of expression is a fundamental human right and access to all types of information is germane.[1600] From the regulatory angle, countries such as China puts the responsibility of ensuring that illegal content is not hosted on internet service providers.[1601] These national policies determine the posture of the varying national governments, shaping their alignment on issues that require international cooperation.

These disagreements also propel countries to take steps to protect their national interests above those of the international community and create serious difficulties in the harmonisation of any international effort in addressing trans-national crime.

In addition to the enmity, rivalry and divergences, efforts towards continued cooperation may be undermined by defections[1602] of stakeholders at any stage of the journey in addressing cybercrime.

b. Difficulty in persuading policymakers and their constituencies that change with all its uncertainties, inconveniencies is essential rather than continuing with the status quo[1603]

The ability of any nation to tilt towards cooperating with other countries involves the input of various policy makers in that country. These policy makers range from technocrats to career civil servants to core politicians in the legislative and executive arms of a country. The technocrats who may have in-depth knowledge of the trans-national problem would normally opt to join other nations in addressing cybercrime. However, since national policies must be backed by laws enacted by the legislative arm of that country and signed into law by the executive arm, the consent of politicians in the legislature and executive arm must be sought for and obtained. For example, international laws, among other things, stipulate the minimum standards expected to be

1599 Duquenoy *et al.* (eds) *issues in computing* 79-95.
1600 Oster J *Media freedom as a fundamental right* (Cambridge University Press Cambridge 2015) 230.
1601 Deibert R *et al* (eds) *Access denied: The practice and policy of global internet filtering* (MIT Press 2008) 263-271.
1602 Sterling-Folker *Neoliberalism* 114-131.
1603 Balzer *International police cooperation* 63-74.

adopted and these treaties have to be domesticated by each signatory to the treaty for it to be effective and binding.[1604] Persuading politicians regarding the need for change may be daunting. On the other hand, politicians have various constituencies that they represent. These constituencies have more pressing issues that need to be addressed. To them, certain government policies may have no direct impact on their lives and, therefore, are not of utmost importance to them. As is the case in most developing countries, the provision of basic amenities may be of the highest concern to the constituents and policies that engender international cooperation in relation to cybercrime appear alien to these constituents. Therefore, convincing these constituents regarding the need for change becomes equally daunting. When these policy makers become apathetic to any move for improved international cooperation, efforts to get that country involved will not make meaningful progress.

c. Difficulty in harmonising law enforcement techniques and varying legal systems[1605]

Varying legal systems and law enforcement techniques also hamper international cooperation. For instance, some nations operate according to the inquisitorial legal system while others apply the accusatorial system. The aforementioned legal systems, being divergent in nature, affect the cooperation of nations in fashioning a common legal system that will address cybercrime.[1606] These varying legal systems determine what the acceptable idea of state justice is. Thus, while the United States emphasises individual rights, the civil law legal system prevalent in Europe emphasises the interests of the community/state.[1607] These varying legal systems and their peculiarities stem

1604 Gibson JS *International organizations, constitutional law and human rights* (Praeger Publishers 1991) 114.

1605 Balzer *International police cooperation* 63-74.

1606 Under the inquisitorial legal system, the judge/adjudicator supervises the evidence gathering in the particular case and questions the witnesses, whereas the accusatorial system pits the parties together before an independent judge/arbiter who weighs the evidences adduced and makes a pronouncement. Wilson SH (ed) *The US justice system: Law and constitution in early America* (ABC-CLIO Publishers California 2012) 399.

1607 Balzer *International police cooperation* 63-74.

from each country's historical backgrounds and customs.[1608] Merging these divergent systems in order to attain cooperation among nations will be daunting.

d. Circumstances where the cost or associated risks of international cooperation outweigh the gains, international cooperation becomes undesirable[1609]

Where the risk of international cooperation outweighs the gains the state will enjoy, nations refrain from international cooperation. For example, the exit of Britain from the EU (Brexit) was triggered by a feeling among the average Briton that the gains of continued membership of the EU are not commensurate to the risks attached.[1610] Those who voted in favour of the Brexit believe that the EU imposed too many rules on Britain, made Britain lose control of its borders and held Britain back in many ways.[1611]

On the other hand, where the gains to be enjoyed by different state stakeholders are disproportionate, international cooperation can be held back. For example, in addressing cybercrime, developed countries seem to be the target of major attacks and the efforts to address cybercrime seem to be in the interest of developed countries, this can make developing countries grow cold in their efforts to combat cybercrime since they are not the main beneficiaries of such international efforts. Again for example, as in the case of the Nigerian advance fee fraud (popularly called 419), the foreign exchange realised by the perpetrators contribute to the economy of the nation, which may further dampen the enthusiasm in addressing the crime.

e. Where nations suspect the intention of other state stakeholders, international cooperation can also be hampered[1612]

1608 Zartner D *Courts, codes, and custom: Legal tradition and state policy toward international human rights and environmental law* (Oxford University Press Oxford 2014) 16-46.

1609 Hasenclever A, Mayer P and Rittberger V *Theories of international regimes* (Cambridge University Press Cambridge 1997) 84-135. See also Balzer *International police cooperation* 66-68.

1610 Hearn J "*Voxpopuli*: Nationalism, globalization and the balance of power in the making of Brexit" in Outhwaite W (ed) *Brexit: Sociological responses* (Anthem Press London 2017) 19-30.

1611 Hearn *Vox populi* 19-30.

1612 Sterling-Folker *Neoliberalism* 114-131.

Distrust and an unnecessary feeling of competition among nations limits international cooperation.[1613] The concern by developed nations that others will ride on their backs to fulfil their selfish goals without ensuring that the collective goal of the international arrangement is always addressed will affect the desire for international cooperation.[1614]

f. Where nations, especially developed countries, perceive that other nations will take advantage and cheat on the international cooperative arrangement, the desire for international cooperation may wither out[1615]

g. Another factor that hampers international cooperation is that, harmonisation efforts and the existing international platforms seem to be the exclusive forum for developed countries[1616]

Unfortunately, nations with larger populations have increased internet penetration and invariably tend to have more incidents of cybercrime emanating from there.[1617] The fact that developing countries and other states feel left out of this exclusive forum will hamper effective international cooperation.

7.3. STRENGTHENING INTERNATIONAL COOPERATION

It has been established that addressing cybercrime requires international cooperation. This research has identified some of the factors that militate against an effective international cooperation that can lead to the harmonisation of efforts to curb cybercrime. It must, however, be pointed out that international efforts come with limitations. For example, international bodies do not have the power to enforce their laws/treaties, since these can only be enforced as a municipal law of a nation once

1613 Lengfelder C "International cooperation as a stepping-stone to a world government" http://www.globalpolicyjournal.com/brookings-audit/international-cooperation-stepping-stone-world-government (Date of use: 19 April 2017).
1614 Sterling-Folker *Neoliberaiism* 114-131.
1615 Sterling-Folker *Neoliberaiism* 114-131.
1616 Li X "International actions against cybercrime: Networking legal systems in the networked crime scene" http://www.webology.org/2007/v4n3/a45.html (Date of use: 30 April 2017).
1617 Li http://www.webology.org/2007/v4n3/a45.html (Date of use: 30 April 2017).

domesticated.[1618] Signatories can pull out of the treaty when it seems not to favour them. Also, smaller, less powerful countries exert little influence on decision making within these international bodies.[1619] Again, these international bodies have limited resources to fund their operations and are constrained to rely on the contributions of nations, especially the powerful stake-holder nations.[1620] Thus, where international cooperation is attained, these limitations, which come in varying degrees, still put international cooperation at a disadvantage.

It is submitted that in order to create an apposite international cooperation (which will span from the initial quest to come together to fight a common cause and when the entire harmonised system has been put into place) that will effectively address cybercrime, a number of factors and steps need to be embarked upon by various international stakeholders. These steps will be examined below.

7.3.1. DEVELOPING AND SUSTAINING INTERNATIONAL COOPERATIVE RELATIONSHIPS

Countries easily cooperate where some form of cooperative relationship already exists. This relationship has to be initiated early when stakeholders find the need for harmonisation and must be sustained to ensure that the lofty ideals of the stakeholders will be continued. That is why it is easier for countries to cooperate along regional lines because of their common interests and cooperative relationships. Nadelman[1621] proposes three steps that will ensure the evolution of some cooperative relationships. He posited that to foster cooperative relationships there must be:

1618 *JH Rayner v Department of Trade* (1989) 3 WLR (HL) 980-985. See also Amerasinghe CF *Principles of the institutional law of international organizations* (Cambridge University Press Cambridge 2005) 408-410.

1619 Souter D "Louder voices and the international debate on developing country participation in ICT decision making" in Drake WJ and Wilson EJ *Governing global electronic networks: International perspectives on policy and power* (MIT Press Massachusetts 2008) 429-462.

1620 Wickremasinghe C *The jurisdictional immunities of international organisations and their officials* (PhD thesis, London School of Economics 2003) 7-8.

1621 Nadelmann EA *Cops across borders: The internationalization of US criminal law enforcement* (Pennsylvania State University Press Pennsylvania 1997) 313-394. See also Song Richardson L "Convicting the innocent in transnational criminal cases: A comparative institutional analysis approach to the problem" 2008 *Berkeley Journal of International Law* 79-82.

a. **Regularisation of relations**

The various national stakeholders must come to a consensus on the need to harmonise their relationship in order to address their common foes.[1622] A common umbrella institution (such as the ITU) may emerge to provide the foundation and meeting point for the formulation, implementation and review of the various ideas in addressing cybercrime.

b. **Accommodation of varying systems**

Every country has its legal and socio-political system that determines its policies, law formulation and enforcement methods.[1623] These varying systems must be galvanised, fused together and accommodated by the varying national and regional stakeholders in order to build consensus on the various factors that must be put in place to address cybercrime.

c. **Harmonisation towards a common norm**

Norms and laws regulate every society. Trans-national efforts to regulate society and to stamp out trans-national crime must be harmonised to formulate a common norm that is acceptable to the international community.[1624]

These processes entail lots of compromises, adjustments, trials and errors.[1625] At the earliest stages, national interests will collide; stakeholders will get to know and study the other national or regional systems and evolve hybrid policies and procedure that will lead to some consensus.

On the other hand, in harmonising and developing international relations among the varying stakeholders, steps must be taken to harmonise the individuals and entities who formulate the various national policies that can be harmonised. For example, in

1622 Nadelmann *Cops across borders* 313-394.
1623 Nadelmann *Cops across borders* 313-394.
1624 Nadelmann *Cops across borders* 313-394.
1625 Nadelmann *Cops across borders* 313-394. See also Song *Convicting the innocent Berkeley Journal IL* 80.

the preceding aspects of this chapter, it was pointed out that the difficulty in persuading policy makers, politicians and their constituencies hamper international cooperation. Thus, the interests of the national or regional policymakers must be aligned with the intention of the progenitors asking for positive change in the efforts at addressing cybercrime. Thus, it must be ensured that:

- the various stakeholders share the same perception or similar perception in relation to the governing legislation, law enforcement strategy, crime prevention and adjudication.[1626] Sharing similar perceptions will be achieved by constant education and awareness from the progenitors (developed countries) of the various steps that will address cybercrime to the other stakeholders (developing countries) until both divides come to the same page on how to address cybercrime.
- experienced career personnel with knowledge on the issues surrounding cybercrime, trans-national crime and international politics are employed both at the international level and the varying national/regional level to help identify the issues and to proffer practical solutions on how these can be addressed.[1627]
- the involvement of politicians and policymakers who formulate, enact and ratify the relevant legislations is be sought after and obtained. Without their consent, international treaties will not be signed and when signed will not be ratified and enacted into national legislation rendering the efforts useless.
- a sustained communication exists between the professionals saddled with the responsibility of formulating the policies and the politicians who will implement the policies under the law.[1628] These channels of communication must be deployed from the initial formative stages and should be sustained while the international cooperation on the subject matter of cybercrime continues.

1626 Samans R, Schwab K and Malloch-Brown M (eds) *Everybody's business: Strengthening international cooperation in a more interdependent world* (World Economic Forum Geneva 2010) 19-44.

1627 Balzer *International police cooperation* 63-74.

1628 Balzer *International police cooperation* 63-74.

7.3.2. CREATING THE RIGHT PLATFORM THAT WILL PROVIDE THE FOUNDATION FOR FORMULATION, IMPLEMENTATION AND PROPAGATION OF THE IDEAS POOLED TOGETHER FROM VARYING STAKEHOLDERS IN ADDRESSING CYBERCRIME

The platform or institution[1629] must be set to lead and also provide the right environment for negotiations, which in turn will lead to the right set of rules and regulations. Bargaining by states will be driven by interests and goals beneficial to the states.[1630] Thus, the method of bargaining that will be championed by this institution will vary and be flexible in order to accommodate the collective goals of the varying state stakeholders.

Again, this institution must be set to prevent and alleviate the fear of defections among the varying stakeholders since the institution will be privy to the information and preferences of the stakeholders.[1631]

Furthermore, the institution must be set to effectively ensure compliance with the agreed rules and regulations and other efforts in tackling cybercrime. It should also be designed to help stakeholders comply with the set rules. The compliance by states will be increased when they know that there are processes set up to monitor how they abide by the rules, regulations and efforts to address cybercrime.

1629 Preceding chapters (especially ch 6) of this research has suggested the emergence of a uniform regulatory internet body which will be an off-shoot and part of the United Nations.

1630 Fearon JD "Bargaining, enforcement, and International cooperation" 1998 *International Organisation* 269-305.

1631 Sterling-Folker *Neoliberalism* 114-131.

7.3.3. STRENGTHENING COMMUNICATION AND UNDERSTANDING AMONG COUNTRIES[1632]

Cooperation among stakeholders can only be enhanced by the emergence of effective information channels. These channels will keep the stakeholders informed about the rules and regulations, the extent of compliance among other stakeholders, and keep them abreast with current trends in addressing cybercrime. Basic understanding among varying national stakeholders and the international institution will be fostered through active information channels.

7.3.4. TRANSPARENCY OF THE INTERNATIONAL INSTITUTION AND NATIONAL OR REGIONAL STAKEHOLDERS

Transparency of the international institution and national or regional stakeholders will reduce distrusts and enmity while increasing the drive of developing countries in participating in the efforts to curb cybercrime. When the international institution appears as the exclusive preserve of developed nations and shrouded in mystery and ambiguity, the cooperation of nations who feel left out will be lost.

7.3.5. FINANCIAL INCENTIVES

The release of financial incentives may induce parties to manage their disagreements, enhancing compliance and discouraging defections by stakeholders.[1633]

1632 Jian GU "Strengthening international cooperation and joining hands in fighting against transnational cybercrime" http://www.china.org.cn/business/2010internetforum/2010-11/09/content_21306503.htm (Date of use: 20 May 2017). See also Balzer *International police cooperation* 66-68.

1633 Sterling-Folker *Neoliberalism* 114-131.

7.3.6. CONFLICT RESOLUTION[1634]

Disagreements by stakeholders on various issues in addressing cybercrime present major challenges that will hamper international cooperation. The establishment of an effective conflict resolution, arbitration or mediation scheme holds an important key to ensuring that stakeholder disagreements are resolved and not left to escalate to the point of disintegrating cooperation. This scheme may be included as part of the legislative intervention or treaty driven by the international institution that provides the foundation for interaction between the various national and regional stakeholders.

7.3.7. SLIGHT LOOSENING OF THE PRINCIPLES OF SOVEREIGNTY[1635]

The sovereignty of nations to a certain extent is a clog in the wheel of efficient trans-national crime prevention. This is because where a nation addresses a trans-national crime in the way it deems fit, another nation affected by the nefarious activities emanating from the first nation will not have the freedom to use its state machineries to apprehend and deal with the culprits without the active participation of the second nation.

International cooperation entails that countries will have to tolerate some form of intervention or interference with its domestic politics and policies for any international effort to succeed.[1636] For example, the success of the various efforts within the EU lies within its increased unity amongst members who can intervene in each other's affairs for the good of the region.

1634 Sterling-Folker *Neoliberaiism* 114-131.

1635 Lengfelder http://www.globalpolicyjournal.com/brookings-audit/international-cooperation-stepping-stone-world-government (Date of use: 19 April 2017).

1636 Lengfelder http://www.globalpolicyjournal.com/brookings-audit/international-cooperation-stepping-stone-world-government (Date of use: 19 April 2017).

7.3.8. STRENGTHENING THE RULE OF LAW AND PROMOTING DEMOCRATIC GOVERNANCE AMONG STAKEHOLDERS[1637]

International cooperation will be easily achieved where stakeholders respect the rule of law and run democratic institutions. For example, nations that constantly derogate the basic principles of the rule of law will hardly be constrained to abide by an international set of rules and regulations. Democratic institutions promote the growth of such national institutions, enhance their law enforcement and implementation mechanisms and places reliance on the ideas of many rather than the dictates of a few who may be bereft of ideas. Emerging democracies are prone to international crime.[1638] The success of international efforts in addressing cybercrime within a state lies in the ability of the state to earn the confidence of its citizens through effective law enforcement institutions. This is dependent on the development of law enforcement agencies, legislation, prosecutors and adjudicators who operate within the ambits of the rule of law. Dahinden opined that nations must come to an understanding that democracy does not revolve merely around changes of government, but entails building the right institutions, right attitudes, respect for the rule of law, freedom of speech, human rights, impartiality in administration and the creation of an independent judiciary.[1639]

7.3.9. CAPACITY BUILDING AND INSTITUTIONAL STRENGTHENING AMONG NATIONAL STAKEHOLDERS[1640]

The lack of capacity of a nation in addressing the issues surrounding cybercrime will affect the enthusiasm to cooperate with other nations in addressing the problem. For example, where the law enforcement agencies, prosecutors and adjudicators do not have the capacity, they cannot interact with other national agencies or assist those

---

1637 Fondevila G "The rule of law in multilateral institutions and international aid for development: Judicial reform in the global order" in Kumar A and Messner D (eds) *Power shifts and global governance: challenges from south and north* (Anthem Press London 2011) 123-138.

1638 Zakaras M "International computer crimes" (2001) *Revue Internationale de Droit Penal* 813-829.

1639 Dahinden M "Democracy promotion at a local level: Experiences, perspectives and policy of Swiss international cooperation" http://poldev.revues.org/1517#tocfrom2n2 (Date of use: 29 May 2017).

1640 Balzer *International police cooperation* 63-74.

nations where the need arises, thereby stalling international cooperation. Thus, when capacity is increased, it will be easier for the parties to collaborate since their efforts complement the other country's efforts. Decisions will also be reached easily because the stakeholders understand what is at stake and they all make inputs to the issues at hand. No country will be left out which will increase international cooperation.

To shore up the capacity of countries especially developing countries, there must be consistent adequate education and training of all national stakeholders – policy makers, law enforcement agencies, prosecutors, judges, and so forth.[1641] These pieces of training must span from the basic to advanced levels of knowledge, ranging from the collection of electronic evidence, to the handling and presentation of the evidence in court.[1642] The pieces of training must run through all spheres of cybercrime adjudicatory processes (both substantive and procedural law).[1643] Proper sustainability planning that will ensure a long-term transfer of skills from international experts to the local recipients must be established.[1644]

In the long run, the capacity-developing institutions end up influencing developing countries to develop their capacity to contribute to cybercrime prevention, and various internet governance agencies.[1645] It also increases the recipient country's capacity for result-oriented planning to improve the existing quality and efficiency while reducing the focus on individuals.[1646]

1641 Palmer A "A model framework for successful cybersecurity capacity building" (2016) *Journal of Internet Law* 15-19.

1642 Palmer *A model framework* 2016 *Journal IL* 18.

1643 Palmer *A model framework* 2016 *Journal IL* 18.

1644 Palmer *A model framework* 2016 *Journal IL* 17.

1645 Palmer *A model framework* 2016 *Journal IL* 15.

1646 The bane of most developing countries is the building of strong individuals instead of institutions. They thus exert energy focusing on individuals and placing their capacity on these individuals instead of evolving efficient institutions. President Obama of the United States of America once made a call on Africa that Africa needs strong institutions and not strong men. See Bawole JN *et al* (eds) *Development management: Theory and practice* (Routledge New York 2017) 32. See http://www.sida.se/contentassets/21d3b77fac2844fd89779048c8b3cfe7/no-10.-methods-for-capacity-develpoment_2645.pdf (Date of use: 1 August 2017).

Effective cooperation between the skill-transferring bodies and the recipients must be in place.[1647]

It is submitted that capacity building for developing countries in relation to cybercrime and their participation in internet governance requires –

- recognising the need for capacity building and then building on existing capacities.[1648] Capacity building can only thrive when the recipients understand the existence of a vacuum and the need to increase their capacity in line with international best practices. There also must be an assessment of the existing capacities within the national stakeholders. This will provide the capacity providers with the needed springboard for their training and a proper understanding of the areas to concentrate upon.

- reaching consensus on the objectives of the capacity building and using a wide range of capacity-building techniques.[1649] The objectives of the capacity building must be clear to the capacity provider and the recipients. This will enable the parties have a clear focus on the type of capacity being developed. That is to say, whether the capacity being built relates to awareness, analytical or decision-making capacity.[1650] The target of the capacity building must also be identified as targeting individuals or institutions or both.[1651] The current position in most developing countries is that seminars and conferences are arranged where blame is apportioned to the inefficiencies of individuals and institutions and after that nothing is done. In fact, the UN environment programme pointed out that many

1647 Palmer *A model framework* 2016 *Journal IL* 187.
1648 https://www.unpei.org/sites/default/files/PDF/institutioncapacity/Ways-to-increase-effectiveness-SD.pdf (Date of use: 30 July 2017).
1649 https://www.unpei.org/sites/default/files/PDF/institutioncapacity/Ways-to-increase-effectiveness-SD.pdf (Date of use: 30 July 2017).
1650 https://www.unpei.org/sites/default/files/PDF/institutioncapacity/Ways-to-increase-effectiveness-SD.pdf (Date of use: 30 July 2017).
1651 https://www.unpei.org/sites/default/files/PDF/institutioncapacity/Ways-to-increase-effectiveness-SD.pdf (Date of use: 30 July 2017).

activities offered through workshops and seminars only raise awareness while only analytical and decision-making capacities produce the necessary change.[1652] The UN environment programme further pointed out that even though human capacities are essential, institutional capacities are more enduring since institutions endure from age to age and ensure organisational change.[1653] Defined objectives will ensure that the capacity building is tailored to suit the needs of the recipient country.[1654]

Again, varying capacity-building techniques should be adopted depending on the immediate recipients. These will range from education, training, networking, and so forth. Policy dialogues, conferences, discussion workshops and seminars may increase the capacity of civil societies and some policy makers, while intricate technical training and international networking will be suitable for the law enforcement agent. Therefore, the capacity-building technique applied in a recipient country will vary with each group in the country in line with its expected output. The UN environment programme revealed that training that is limited to Powerpoint presentations may end up as an awareness-creating experience that does not transfer skills to its audience.[1655] Thus, an effective capacity-building scheme will not be a one-day programme but will span a reasonably long-term period to allow for interactive workshops, case studies, role-playing, field visits, live experiments and other methods that will allow the proper understanding of the relevant skills sought to be transferred.[1656] For example, the Swedish International Development Cooperation Agency (SIDA) established the concept of “twinning” which mandates an agency in a developed country to

1652 https://www.unpei.org/sites/default/files/PDF/institutioncapacity/Ways-to-increase-effectiveness-SD.pdf (Date of use: 30 July 2017).
1653 https://www.unpei.org/sites/default/files/PDF/institutioncapacity/Ways-to-increase-effectiveness-SD.pdf (Date of use: 30 July 2017).
1654 https://www.unpei.org/sites/default/files/PDF/institutioncapacity/Ways-to-increase-effectiveness-SD.pdf (Date of use: 30 July 2017).
1655 https://www.unpei.org/sites/default/files/PDF/institutioncapacity/Ways-to-increase-effectiveness-SD.pdf (Date of use: 30 July 2017).
1656 https://www.unpei.org/sites/default/files/PDF/institutioncapacity/Ways-to-increase-effectiveness-SD.pdf (Date of use: 30 July 2017).

pair with its sister agency in the recipient country in order to build up the recipient's capacity.[1657] This invariably will entail an exchange of staff, intricate capacity-building training, seminars, workshops, short-term supply and the placement of expertise through consultants, provision and support for equipment.[1658] Thus, the professional competence of all classes of the personnel is stimulated and sustained.

- targeting the right people or institutions.[1659] Most capacity-building expeditions in developing countries are targeted or taken over by the wrong persons or institutions. Individuals in government who exert influence but have no involvement with information technology may take over the training simply because some pecuniary or other benefits are attached. On the other hand, the UN environment programme pointed out that most capacity-building ventures emanating from international organisations mostly targeted key government players that are policy makers.[1660] Unfortunately, most policy makers are not the implementers and this leaves a gap between policy formulation and implementation. Therefore, capacity building must not be restricted to policy makers but must cut across all stakeholders that have a role in implementing IT laws and regulations.

- training trainers and building capacity-building institutions at national and regional levels.[1661] The essence of capacity building is that the recipient nation becomes independent from the international organisation while continuing to increase the capacity of that nation's institutions and individuals. Thus, adopting the training-the-trainer approach will help sustain

1657 http://www.sida.se/contentassets/21d3b77fac2844fd89779048c8b3cfe7/no-10.-methods-for-capacity-develpoment_2645.pdf (Date of use: 1 August 2017).
1658 http://www.sida.se/contentassets/21d3b77fac2844fd89779048c8b3cfe7/no-10.-methods-for-capacity-develpoment_2645.pdf (Date of use: 1 August 2017).
1659 https://www.unpei.org/sites/default/files/PDF/institutioncapacity/Ways-to-increase-effectiveness-SD.pdf (Date of use: 30 July 2017).
1660 https://www.unpei.org/sites/default/files/PDF/institutioncapacity/Ways-to-increase-effectiveness-SD.pdf (Date of use: 30 July 2017).
1661 https://www.unpei.org/sites/default/files/PDF/institutioncapacity/Ways-to-increase-effectiveness-SD.pdf (Date of use: 30 July 2017).

the capacity when the term of the international institution elapses.[1662] The trained trainers then will be equipped to train other untrained and emerging personnel while keeping themselves abreast of further changes in the international sphere.

On the other hand, capacity-building institutions should be established at the national and regional levels.[1663] This will make it easier for the capacity builders to reach their targets. The recipients will no longer be deterred by travel expenses, facilities, financial constraints, etc. The international organisations can also easily monitor and coordinate the activities of these capacity-endowing institutions or persons at the national or regional level. This will ensure that capacity development is brought closer to the recipients, made more regular on a long-term basis and steadily evolving to suit emerging trends in technological development.

It must be pointed out that international cooperation and the fight against cybercrime cannot be effective without a strong political will among the stakeholders at the national and international level.[1664] According to Ghernaouti, the major limitation is not the absence of guidelines or laws since there are always laws that can be relied upon or stretched to address a particular crime.[1665] He pointed out that difficulties in addressing trans-national crime stem from the complexities of the task required, the high volume of resources and funds needed to address the crime.[1666]

The various stakeholders must understand and address cybercrime from a global perspective, promote a culture of cybersecurity and propagate awareness on

1662 https://www.unpei.org/sites/default/files/PDF/institutioncapacity/Ways-to-increase-effectiveness-SD.pdf (Date of use: 30 July 2017).
1663 https://www.unpei.org/sites/default/files/PDF/institutioncapacity/Ways-to-increase-effectiveness-SD.pdf (Date of use: 30 July 2017).
1664 Ghernaouti-Helie S *Cyber power: Crime, conflict and security in cyberspace* (EPFL Press Lausanne 2013) 255-292.
1665 Ghernaouti-Helie *Cyber power* 255-292.
1666 Ghernaouti-Helie *Cyber power* 255-292.

cybercrime within its various borders.[1667] Developed and developing nations alike must strengthen their institutions to tackle political issues, socio-economic issues, law enforcement and legal issues because when a country's institutions cannot ordinarily address these issues cybercrime will be daunting.[1668] For example, most developing countries have weak institutions that only wake up to their responsibilities when the head of state or other political leaders have a reason to request the institution to live up to its responsibility.[1669] In Nigeria, for example, a semblance of the fight against corruption is spearheaded by its Economic and Financial Crime Commission (EFCC) depending on the posture of the head of state, and where the head of state does not emphasise the need for corruption to be addressed, the same agency goes into hibernation.[1670] In fact, the head of state even determines those who will be investigated, thereby building strong men and not strong institutions that will perform their duties irrespective of the persons at the helm of a nation's affairs.[1671]

Bearing in mind that there are a number of limitations that hamper any attempt to properly harmonise international efforts in tackling cybercrime, scholars have identified several steps that the international community must take in order to have an effective international cooperation.

The international system must be redefined to take the form of a more open and multifaceted system of global cooperation which recognises and relies on intergovernmental institutions as a crucial component but not its sole component.[1672] Currently, international cooperation is modelled as an interaction between government-state actors and their institutions, with the international body providing the platform. However, the current state of interconnection among individuals across the globe

1667 Ghernaouti-Helie *Cyber power* 277.
1668 Ghernaouti-Helie *Cyber power* 277.
1669 Oladele B "Weak institutions make corruption thrive" *The Nation Nigeria* 21 February 2016. See also Lewis PM "The dysfunctional state of Nigeria" in Birdsall N, Vaishnav M and Ayres RL (eds) *Short of the goal: US policy and poorly performing states* (Centre for Global Development Washington 2006) 83-116.
1670 Odionikhere P *Bringing down this house* (Lit Verlag Berlin 2008) 102-109.
1671 Odionikhere *Bringing down* 102-109.
1672 Samans, Schwab and Malloch-Brown *Everybody's business* 19-44.

without placing reliance or going through their formal national/government/political institutions calls for a redefinition of the operation of international cooperation. The level of interdependence among states is constantly on the increase and individuals continue to reach out over the borders without relying on existing formal political state structures.[1673] This puts the traditional state law enforcement mechanism, which is driven by the overriding defence of its national interests, at some disadvantage in addressing trans-border challenges.[1674]

Therefore, in order to scale the limitations of the existing state-centric international cooperation and increase cohesion, nations and the international platform must deliberately evolve a system anchored by interactions between interdisciplinary and multi-stakeholder network of relevant experts and stakeholders.[1675] The involvement of states must be de-emphasised, giving more leverage to the individual stakeholders and experts, although with the states still giving the final approval. As Samans *et al* succinctly put it, this mode of international cooperation can be achieved "through a 'we the peoples' rather than 'we the states' approach to international governance and cooperation".[1676]

Flowing from a redefinition of the system, the state-based aspect of the system must be strengthened to become more efficient.[1677] On the other hand, practical steps must be taken to widen the circle of cooperation to allow the active participation of non-state experts and resources.[1678] This can be achieved through capacity building of the various intergovernmental institutions and incorporation of non-governmental expertise and resources in order to strengthen policy formulation and execution.[1679] This will entail expanding intergovernmental norms and legal frameworks to accommodate the incorporation of the non-governmental institutions.[1680]

1673 Samans, Schwab and Malloch-Brown *Everybody's business* 19-44.
1674 Samans, Schwab and Malloch-Brown *Everybody's business* 19-44.
1675 Samans, Schwab and Malloch-Brown *Everybody's business* 19-44.
1676 Samans, Schwab and Malloch-Brown *Everybody's business* 19-44.
1677 Samans, Schwab and Malloch-Brown *Everybody's business* 19-44.
1678 Samans, Schwab and Malloch-Brown *Everybody's business* 19-44.
1679 Samans, Schwab and Malloch-Brown *Everybody's business* 19-44.
1680 Samans, Schwab and Malloch-Brown *Everybody's business* 19-44.

The participation and accountability of the state stakeholders must be strengthened.[1681] This is essential in order to retain the confidence of the non-governmental actors (as suggested above) and the international community in the existing multilateral system. The voting strength must be rebalanced to increase the input of developing nations and other emerging economies, so that decisions will not always tilt towards the dictates of developed states.[1682] This will give the developing countries a sense of belonging and will encourage more participation in the leadership, and give legitimacy to the international platform. Samans *et al* further suggest that the voting structures within the international platform must be updated with a view to citizens and non-state actors being consulted more directly or through representatives.[1683] Samans *et al* also note that "citizens around the world are increasingly educated, interconnected and engaged in global affairs. This trend is generating new demands on institutions of all types to explain and account for their strategies and performance".[1684]

These redefinitions and their attendant restructuring cannot be attained without orchestrating a shift in values within participating societies since globalisation involves shifting the foundations beneath political leaders.[1685] International cooperation can be initiated through laws, institutional arrangements and incentives. However, its efficiency is tied to the culture and values of the participants since people make up these institutions and determine the effectiveness of any political arrangement. Commitments to performance can only be elicited from human beings who make up the structures. "All formal institutions – constitutions, written laws, governmental bodies – rest upon the informal institution of culture".[1686] The current spate of global interdependence entails that international institutions must be updated and adapted to involve all genres of participants who are affected by the institutions' decisions ranging from businessmen to

1681 Samans, Schwab and Malloch-Brown *Everybody's business* 19-44.
1682 Samans, Schwab and Malloch-Brown *Everybody's business* 19-44.
1683 Samans, Schwab and Malloch-Brown *Everybody's business* 19-44.
1684 Samans, Schwab and Malloch-Brown *Everybody's business* 19-44.
1685 Samans, Schwab and Malloch-Brown *Everybody's business* 19-44.
1686 Samans, Schwab and Malloch-Brown *Everybody's business* 19-44.

technicians to local politicians, scientists and even faith leaders.[1687] Thus, the political culture of the various states must be adapted to understand the need for the participation of all citizens, while the international platform must update its voting rights to accommodate more input from developing countries.[1688]

It must be pointed out that when some states feel disenfranchised from the international platform, they feel less interested in contributing to the success of the institution.[1689] Also, the more developing countries feel that their interests are not taken into account, the more they tend to detach from the international institution, making the institution the exclusive preserve of developed countries.[1690] This will defeat the essence of a global fight against a ubiquitous menace. In fact, Samans *et al* further suggested that secretariats be established in developing countries with staff from varying state stakeholders as this will help engender proper integration of various individuals from diverse countries.[1691] This will foster better cooperation that gives developing countries a sense of inclusion in the larger system.

It is submitted that efficient international cooperation will focus on:

a. The emergence of a unified global and harmonised legislative framework enforceable at the national, regional and international level.[1692] This legislative framework must take into account the need for genuine regard for individuals' fundamental human rights and respect for the rule of law.
b. The emergence of cyber-security, legal and law enforcement framework that will address the operational, procedural, regulatory, economic, technical, and human

1687 Samans, Schwab and Malloch-Brown *Everybody's business* 19-44.
1688 Samans, Schwab and Malloch-Brown *Everybody's business* 19-44.
1689 Samans, Schwab and Malloch-Brown *Everybody's business* 19-44.
1690 Samans, Schwab and Malloch-Brown *Everybody's business* 19-44.
1691 Samans, Schwab and Malloch-Brown *Everybody's business* 19-44.
1692 Schjølberg S and Ghernaouti-Helie S "A global protocol on cybersecurity and cybercrime" http://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf (Date of use: 3 June 2017).

aspects in relation to addressing this trans-national menace.[1693] These frameworks must be redefined to promote an effective means of bringing perpetrators to book.[1694]

c. Proper addressing of jurisdictional issues and measures to avoid frictions arising therefrom.[1695]

d. Promotion of effective mutual assistance amongst nations in tackling cybercrime,[1696] also ensuring cooperation and better coordination in law enforcement especially across national borders.[1697]

e. Promotion of the emergence of regional hubs that will provide technical assistance and information in addressing cybercrime.[1698]

f. Improvement of effective cooperation and coordination among all the relevant stakeholders.[1699]

g. The development of uniform best practices with regards to IT protection and response.[1700] This will ensure the evolution of higher uniform standards for IT content and service providers with regards to the security of their products and

---

1693 Schjølberg and Ghernaouti-Helie http://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf (Date of use: 3 June 2017).

1694 Schjølberg and Ghernaouti-Helie http://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf (Date of use: 3 June 2017).

1695 Schjølberg and Ghernaouti-Helie 'http://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf (Date of use: 3 June 2017).

1696 Schjølberg and Ghernaouti-Helie http://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf (Date of use: 3 June 2017).

1697 Li http://www.webology.org/2007/v4n3/a45.html (Date of use: 30 April 2017).

1698 Schjølberg and Ghernaouti-Helie http://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf (Date of use: 3 June 2017).

1699 Schjølberg and Ghernaouti-Helie http://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf (Date of use: 3 June 2017).

1700 Schjølberg and Ghernaouti-Helie http://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf (Date of use: 3 June 2017).

services.[1701] These measures must be easily understood and easily set up by the end users.[1702]

h. Education and promotion of cyber-security awareness at the national, regional and international levels.[1703]

CONCLUSION

This chapter has demonstrated that international cooperation is the bond that holds together all efforts by the various nations to tackle this ubiquitous trans-national crime – cybercrime.

Tackling cybercrime involves many angles, such as the detection, investigation and prosecution of the crime; the seizure of digital evidence and its forensic analysis; information sharing; effective public-private sector cooperation; crime awareness; and deterrence of future occurrences. All these angles require concerted and effective international cooperation in order to succeed.

It has been demonstrated that developing countries constantly lag behind in the quest for a lasting solution in addressing cybercrime. Unfortunately, it is in the best interest of developed countries to take every practical measure to get the cooperation of the developing countries. This is because the ubiquitous nature of the internet makes every country that provides a safe haven by its acts of omission to constitute a weak link that leaves countries with inadequate steps in tackling cybercrime vulnerable.

1701 Schjølberg and Ghernaouti-Helie http://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf (Date of use: 3 June 2017).

1702 Schjølberg and Ghernaouti-Helie http://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf (Date of use: 3 June 2017).

1703 Li http://www.webology.org/2007/v4n3/a45.html (Date of use: 30 April 2017).

It is therefore imperative that developed and developing countries alike start taking appropriate steps to cooperate adequately in order to ensure that no country becomes a safe haven for cyber-criminal activities. International cooperation must be strengthened. There must be some harmony in all legal and technological solutions being set up to tackle this trans-border menace. Any state that constitutes a weak link creates a loophole and leaves the other nations vulnerable.

Chapter 8 will conclude the entire research. It will provide a summary of the entire research and also make recommendations that when employed, will ensure the participation of developing countries in the fight against cybercrime.

CHAPTER 8

CONCLUSION, SUMMARIES AND RECOMMENDATIONS

8.1. CONCLUSION

The world continues to change, and technology continues to push boundaries. Situations that existed only in the realm of imaginations are constantly coming to life. Information is transferred across the globe in microseconds and technology has squeezed the world into a global village. Technology constantly pushes away the traditional ways of doing things and, daily, every facet of human endeavour adapts to this ever-changing innovations brought by technology. This presupposes that the law must also jettison its traditional methods and modify its time-tested established norms in order to remain relevant in governing these novel and ever-emerging systems that technology continues to churn out to make life easier for mankind.

Our legislation, judicial processes and modes of investigation cannot rely on their traditional state to effectively regulate information technology as it constantly evolves. The nefarious criminal actions that pose a threat to this human innovation cannot effectively be addressed by the current legal jurisprudence in its nationally-segmented approach without evolving a transnational approach. As the law keeps adapting itself to effectively regulate cyber activities, the ubiquitous nature of the internet, which is not hindered by national boundaries, presumes that any effort to properly regulate the internet must be a collective effort cutting across regions and continents. Solutions to the menace of cybercrime cannot be balkanised along regional lines and nevertheless become effective.

The objective of this research was to consider the various efforts evolved by various national (developed and developing nations alike) and international bodies in tackling cybercrime. The research took into consideration the ubiquitous nature of the internet, and thus acknowledged and highlighted the efforts of developed countries while focusing more on the extent of preparedness of developing countries and their current involvement in the global fight against cybercrime.[1704] The research identified some of the major factors that hampered any meaningful participation by developing countries and also proffered a number of solutions that will draw developing countries out of their apathy in effectively being part of the global drive to tackle cybercrime.[1705] The research further called for the modification of existing regulatory structures such as the establishment of a uniform treaty, a unified global law enforcement system, a uniform cybercrime adjudicatory system, and a unified internet governing scheme.[1706]

In doing this, this thesis examined the steps taken by several developing countries (India, Nigeria and South Africa) and compared their efforts with the efforts of some developed countries (the United States of America and the United Kingdom) that had achieved major breakthroughs in their fight against e-crime.[1707] The developing countries analysed were at varying degrees of development as countries. For example, Nigeria is at the lower rung of development, while India and South Africa were high on the ladder of national development. These two countries can compete with developed countries because of their level of national development.

This research considered the approaches of the United States of America and the United Kingdom as examples of developed countries that have taken innovative steps in countering e-crime.[1708] On the other hand, South Africa, Nigeria and India were analysed as examples of developing countries in exposing the various degrees of actions or inactions of developing countries in addressing the menace of cybercrime.[1709]

1704 See ch 2 of this research.
1705 See ch 2 sec 2.6, and ch 5 secs 5.1 and 5.2 of this research.
1706 See ch 3 sec 3.4, ch 4 secs 4.2 - 4.3, and ch 6 sec 6.4 of this research.
1707 See ch 2 of this research.
1708 See ch 2 secs 2.1 and 2.3 of this research.
1709 See ch 2 secs. 2.2 and 2.4 of this research.

This thesis in reviewing the approaches of the various nations (developed and developing countries alike) analysed the legislative responses, technological capacities, investigative capabilities, adjudicatory competence and further preventive measures deployed by the various nations.[1710]

At the commencement of this research, this work proposed to address the following questions:

i. What is the extent of the involvement of developing countries in tackling the menace posed by cybercrime?
ii. What are the factors that impede the active participation of emerging economies in taking decisive steps in joining the fight against cybercrime?
iii. What effective strategies will ensure the participation of various stakeholders in developing countries in the fight against cybercrime?
iv. Would a harmonised cybercrime convention/legislation provide the much-needed regulatory framework to address cybercrime, on the one hand, and get the developing countries involved, on the other?
v. What is the level of the participation of the developing countries in the control of cyberspace and/or policy making that affects the cyberspace?

The research addressed the above-mentioned questions as well as others. The thesis further considers that various internet governance forums such as ICANN formulate global internet policies to shape the national policies of developed and developing countries alike.[1711] For example, national telecommunication standards must align with ITU-agreed infrastructure management and standards[1712] and national radio spectrum allocation must align with the international radio frequency table as laid down by the

1710 See ch 2 of this research.
1711 See ch 6 sec 6.1 of this research.
1712 Bekkers R *Mobile telecommunications standards: GSM, UMTS, TETRA, and ERMES* (Artech House Norwood 2001) 87-118.

ITU.[1713] The standard-setting policies, protocol and guidelines of the World Wide Web Consortium also govern the internet infrastructure, applications and technical development of the developing countries.[1714] The national policies of developing nations thus take into account the policies formulated at the various internet governance fora and are fashioned to meet those standards and requirements.

The active participation of developing countries in every facet of internet governance is not only desirable but expedient. This is so because it accords with common sense that developing countries contribute to policies that they will eventually adopt so that while the policy is still being evolved, developing countries can ensure that those policies are well suited for their peculiar jurisdiction.

8.2. SUMMARIES

As the thesis progressed in its quest to find a solution on how to enlist the participation of developing countries in addressing the menace of cybercrime, a number of findings were made. Some of these findings include:

- Cybercrime is ubiquitous, and is not weighed down by jurisdictional boundaries and, thus, cannot effectively be tackled by one or a few nations or regions. No nation has absolute sovereignty and powers to regulate activities on cyberspace.
- The menace of cybercrime grows in leaps and bounds and the current efforts of developing countries in fighting the menace are not assisting the fight.
- Countries without adequate measures to tackle cybercrime will provide a weak link and become a safe haven from where perpetrators can send their offending activities on to other countries.
- Every country must join the fight against cybercrime, otherwise some countries will provide safe havens for perpetrators to operate from in conducting their

1713 Mazar H *Radio spectrum management: Policies, regulations and techniques* (John Wiley Chichester 2016) 112-148.

1714 Nevile CM "World wide web consortium process document" https://www.w3.org/2015/Process-20150901/ (Date of use: 22 July 2017).

nefarious activities. Allowing safe havens would hamper any meaningful effort made by other progressive nations to contain cybercrime.

- The support and active participation of the developing countries must be obtained since cybercrime is a global phenomenon. Regulating cyberspace must be supranational.
- Developing countries have been left behind in the scheme of things with regard to internet governance and the various regulatory processes that govern the internet. There is a veritable need for an efficient regulatory structure to be formulated and developing countries to be made part of the process.
- The enactment of an efficient international legal structure and legislation holds an important key to the involvement of developing countries in the fight against cybercrime.
- Enlisting the support of developing countries in fighting the menace of cybercrime transcends the formulation of cybercrime legislation and includes socio-economic strategies that will compel the involvement of developing countries in fighting cybercrime.
- An understanding and identification of the socio-economic and political culture of the developing countries holds another key to resolving the apathy of developing countries.
- Legislative, law enforcement, judicial and other efforts to address cybercrime must be transnational, uniform and can only be achieved by ways of international law.
- The sovereignty of nations must be slightly slackened to encourage effective trans-border investigations and law enforcement.
- Developed and developing countries must play an active role in internet governance. Developing countries must be encouraged to increase their participation in the governance of the internet.

The thesis made some notable findings, and came up with some contributions and proposals which, when put into place, will help bridge the gulf between the efforts of developed and developing countries in addressing cybercrime; and will propel

developing countries to join the fight against cybercrime. Some of the contributions and proposal include:

- proposing a uniform consistent cybercrime taxonomy that will ensure adequate crime reporting, collaborative working among agencies, knowledge sharing and provision of clear measurements on the impact of cybercrime across jurisdictions which will bring forth efficiency in addressing cybercrime;[1715]
- proposing the emergence and adoption of a harmonised uniform cybercrime legislation/treaty that will, on the one hand, provide a minimum legislative response for both developed and developing countries, and on the other, ensure that no nation provides a safe haven because of the absence of an adequate legislative response.[1716] The thesis also proposed a number of measures that will propel every nation into subscribing to this uniform cybercrime treaty.[1717]
- revealing the progressive legislative responses, technological capabilities, law enforcement competence and proactive preventive measures deployed by developed countries;[1718]
- revealing the state of average legislative responses, deplorable technological capacity, inept law enforcement mechanisms and derelict preventive measure that characterise the efforts of most[1719] developing countries in addressing cybercrime;[1720]
- identifying the various factors that aid the apathy of developing countries in actively participating in addressing cybercrime.[1721] The thesis also proffered various socio-economic solutions that will bring about the active participation of developing countries in addressing cybercrime;[1722]

1715 See ch 3 sec 3.1 of this research.
1716 See ch 3 sec 3.4 of this research.
1717 See ch 3 sec 3.4 of this research.
1718 See ch 2 secs 2.1 and 2.3 of this research.
1719 Developing countries that have attained a high level of development, such as South Africa, have more enhanced law enforcement systems and are taking steps in line with most developed countries to curb cybercrime in their jurisdictions.
1720 See ch 2 secs 2.2 and 2.4 of this research.
1721 See ch 2 secs 2.6 and ch 5 sec 5.1 of this research.
1722 See ch 5 sec 5.2 of this research.

- proposing the emergence of an International Criminal Court for Cyberspace (ICCC) with appellate jurisdiction and original jurisdiction in some cases;[1723]
- proposing the emergence of a global uniform law enforcement agency;[1724]
- proposing the emergence of a uniform internet regulatory body that will accommodate and encourage the participation of developing countries in internet governance;[1725]
- proposing measures that will compel nations to take proactive steps in participating in the various proposed schemes

8.3. RECOMMENDATIONS

This research proposed steps and made recommendations at the end of each chapter that will bring about the participation of developing countries in the fight against cybercrime. It is submitted that various stakeholders should adopt these recommendations in order to ensure that cybercrime is effectively tackled.

However, it must be pointed out that the enactment of laws, the ratification of treaties and the modification of existing laws that will combat cybercrime clearly is not a difficult task for developing countries. For example, while this research was in progress, the Nigerian legislative body enacted the Cybercrime Act of 2015.[1726] A survey of most developing countries reveals that they have some form of legislative response to cybercrime even though most of these responses may be outdated. The challenge, therefore, is in the implementation of the law. The ability of law enforcement agencies to live up to their expectations is always in question. Another challenge is the ability of the ruling class to take adequate steps that will properly steer the nation to effectively participate in the various suggested international efforts to combat cybercrime and to participate in internet governance, bearing in mind that there are other pressing factors that weigh the nation down. The limited bargaining clout of developing countries and the

1723 See ch 4 sec 4.3 of this research.
1724 See ch 4 sec 4.2 of this research.
1725 See ch 6 sec 6.4 of this research.
1726 The Act was signed into law on 15 May 2015. Onyekwere J "Cybercrimes Act 2015 and need for further amendments" *The Guardian* 24 August 2015 24.

inability of developing countries to form a cohesive position on global issues and governance affect their ability to participate and advance their position in global efforts to curb cybercrime.[1727] The absence of ICT-experienced individuals and the constant brain-drain of available ICT experts from developing countries to developed countries further deplete the ability of developing countries to contribute to global ICT policy formulations.[1728] The absence of effective cooperation among developing countries and the desire of most developing countries to join and identify with most extra-regional blocs[1729] of developed countries make developing countries unable to act as a group to negotiate or present a common front on global policy issues that affect them.[1730] Thus, most developing countries acquiesce to policies enacted by developed countries made without their input and also not modelled to address their peculiar regions or nations.

In sum, the capacity of most developing countries is asinine and this grossly affects their participation in addressing cybercrime.

Chapter 2 of the research highlighted the dearth of technical and policy capacity in the various cybercrime fighting institutions of various developing countries.[1731] Several technical,[1732] informational,[1733] financial[1734] and institutional[1735] hurdles exist that affect

---

1727 Dzidonu C and Quaynor NN "Broadening and enhancing the capacity of developing countries to effectively participate in the global ICT policy fora and the ICT for development (ICTfDev) Process" https://archive.icann.org/en/meetings/carthage/conceptpaper-carthage-globalict.pdf (Date of use: 22 July 2017).

1728 Dzidonu and Quaynor https://archive.icann.org/en/meetings/carthage/conceptpaper-carthage-globalict.pdf (Date of use: 22 July 2017).

1729 For example, a number of developing countries are signatories to the Council of Europe Convention on Cybercrime. See https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (Date of use: 22 July 2017).

1730 Dzidonu and Quaynor https://archive.icann.org/en/meetings/carthage/conceptpaper-carthage-globalict.pdf (Date of use: 22 July 2017).

1731 Sec 2.4 of this research.

1732 This points to a situation where there is an absence of necessary technical skills to "(i) effectively participate in relevant global fora; (ii) comprehend the details of the deliberations and the proceedings of the event; (iii) effectively contribute to the discussions of the fora and (iv) learn/benefit from the proceedings of fora." See Dzidonu and Quaynor https://archive.icann.org/en/meetings/carthage/conceptpaper-carthage-globalict.pdf (Date of use: 22 July 2017).

1733 This relates to situations where the stakeholders are unable to participate as a result of their inability to access the about the relevant ICT fora. Dzidonu and Quaynor https://archive.icann.org/en/meetings/carthage/conceptpaper-carthage-globalict.pdf (Date of use: 22 July 2017).

the capacity of developing countries. These hurdles lead to varying degrees of participation of developing countries and their institutions. According to Dzidonu *et al*, full participation in internet governance requires that national stakeholders overcome every form of barrier, while possessing the requisite expertise to attend and actively participate in policy-formulating events, and contributing to and learning from internet governance events without any structural inhibitions.[1736] Dzidonu *et al* referred to a lesser form of participation as partially effective participation which entails that stakeholders overcome all forms of barriers, possess the requisite expertise, have no structural inhibitions but partially participate because of other factors.[1737] In other circumstances, stakeholders may experience non-effective participation where, although they are part of the internet governance event, they are restrained from participating due to a lack of technical know-how and institutional barriers.[1738] In the case of some stakeholders, they may possess the requisite technical know-how when attending an event, but are distracted by other priorities (such as shopping and sight-seeing) making them unable to participate.[1739] Some stakeholders may possess the skills to participate and in fact are willing to participate but are constrained by financial barriers which make them unable to participate.[1740] The final category are stakeholders plagued by the four identified barriers, namely, being bereft of technical know-how;

1734 This relates to situations where the stakeholders lack the financial capability to participate adequately; access information; travel for the purpose of meetings and conferences; contribute financially to the ICT fora; and handle other incidental matters that require finances. See Dzidonu and Quaynor https://archive.icann.org/en/meetings/carthage/conceptpaper-carthage-globalict.pdf (Date of use: 22 July 2017).

1735 This relates to the absence of capacity of the stake-holding institutions in developing countries. This may be as a result of weak structures and an absence of synergy with other developing countries that will deprive the countries from forming a collective front for their mutual benefit. The weak structures delegate unqualified persons to attend ICT fora and to formulate polices. See Dzidonu and Quaynor https://archive.icann.org/en/meetings/carthage/conceptpaper-carthage-globalict.pdf (Date of use: 22 July 2017).

1736 Dzidonu and Quaynor https://archive.icann.org/en/meetings/carthage/conceptpaper-carthage-globalict.pdf (Date of use: 22 July 2017).

1737 Dzidonu and Quaynor https://archive.icann.org/en/meetings/carthage/conceptpaper-carthage-globalict.pdf (Date of use: 22 July 2017).

1738 Dzidonu and Quaynor https://archive.icann.org/en/meetings/carthage/conceptpaper-carthage-globalict.pdf (Date of use: 22 July 2017).

1739 Dzidonu and Quaynor https://archive.icann.org/en/meetings/carthage/conceptpaper-carthage-globalict.pdf (Date of use: 22 July 2017).

1740 Dzidonu and Quaynor https://archive.icann.org/en/meetings/carthage/conceptpaper-carthage-globalict.pdf (Date of use: 22 July 2017).

being financially crippled; not being able to effectively participate when given the opportunity; and not being able to even attend the event.[1741]

However, full and active participation of developing countries is the only acceptable level of participation that should be aimed at. This calls for shared responsibility of all stakeholders from both developed and developing countries. As pointed out in the preceding chapters of the thesis, developing countries cannot be left alone to sort out their challenges by themselves. It is evident that developing countries cannot by themselves rise to the enviable height of active participation. This is because a country that lacks capacity actually needs help to appreciate the extent of its despondency, to seek appropriate solutions and be drawn out of its deplorable state.

To this end, in order to increase the capacity of developing countries, it is submitted that the recommendations in chapters 5 and 6 of the research be applied. That is to say, policy awareness must be raised; national policy institutions must be strengthened; and national priorities must be repositioned to make the fight against cybercrime a priority. Adequate fiscal support must be deployed by both developed countries and the developing countries that require assistance, and participation in internet governance forums must be a priority. On the other hand, the deployment of sanctions, coercive diplomacy, trans-border data flow restrictions and constant pressures from civil societies will compel developing nations to take any steps to increase the capacity of individuals and institutions within their jurisdictions. Again, the adoption of the recommendations of chapter 7 sub-section 7.3.9 of this research will be an apposite step in shoring up the capacity of developing countries.

It must be pointed out that even though there should be some shared responsibilities by both developed and developing countries in shoring up the capacity of developing countries, many responsibilities rest on the shoulders of developing countries. For example, developing countries must ensure that the funding received is not channelled

---

[1741] Dzidonu and Quaynor https://archive.icann.org/en/meetings/carthage/conceptpaper-carthage-globalict.pdf (Date of use: 22 July 2017).

to personal or other needs of greedy politicians and policymakers. It is the responsibility of developing nations to mobilise its stakeholders to take part in the capacity-building venture.

When there is adequate capacity, it will be easy to implement the various suggestions proffered in this research and it will be easier for developing countries to adequately participate and contribute to the efforts of developed countries in combating cybercrime.

This study has brought to fore the extent of the menace that cybercrime currently poses to mankind and the need for nations to forge a formidable common front in tackling this menace. In achieving this, the study has shown that developing nations must take proactive steps in addressing cybercrime through its legislative responses, judicial and adjudicatory processes, and law enforcement strategies. The thesis has also demonstrated that without the active participation of developing nations in the fight against cybercrime, the commendable efforts of developed countries to nip the menace in the bud will not yield the desired results, thereby leaving these developed countries vulnerable and their efforts made futile. The thesis have shown that there is a need for uniformity in addressing cybercrime while drawing attention to the factors that orchestrate the apathy of developing countries in joining the fight against cybercrime.

Drawing from the findings made in this research, further recommendations are made with the hope that when they are adhered to, addressing cybercrime will be a collective effort of both developed and developing nations. It is further recommended that nations of the world should come together and –

- **enact a uniform cybercrime treaty**

  This study has shown that the primary step in addressing any crime is the enactment of an appropriate legislative response. Unfortunately, existing efforts of developed countries or regional bodies to provide a consistent legislative framework have failed to provide the desired result. Cybercrime, being of a

ubiquitous nature, needs a ubiquitous legislative response that will engender harmony across regions and nations. A uniform cybercrime convention/legislation championed by the UN will provide the much-needed regulatory framework in addressing cybercrime, on the one hand, and will get the developing countries involved, on the other.[1742] Regional treaties and bilateral agreements do not provide the much-needed global solution and will not demand the active participation of developing countries.

Enacting a cybercrime legislation/convention will lead to harmonised national cybercrime legislations which will eliminate safe havens, enable international cooperation in trans-border investigations, prosecutions and general prevention.

It is recommended that the UN sets in motion the process of actualising this harmonised cybercrime legislation. The UN can employ all its machineries to mount pressure on every nation, especially developing nations, to adopt the harmonised cybercrime legislation/convention and further domesticate same within its jurisdiction to eliminate the inconsistencies and gaps that characterise legislative responses that vary across national jurisdictions. The evolution of this harmonised cybercrime legislation by the UN will take care of the reluctance of nations that refuse to adopt the CoE Cybercrime Convention[1743] and remain without adequate cybercrime legislation.[1744] This will compel developing nations to lend their support to the fight against cybercrime having had all their legislative hurdles cleared.

- **establish a uniform cybercrime law enforcement agency**

  The enactment of laws is futile without adequate enforcement mechanism. As shown in chapter 4 of this research, the mere cooperation of regional and

1742 See ch 3 of this research.

1743 The CoE Cybercrime Convention, being a European initiative, may not be accepted by nations outside Europe.

1744 For example, Zimbabwe's effort to secure a cybercrime Act is still undergoing several legislative processes and has not been enacted. See https://www.theindependent.co.zw/2017/01/13/cybercrimes-bill-flaws-remedies/ (Date of use: 14 August 2017).

national law enforcement bodies will remain to be subjected to several jurisdictional hurdles. Unfortunately, the efficient cooperation of law enforcement bodies is not easily attained. The establishment of an online international crime control mechanism that effectively and efficiently tackles trans-border investigations, while not eroding the sovereignty of states, will be a step in the right direction.

It is recommended that a uniform law enforcement body with branches in all nations of the world be established for the efficient enforcement of the uniform cybercrime legislation/convention. It is recommended that this online global uniform law enforcement be carved out as a distinct and most prominent unit of the said international police body.

It is recommended that while the parent body (INTERPOL) maintains its global policing model of operation, this online global uniform law enforcement agency (a distinct section inside INTERPOL) maintains a global police force model of operation.[1745] This online global uniform law enforcement agency will be saddled with the responsibility of policing or intervening only on transnational cyber-criminal activity. The local or national police of each national jurisdiction should maintain its power of coercion within its national precincts and should investigate cyber-criminal activities that take place and are restricted within its national confines.

With this law enforcement arrangement, developing countries will have the requisite drive to participate in the fight against cybercrime since they will be part of this online global uniform law enforcement which will operate within its borders. Also, the national police will readily receive assistance and capacity

[1745] As shown earlier in ch 4 of this research, global policing, which INTERPOL maintains, entails surveillance and coercive powers while a global police force entails the possession of universal jurisdiction and formal powers to arrest and detain suspects anywhere in the world, as national police forces do. See also Bowling B and Sheptycki J *Global policing* (Sage Publications London 2012) 129.

development from the branch of the online global uniform law enforcement agency within the nation's jurisdiction.

- **establish an International Criminal Court for Cyberspace (ICCC)**

  Legislations/treaties, law enforcement and the courts are the major three-pronged entity that produces law and order in every society. The ubiquitous nature of the internet calls for some uniformity in the adjudicatory process. Most cybercrimes are trans-national in nature, violating the laws of several national precincts and thus presupposes (as shown in chapter 4 of this research) that an international court should have some adjudicatory powers over offenders.

  It is recommended that an international cyber-criminal court be established as a sub-division of the International Criminal Court. As already posited in chapter 4 of this research, it is recommended that the Court should exercise appellate jurisdiction in most cases provided the crime is of a trans-national nature.

  It is recommended that the composition of the said Court, its jurisdictional authority, its appellate powers and original jurisdictional powers as proposed in chapter 4 of this research be adopted in the institution of this International Criminal Court for Cyberspace (ICCC).

  This Court will ensure uniformity in adjudicating over cybercrime, and the participation of developing countries since its judges will be picked from across developed and developing countries. Also, when appeals lie from the national courts to this International Criminal Court for Cyberspace (as proposed in chapter 4 of this research), the efforts of developing countries will be reviewed by the Court constraining the stakeholders to become more efficient.

- **tackle the socio-economic problems of developing countries that exacerbate their apathy**

A major cause behind the apathy of developing countries and their lack of capacity to tackle cybercrime is the socio-economic state of the nations. Chapter 5 of this research identified some socio-economic factors that fuel the apathy of developing countries and also proffered a number of solutions to these socio-economic challenges. The higher the socio-economic challenges, the lower the development within those nations and the higher the inability to address e-crime. There is no gainsaying the fact that until developing countries are drawn out from their socio-economic predicament, cybercrime will largely remain unattended. As stated earlier, there is a nexus between national development and the nation's capacity and desire to actively participate in the fight against cybercrime.

Therefore, it is recommended that developed countries aid developing countries to overcome their socio-economic problems. Stakeholders in developing countries must also take adequate steps to compel their leaders to address the various socio-economic challenges. Leaders must be held accountable. Developed countries may have to intervene when bad leadership continue to pervade developing countries.

- **strengthen cybercrime curbing institutions within developing countries**

  The establishment of cybercrime regulatory frameworks, their successful implementation, adjudication and effective participation of nations at the international scene require strong institutions. Fighting cybercrime involves various institutions – the judiciary, law enforcement agencies, legislature and several institutional stakeholders. Effective legal, technical and procedural measures are imperative and the institutions that provide these in developing countries must be strengthened.

  The legal systems of developing countries have mostly evolved through various stages of their national development and are tied to the level of development of the countries. Developing countries are at their current level of development because of their weak institutions, invariably also leaving the institutions that

make up the legal systems weak. Obsolete investigative capabilities and rules of procedure hamper meaningful strides in tackling cybercrime, are not victim-friendly and unable to align with any international efforts. It therefore is imperative that every institution saddled with criminal investigations and adjudication especially in relation to e-crime be strengthened. The law makers, policy formulators, prosecutors, judges, international agency representatives and all stakeholders most exposed to ICT and consistently trained in cyberaws and getting rid of cybercrime. The capacity of all stakeholders must be strengthened.

- **the UN should conduct further studies and bring together all stakeholders in order to adopt a united system that will combat cybercrime with the active participation of developed and developing countries alike**

  It is established that cybercrime cannot be effectively tackled by one or a few nations. Developing countries cannot afford to be marginalised or left behind because they simply create safe havens. A united battle under a global democratic setting will create the proper environment that engenders shared responsibilities which will propel developing nations into joining the fight against internet crime. Every person or nation affected by or involved in the use of the internet should actively participate in its regulations and contribute to its growth and security. It is hoped that the emergence of a uniform legislation, cybercrime court and law enforcement agency will engender the fundamental changes that will lead to the proper fight against cybercrime across the globe. This global democratic intervention will be in line with WGIG's position that "no single government should have a pre-eminent role in relation to international internet governance".[1746] "The organisational form for the governance function will be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organisations."[1747]

1746 Hassan A "Internet governance: Strengths and weaknesses from a business perspective" in Drake WJ (ed) *Reforming internet governance: Perspectives from Working Group on Internet Governance (WGIG)* (United Nations New York 2005) 117-128.

1747 Pal LA "Governing the electronic commons: Globalization, legitimacy, autonomy and the internet" in Bernstein S and Coleman WD (eds) *Unsettled legitimacy: Political community, power, and authority in a global era* (UBC Press Vancouver 2009) 280-299.

> "The organisational form for the governance function will involve all stakeholders and relevant intergovernmental and international organisations within their respective roles".[1748]

It is evident that this research, although broad, cannot pretend to have covered all areas that touch on addressing cybercrime on a global scale. The work has recommended uniformity in law enforcement, the adjudicatory system, legislation and better trans-national cooperation. The complexities of managing these regulatory structures under a global democratic setting in order to operate effectively poses an enormous burden on all stakeholders. The recommended united systems must evolve into a reasonably well-functioning trans-national legal system. Until such time as the legal system on a trans-national scale has been strengthened, eliminating safe havens and maintaining tranquillity in cyberspace will be far-fetched. The world must present a common front if cybercrime is to be halted.

[1748] Pal *Governing the electronic commons* 294.

BIBLIOGRAPHY

BOOKS AND JOURNALS

Abimbola A “Pressure groups and the democratic process in Nigeria (1979-1993)” 2002 *Nordic Journal of African Studies* 38-47

Achugbue EI and Akporido CE “National information and communication technology policy process in developing countries” in Adomi EE (ed) *Framework for ICT policy: Government, social and legal issues* (IGI Global New York 2011) 218-232, abbreviated as Achugbue and Akporido *National information and communication technology*

Agnew R “Strain theories” in Parrillo VN (ed) *Encyclopaedia of social problems* (Sage Publications California 2008) 904-906

Al-Darrab AA “The need for international internet governance oversight” in Drake WJ (ed) *Reforming internet governance: Perspectives from the Working Group on Internet Governance* (United Nations ICT Task Force New York 2005) 175-184, abbreviated as Al-Darrab *Internet governance oversight*

Alexander JC “Analytic debates: Understanding the relative autonomy of culture” in Alexander JC and Seidman S (eds) *Culture and society: Contemporary debates* (Cambridge University Press Cambridge 1990) 1-66

Alkaabi A *et al* “Dealing with the problem of cybercrime” in Baggili I (ed) *Digital forensics and cyber crime* (Springer Heidelberg 2011) 1-18, abbreviated as Alkaabi *et al Dealing with the problem of cybercrime*

Ambos K "The International Criminal Court and the traditional principles of international cooperation in criminal matters" in Takamaa K and Koskenniemi M (eds) *The Finnish yearbook of international law 1998* (Kluwer Law International The Hague 2000) 413-425 abbreviated as Ambos *Traditional principles*

Amerasinghe CF *Principles of the institutional law of international organisations* (Cambridge University Press Cambridge 2005) 408-410

Andreas P and Nadelmann E *Policing the globe: Criminalisation and crime control in international relations* (Oxford University Press New York 2006) 10-58

Ang PH "The role of self-regulation of privacy and the internet" (2001) *Journal of Interactive Advertising* 1-9

Ani L "Cyber crime and national security: The role of the penal and procedural law" in Azinge E and Bello F *Law and security in Nigeria* (NIALS Press Lagos 2011) 197-234

August R "International cyber-jurisdiction: A comparative analysis" (2002) *American Business Law Journal* 531-574

Axelrod EM *Violence goes to the internet: Avoiding the snare of the net* (Charles C Thomas Publishers Springfield 2009) 5-16

Balzer AJ "International police cooperation: Opportunities and obstacles"in Pagon M (ed) *Policing in Central and Eastern Europe: **C**omparing first hand knowledge with experience from the West* (College of Police and Security Studies Ljubljana 1996) 63-74, abbreviated as Balzer *International police cooperation*

Bansal SK *Information system management* (APH Publishing New Delhi 2002), abbreviated as Bansal *Information system management*

Banzal S *Data and computer network communication* (Firewall Media Publishers New Delhi 2007)

Bawole JN *et al* (eds) *Development management: Theory and practice* (Routledge New York 2017) 32

Bekkers R *Mobile telecommunications standards: GSM, UMTS, TETRA, and ERMES* (Artech Publications Boston 2001) 87-136

Blackman K "The uniform domain name dispute resolution policy: A cheaper way to hijack domain names and suppress critics" (2001) *Harvard Journal of Law and Technology* 223-230

Bowling B and Sheptycki J *Global policing* (Sage Publication London 2012) 1-129, abbreviated as Bowling and Sheptycki *Global policing*

Brenner S "State cybercrime legislation in the United States of America: A survey" (2001) *Richmond Journal of Law and Technology* 28-36 abbreviated as Brenner 2001 *Richmond JLT*

Brenner SW and Koops B "Approaches to cybercrime jurisdiction" (2004) *Journal of High Technology Law* 1-46, abbreviated as Brenner and Koops cybercrime jurisdiction *Journal of HTL*

Brenner SW *Cybercrime: Criminal threats from cyberspace* (Greenwood Publishing California 2010) 142-163, abbreviated as Brenner *Cybercrime: Criminal threats from cyberspace*

Broadhurst R "Developments in the global law enforcement of cyber-crime" (2006) *International Journal of Police Strategies and Management* 408-433, abbreviated as Broadhurst 2006 *International JPSM*

Broadhurst R and Chang YC "Cybercrime in Asia: Trends and challenges" in Liu J and Hebenton B (eds) *Handbook of Asian criminology* (Springer New York 2013)

Burns RG, Whitworth KH and Thompson CY "Assessing law enforcement preparedness to address internet fraud" (2004) *Journal of Criminal Justice* 477-493, abbreviated as Burns, Whitworth and Thompson 2004 *Journal CJ*

Butler AH "The growing support for universal jurisdiction in National legislation" in Macedo S (ed) *Universal jurisdiction: National courts and the prosecution of serious crimes under international law* (University of Pennsylvania Press Philadelphia 2004) 67-76

Carmody B *Online promotions: Winning strategies and tactics* (Black Forest Press San Francisco 2004) 47-77, abbreviated as Carmody *Online promotions*

Casey E *Digital evidence and computer crime: Forensic science, computers and the internet* (Elsevier Waltham 2011) 35-48, abbreviated as Casey *Digital evidence*

Cassim F "Addressing the challenges posed by cybercrime: A South African perspective" (2010) *Journal of International Commercial Law and Technology* 118-123

Cassim F "Formulating specialised legislation to address the growing spectre of cybercrime: A comparative study" (2009) *Potchefstroom Electronic Law Journal* 36-123, abbreviated as Cassim 2009 *Potchefstroom ELJ*

Castro D "US federal cybersecurity policy" in Andreasson KJ *Cybersecurity: Public sector threats and responses* (CRC Press Florida 2012) 127-156

Chang Y *Cybercrime in the greater China region* (Edward Elgar Publishing Cheltenham 2012) 89-145

Chango M "Accountability in private global governance: ICANN and civil society" in Scholte JA (ed) *Building global democracy? Civil society and accountable global governance* (Cambridge University Press Cambridge 2011) 267-287

Chapuis RJ and Joel AE *100 years of telephone switching* (IOS Press Amsterdam 2003)

Chawki M "Nigeria tackles advance fee fraud" (2009) *Journal Information Law and Technology* 1-20, abbreviated as Chawki *Journal ILT*

Chen TM and Davis C "An overview of electronic attacks" in Kanellis P *et al* (eds) *Digital crime and forensic science in cyberspace* (Idea Publishing London 2006) 1-26, abbreviated as Chen and Davis *An overview of electronic attacks*

Chinn MD and Fairlie RW "ICT use in the developing world: An analysis of differences in computer and internet penetration" (2010) *Review of International Economics* 153-167

Clifford RD (ed) *Cybercrime: The investigation, prosecution and defense of a computer-related crime* (Carolina Academic Press Durham 2011) 15-38, abbreviated as Clifford *The investigation, prosecution and defense of a computer-related crime*

Clough J *Principles of cybercrime* (Cambridge University Press Cambridge 2010) 3-130

Deibert R *et al* (eds) *Access denied: The practice and policy of global internet filtering* (MIT Press Cambridge 2008) 263-271

Dempsey J and Forst L *An introduction to policing* (Delmar New York 2010) 1-108

Dierks MP "Computer network abuse" (1993) *Harvard Journal of Law and Technology* 307-342

Downing RW "Shoring up the weakest link: What lawmakers around the world need to consider in developing comprehensive laws to combat cybercrime" (2005) *Columbia Journal of Transnational Law* 705-762

Doyle C *Extradition to and from the United States* (Nova Science Publishers New York 2008)1-64

Drahozal CH *The supremacy clause: A reference guide to the United States Constitution* (Greenwood California 2004) 89-94.

Driscoll W, Zompetti JP and Zompetti S (eds) *The International Criminal Court: Global politics and the quest for justice* (The International Debate Association New York 2004) 24-29

Drucker S, Gumpert G and Cohen HM "Social media" in Drucker SJ and Gumpert G (eds) *Regulating convergence* (Peter Lang Publishing New York 2010) 80-81

Duquenoy P, Jones S and Blundell BG (eds) *Ethical, legal and professional issues in computing* (Middlesex University Press London 2008) 79-95, abbreviated as Duquenoy *et al.* (eds) *issues in computing*

Fearon JD "Bargaining, enforcement, and international cooperation" (1998) *International Organisation* 269-305

Fondevila G “The rule of law in multilateral institutions and international aid for development: Judicial reform in the global order” in Kumar A and Messner D (eds) *Power shifts and global governance: Challenges from south and north* (Anthem Press London 2011) 123-138

Franda M *Governing the internet: The emergence of an international regime* (Lynne Riener Publishers Boulder 2001) 43-82

Freiberger P “Micro crime macro problem” (*Infoworld Texas 1981*) 37-38

Fuster GG *The emergence of personal data protection as a fundamental right of the EU* (Springer Heidelberg 2014) 75-108 Fuster *personal data protection*

Gay MK *Recent advances and issues in computers* (Oryx Press Phoenix 2000)

George AL *Forceful persuasion: Coercive diplomacy as an alternative to war* (United States Institute of Peace Washington DC 1991) 3-14

Ghernaouti-Helie S *Cyber power: Crime, conflict and security in cyberspace* (EPFL Press Lausanne 2013) 255-292, abbreviated as Ghernaouti-Helie *Cyber power*

Gibson JS *International organizations, constitutional law and human rights* (Praeger Publishers New York 1991) 114

Gibson W *Neuromancer* (Voyager London 1995) 4

Giles K “Russia’s public stance on cyberspace issues” in Czosseck C, Ottis R and Ziolkowski K (eds.) (papers delivered at 4th international conference on cyber space conflict 5-8 June 2012 Tallinn Estonia) 63-75, abbreviated as Giles *Russia’s public stance in cyberspace issues*

Goldsmith J “The internet and the legitimacy of remote cross-border searches” (2001) *Public Law and Legal Theory Working Papers* 1-12, abbreviated as Goldsmith *Public law and legal*

Goodman MD and Brenner SW “The emerging consensus on criminal conduct in cyberspace” (2002) *International Journal of Law and Information Technology* 139-223

Gordon GR and McBride RB *Criminal justice internships: Theory into practice* (Anderson Publishing Waltham 2012) 11-17

Govern K and Winn J "Data integrity preservation and identity theft prevention: Operational and strategic imperatives to enhance shareholder and consumer value" in Jalivand A and Malliaris *Risk Management and corporate governance* (Routledge New York 2012)

Gragido W, Molina D, Pirc J and Selby N *Blackhatonomics: An inside look at the economics of cybercrime* (Syngress Burlington 2012) 5-6

Great Britain: Parliament: House of Commons: Home Affairs Committee *Justice and Home Affairs Issues at European Union level* Third report of session 2006-07, Vol 2: Oral and written evidence (The Stationery Office Norwich 2007) 46-63

Haider S "The politics of providing basic amenities to the urban poor" in Mohanty B (ed) *Urbanisation in developing countries: Basic services and community participation* (Concept Publishing New Delhi 1993) 389-396

Hamelink CJ "Communication rights and the European information society" in Servaes J (ed) *The European Information Society: A reality check* (Intellect Bristol 2003) 121-147, abbreviated as Hamelink *Communication rights*

Hamilton J *Defending the nation: The FBI* (Abdo Publishing Edina 2007) 12-17

Haqqani AB (ed) *The role of information and communication technologies in global development* (United Nations Publication New York 2005) 3-18, abbreviated as Haqqani *global development*

Hasenclever A, Mayer P and Rittberger V *Theories of international regimes* (Cambridge University Press Cambridge 1997) 84-135

Hassan A "Internet governance: Strength and weaknesses from a business perspective" in Drake WJ (ed) *Reforming internet governance: Perspectives from Working Group on Internet Governance (WGIG)* (United Nations New York 2005) 117-128

Hearn J "*Voxpopuli*: Nationalism, globalization and the balance of power in the making of Brexit" in Outhwaite W (ed) *Brexit: Sociological responses* (Anthem Press London 2017) 19-30, abbreviated as Hearn *Vox populi*

Held D, McGrew A, Goldblatt D and Perraton J *Global transformations: Politics, economics and culture* (Stanford University Press Stanford 1999) 32-85, abbreviated as Held *et al Global transformations*

Hill R *The new international telecommunication regulations and the internet: A commentary and legislative history* (Springer Heidelberg 2014) 19

Holden G *et al E-business* (John Wiley Publishers New Jersey 2009), abbreviated as Holden *et al E-business*

Hunt H and Monhait JM "Extradition: Companies should invest in protecting their assets" (2013) *The Legal Intelligencer Journal* 1-3, abbreviated as Hunt and Monhait 2013 *The Legal Intelligencer Journal*

Jacovides A *International law and diplomacy: Selected writings of Ambassador Andrew Jacovides* (Martinus Nijhoff Publication Leiden 2011) 155

Jain VK *Basic computer programming* (Pustak Mahal Publishers New Delhi 1995)

Jakobs K *Standardisation processes in IT: Impact, problems and benefits of user participation* (ViewegLengerich 2000) 61-64

James S and Warren I "Australian police responses to transnational crime" in Eterno JA and Das DK (eds) *Police practices in global perspective* (Rowman & Littlefield Maryland 2011) 131-172

Johnson DR and Post DG "Law and Borders—The Rise of Law in Cyberspace" 1996 *Stanford Law Review* 1378 – 1379

Johnstone G *Restorative justice: Ideas, values, debates* (Routledge New York 2011) 72-93

Kent A and Hall CM *Encyclopedia of library and information science: Volume 71* (Marcel Dekker New York 2002) 146-161

Kohn MD, Eloff JHP and Olivier MS "UML modelling of digital forensic process models (DFPMs)" (Papers delivered at the Information Security for South Africa (ISSA) 2008 Innovative Minds Conference 7-9July 2008, Johannesburg, South Africa) 149-162, abbreviated Kohn *et al UML modelling*

Kshetri N “Cybercrime and cybersecurity in sub-Saharan African economies” in Kshetri N (ed) *Cybercrime and cybersecurity in the global south* (Palgrave Macmillan Hampshire 2013) 152-170, abbreviated as Kshetri *Cybersecurity*

Kshetri N “Cybercrime and cybersecurity issues in the developing Pacific Island economies: The current state, future prospects and policy measures” in *Harnessing disruption: Global, mobile, social, local* (Papers delivered at 34th Annual Pacific Telecommunications Conference 15-18 January 2012) 1023-1051

Kshetri N “The simple economics of cybercrimes” (2006) *IEEE Security and Privacy* 33-39, abbreviated as Kshetri *IEEE Security and Privacy*

Ladapo OA “Effective investigations, a pivot to efficient criminal justice administration: Challenges in Nigeria” (2011) *African Journal of Criminology and Justice Studies* 79-94, abbreviated as Ladapo *Effective investigations* 2011 *African JCJS*

Lewis BC “Prevention of computer crime amidst international anarchy” (2004) *American Criminal Law Review* 1353-1372

Lewis PM “The dysfunctional state of Nigeria” in Birdsall N, Vaishnav M and Ayres RL (eds) *Short of the goal: US policy and poorly performing states* (Centre for Global Development Washington 2006) 83-116

Maat SM *Cyber crime: A comparative law analysis* (LLM dissertation, University of South Africa 2004)

Macintosh KL “How to encourage global electronic commerce: The case for private currencies on the internet” (1998) *Harvard Journal of Law and Technology* 739-740, abbreviated as Macintosh global electronic commerce 1998 *Harvard JLT*

Maghaireh AMS *Jordanian cybercrime investigations: A comparative analysis of search for and seizure of digital evidence* (PhD thesis, University of Wollonong 2009) 251-252, abbreviated as Maghaireh *Jordanian cybercrime investigations*

Malcolm J *Multi-stakeholder governance and the Internet Governance Forum* (Terminus Press Australia 2008) 29-356, abbreviated as Malcolm *Multi stakeholder*

Malek A, Carbone F and Alder J “Community engagement, rural institutions and rural tourism business in developing countries” in Oriade A and Robinson P (eds)

Rural tourism and enterprise: Management, marketing and sustainability (Cabi Wallingford 2017) 145-157

Maness RC and Valeriano B (eds) *Russia's coercive diplomacy: Energy, cyber, and maritime policy* (Palgrave Macmillan Publication Hsmpshire 2015) 45-84

Marcum CD, Higgins GE and Tewksbury R "Doing time for cyber crime: An examination of the correlates of sentence length in the United States" (2011) *International Journal of Cyber Criminology* 824-835

Marinez JL *The link between poverty and crime: Utilizing Ruby Payne's framework of poverty* (MSc dissertation, Texas State University 2013) 2

Marler SL "The Convention on Cyber-Crime: Should the United States ratify?" (2002) *New England Law Review*

Matsueda RL "Social structure, culture, and crime: Assessing Kornhauser's challenge to criminology" in Cullen FT *et al Challenging criminological theory: The legacy of Ruth Rosner Kornhauser* (Routledge Publishers New York 2015) 117-143, abbreviated as Matsueda *Social structure*

Maxeiner JR "Uniform law and its impact on national laws limits and possibilities" in *United States of America national report* (papers delivered at the Intermediary Congress of the International Academy of Comparative Law 13-15 November 2009, Mexico City) 1-46

Mazar H *Radio spectrum management: Policies, regulations and techniques* (John Wiley Chichester 2016) 112-148

Mehta D "Economic crime in a globalizing society: Its impact on the sound development of the state − An indian perspective" in *Economic crime in a globalizing society − Its impact on the sound development of the state* (Papers delivered at the 126th Senior Seminar of United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI) 13 January-12 February 2004, Tokyo, Japan) 71-84, abbreviated as Mehta *Economic crime*

Mooney LA, Knox D and Schacht C *Understanding social problems* (Wadsworth Cengage Belmont 2013) 232-263

Moses LB "*Sui generis* rules" in Marchant GE, Allenby BR and Herkert JR (eds) *The growing gap between emerging technologies and legal-ethical oversight: The pacing problem* (Dordrecht Springer 2011) 77-93

Murray A *The regulation of cyberspace: Control in the online environment* (Routledge-Cavendish New York 2007) 91

Nadelmann EA *Cops across borders: The internationalization of US criminal law enforcement* (Pennsylvania State University Press Pennsylvania 1997) 313-394, abbreviated as Nadelmann *Cops across borders*

Nemerofsky J "The crime of 'interruption of computer services to authorized users': Have you ever heard of it?" (2000) *Richmond Journal of Law and Technology,* abbreviated as Nemerofsky 2000 *Richmond JLT*

Nicholls C *et al Nicholls, Montgomery, and Knowles on the law of extradition and mutual assistance* (Oxford University Press Oxford 2013) 112

Null L and Lobur J *The essentials of computer organization and architecture* (Jones and Bartlett Publishers Sudbury 2006)

Nzarga FD "Appraisal of human rights non-governmental organizations (NGOs) in Nigeria" (2014) *Journal of Law, Policy and Globalization* 148-151, abbreviated as *Appraisal* 2014 *Journal LPG*

Obamwonyi SE and Aibieyi S "Public policy failures in Nigeria: Pathway to underdevelopment" (2014) *Public Policy and Administration Research Journal* 38-42

Odionikhere P *Bringing down this house* (Lit verlag Berlin 2008) 102-109, abbreviated as Odionikhere *Bringing down*

Ogwezzy MC "Cyber crime and the proliferation of yahoo addicts in Nigeria" (2012) *AGORA International Journal of Juridical Sciences* 86-102, abbreviated as Ogwezzy *Cyber crime* 2012 *AGORA IJJS*

Okeke VOS "Pressure groups and policy process in Nigeria: A case of fourth republic" (2014) *Global Advanced Research Journal of Social Science* 15-24, abbreviated as Okeke *Pressure groups* 2014 *Global ARJSS*

Oladele B “Weak institutions make corruption thrive” *The Nation Nigeria* 21 February 2016

Omoniyi MBI “The role of education in poverty alleviation and economic development: A theoretical perspective and counselling implications” (2013) *British Journal of Arts and Social Sciences* 176-185

Omotor DG “Socio-economic determinants of crime in Nigeria” (2009) *Pakistan Journal of Social Sciences* 54-59

Onyekwere J “Cybercrimes Act 2015 and the need for further amendments” *The Guardian Newspaper* 24 August 2015

Oriola TA “Advance fee fraud on the internet: Nigeria’s regulatory response” (2005) *Computer Law and Security Report* 237-248

Oster J *Media freedom as a fundamental right* (Cambridge University Press Cambridge 2015) 230

Pakalniškis S *What factors explain why there is not a common and comprehensive global response to cyber threats?* (LLM dissertation, Leiden University 2012) 35

Pal LA “Governing the electronic commons: Globalization, legitimacy, autonomy and the internet” in Bernstein S and Coleman WD (eds) *Unsettled legitimacy: Political community, power, and authority in a global era* (UBC Press Vancouver 2009) 280-299, abbreviated as Pal *Governing the electronic commons*

Palmer A “A model framework for successful cybersecurity capacity building” (2016) *Journal of Internet Law* 15-19, abbreviated as Palmer *A model framework* 2016 *Journal IL*

Park YJ *The political economy of country code top level domains* (ProQuest Ann Arbor 2008) 156

Parker D *Computer abuse perpetrators and vulnerabilities of computer systems in national computer conference* (ACM New York 1976)

Parker DB *Fighting computer crime – A new framework for protecting information* (Wiley Computer New York 1998) 27-55, abbreviated as Parker *Fighting computer crime*

Pratt TC, Gau JM and Franklin TW (eds) *Key ideas in criminology and criminal justice* (Sage Publications Los Angeles 2011) 55- 69, abbreviated as Pratt, Gau and Franklin *Key ideas*

Price ME and Verhulst SG *Self-regulation and the internet* (Kluwer The Hague 2005) 1-27, abbreviated as Price and Verhulst *Self regulation*

Putnam TL and Elliot DD "International responses to cyber crime" in Sofaer AD and Goodman SE (eds) *The transnational dimension of cyber crime* (Hoover Stanford 2001) 35-67, abbreviated as Putnam and Elliott *International responses*

Quarshie HO and Martin-Odoom AM "Fighting cybercrime in Africa" (2012) *Computer Science and Engineering Journal*

Rasch MD "Criminal law and the internet" in Ruh JF (ed) *The internet and business: A lawyer's guide to the emerging legal issues* (1996) *Journal of the Computer Law Association* 141-148, abbreviated as Rasch *Criminal law* 1996 *Journal CLA*

Rawal R "Danger mouse? The growing threat of cyberterrorism" in Nixon PG and Koutrakou VN (eds) *E-government in Europe: Re-booting the state* (Routledge Publication New York 2007) 54

Rayes A and Salam S *Internet of things from hype to reality: The road to digitization* (Springer Publishers Cham 2017)

Rezek JF "Reciprocity as a basis of extradition" (1982) *British Yearbook Of International Law* 171-203

Samans R, Schwab K and Malloch-Brown M (eds) *Everybody's business: Strengthening international cooperation in a more interdependent world* (World Economic Forum Geneva 2010) 19-44

Saunders KM *Practical internet law for business* (Artech House Norwood 2001)

Schinder DL and Cross M *Scene of the cybercrime* (Syngress Burlington 2008) 1-39, abbreviated as Schinder and Cross *Scene*

Schweighofer E “Roles and perspectives of ICANN” in Benedek W, Bauer V and Kettemann MC (eds) *Internet governance and the information society: Global perspectives and European dimensions* (Eleven International Publishing Utrecht 2008) 79-90, abbreviated as Schweighofer *ICANN*

Sen ON *Criminal justice responses to emerging computer crime problems (*MSc dissertation, University of North Texas 2001) 48-50

Shalhoub ZK and Al Qasimi SL *Cyber law and cyber security in developing and emerging economies* (Edward Elgar Cheltenham 2010) 1-29

Sharma V, Varshney M and Sharma S. *Design and implementation of operating system* (University Science Press New Delhi 2010)

Shinder DL and Tittel E *Scene of the cybercrime* (Syngress Burlington 2002)

Sieber U *The international emergence of criminal information law (LusInformationis)* (Heymanns Cologne 1992) 5

Sliedregt E and Stoitchkova D “International criminal law” in Joseph S and McBeth A (eds) *Research handbook on international human rights law* (Edward Elgar Cheltenham 2010) 241-271

Smith RG, Grabosky P and Urbas G *Cyber criminals on trial* (Cambridge University Press Cambridge 2004) 48-60, abbreviated as Smith, Grabosky and Urbas *Cyber criminals on trial*

Snail S “Cyber crime in South Africa – Hacking, cracking, and other unlawful online activities” (2009) *Journal of Information Law and Technology* 1-13, abbreviated as Snail *Cyber crime* 2009 *Journal ILT*

Solum LB “Models of internet governance” in Bygrave LA and Bing J (eds) *Internet governance: Infrastructure and institutions* (Oxford University Press Oxford 2009) 48-91, abbreviated as Solum *Models*

Song Richardson L “Convicting the innocent in transnational criminal cases: A comparative institutional analysis approach to the problem” (2008) *Berkeley Journal of International Law* 79-82, abbreviated as Song *Convicting the innocent Berkeley Journal IL*

Souter D “Louder voices and the international debate on developing country participation in ICT decision making” in Drake WJ and Wilson EJ *Governing global electronic networks: International perspectives on policy and power* (MIT Press Massachusetts 2008) 429-462

Spiegel HW (ed) *The growth of economic thought* (Duke University Press Durham 1991) 23-46

Sterling-Folker J “Neoliberalism” in Dunne T, Kurki M & Smith S (eds*) International relations theories: Discipline* (Oxford University Press Oxford 2010) 114-131, abbreviated as Sterling-Folker *Neoliberalism*

Stigall DE “Ungoverned spaces, transnational crime, and the prohibition on extraterritorial enforcement jurisdiction in international law” (2013) *Notre Dame Journal of International and Comparative Law* 1-50, abbreviated as Stigall *Ungoverned spaces* 2013 *Notre Dame JICL*

Subramanian R “Internet governance: A developing country perspective” (2013) *Communications of the International Information Management Association* 9-10, Subramanian *Internet governance* 2013 *Communications of the IIMA*

Sukhai NB “Hacking and cybercrime” (Proceedings of the 1st annual conference on information security development, 17-18 September 2004, Kennesaw) 128-132

Sutton R *The policy process: An overview* (Overseas Development Institute working paper) (Chameleon Press London 1999) 22-29

Terwange C “Is a global data protection regulatory model possible?” in Gutwirth S *et al* (eds) *Reinventing data protection* (Springer SBM Heidelberg 2009) 175-190, abbreviated as Terwange *Is a global data protection regulatory model possible*

Totty R and Hardcastle A “Computer-related crime” in Edwards C, Savage N and Walden I (eds) *Information technology and the law* (Macmillan Basingstoke 1990) 142-172

Ukwaeze ER and Nwosu EO “Does higher education reduce poverty among youths in Nigeria?” (2014) *Asian Economic and Financial Review* 1-19

United States Congressional Serial Set, Serial No 15006, Senate Treaty Documents No 9-12 (United States Government Printing office Washington 2006) 333-335

Van der Merwe DP "Computer crime – Recent national and international developments" (2003) *THRHR* 31

Vatis MA "The Council of Europe Convention on Cybercrime" in *Proceedings of a workshop on deterring cyberattacks: Informing strategies and developing options for US Policy* (Papers delivered at Committee on Deterring Cyberattacks: Informing strategies and developing options for US Policy 10-11 June 2010, Washington DC) 207-226

Wacks R *Personal information privacy and the law* (Claredon Press Oxford 1989) 25

Wada F and Odulaja GO "Assessing cyber crime and its impact on e-banking in Nigeria using social theories" (2012) *African Journal of Computer and ICT* 69-82

Walden I *Computer crimes and digital investigations* (Oxford University Press New York 2007) 16-19, abbreviated as Walden *Computer crimes*

Wall D "Maintaining order and law in the internet" in *Crime and the internet* (Routledge New York 2001) 167-183

Wall D "Policing cybercrimes: Situating the public police in network of security within cyberspace" in Palmer D, Berlin MM and Das DK (eds) *Global environment of policing* (CRC Press Boca Raton 2012)

Wall DS *Cybercrime: The transformation of crime in the information age* (Polity Press Cambridge 2007) 8-29, abbreviated as Wall *Cybercrime*

Watney M "The way forward in addressing cybercrime regulation on a global level" (2012) *Journal of Internet Technology and Secured Transactions* 61-67

Weber RH *Shaping internet governance: Regulatory challenges* (Springer Heidelberg 2010) 39-72, abbreviated as Weber *Shaping internet governance*

Westby JR (ed) *International guide to cyber security* (ABA Chicago 2004) 35-102, abbreviated as Westby *International guide to cyber security*

Wickremasinghe C *The jurisdictional immunities of international organisations and their officials* (PhD thesis, London School of Economics 2003) 7-8

Wilson SH (ed) *The US justice system: Law and constitution in early America* (ABC-CLIO Publishers California 2012) 399

Wu C and Irwin JD *Introduction to computer networks and cybersecurity* (CRC Press New York 2013) 95-97

Xue H "Multinationals' global governance on the internet" in Rosen J (ed) *Individualism and collectiveness in intellectual property law* (Edward Elgar Cheltenham 2012) 269

Yasin M "Global nature of computer crimes and the Convention on Cybercrime" (2006) *Ankara Law Review* 129-142, abbreviated as Yasin *Global nature* 2006 *Ankara LR*

Yar M "The novelty of cybercrime" (2005) *European Journal of Criminology* 407-427

Yar M *Cybercrime and society* (Sage Publications London 2013) 142-155, abbreviated as Yar *Cybercrime*

Yearbook: 1985 vol. XVI (United Nations Publication New York 1988) 47

Zakaras M "International computer crimes" (2001) *Revue Internationale de Droit Penal* 813-829

Zartner D *Courts, codes, and custom: Legal tradition and state policy toward international human rights and environmental law* (Oxford University Press Oxford 2014) 16-46

ONLINE (INTERNET) SOURCES

Adepoju P "Illiteracy: Causes, effects and solutions" http://iluvjetnoise.blogspot.com/2012/08/illiteracy-causes-effects-solutions.html (Date of use: 16 April 2015), abbreviated as Adepoju http://iluvjetnoise.blogspot.com/2012/08/illiteracy-causes-effects-solutions.html (Date of use: 16 April 2015)

Adibe J "Pervasive kidnapping in Nigeria: Symptom of a failing State?" http://www.hollerafrica.com/showArticle.php?artId=304&catId=&page=1 (Date of use: 20 January 2015), abbreviated as Adibe http://www.hollerafrica.com/showArticle.php?artId=304&catId=&page=1 (Date of use: 20 January 2015)

Agbaje O "Kidnappers to target politicians – Ozekhome" http://sunnewsonline.com/new/?p=38186 (Date of use: 20 January 2015), Agbaje http://sunnewsonline.com/new/?p=38186 (Date of use: 20 January 2015)

Aginam E "FG trains legal officers on forensic evidence" http://www.vanguardngr.com/2012/11/fg-trains-legal-officers-on-forensic-evidence/ (Date of use: 24 February 2013); abbreviated as Aginam http://www.vanguardngr.com/2012/11/fg-trains-legal-officers-on-forensic-evidence/ (Date of use: 24 February 2013)

All Africa Newspaper http://allafrica.com/stories/201204170035.html (Date of use: 24 April 2012)

Alvestrand H "A Mission statement for the IETF" https://www.ietf.org/rfc/rfc3935.txt (Date of use: 2 January 2016), Alvestrand https://www.ietf.org/rfc/rfc3935.txt (Date of use: 2 January 2016)

Alvestrand H "An IESG Charter" https://www.ietf.org/rfc/rfc3710.txt (Date of use: 24 December 2015), abbreviated as Alvestrand https://www.ietf.org/rfc/rfc3710.txt (Date of use: 24 December 2015)

Ameer-Mia F and Pienaar C "South Africa: Cybersecurity 2019" https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/south-africa (Date of use: 18 September 2019), abbreviated as Ameer-Mia and Pienaar

https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/south-africa (Date of use: 18 September 2019)

Ang PH "Self-regulation after WGIG" http://www.wgig.org/docs/book/Peng_Hwa_Ang%20.pdf (Date of use: 20 September 2015), abbreviated as Ang http://www.wgig.org/docs/book/Peng_Hwa_Ang%20.pdf (Date of use: 20 September 2015)

Aquino M "Thailand's strict *Lese Majeste* laws - The Thai reverence for the King" http://goseasia.about.com/od/thaipeopleculture/a/lesemajeste.htm (Date of use: 8 March 2013), abbreviated as Aquino http://goseasia.about.com/od/thaipeopleculture/a/lesemajeste.htm (Date of use: 8 March 2013)

Archick K "Cybercrime: The Council of Europe Convention" http://fpc.state.gov/documents/organization/58265.pdf (Date of use: 1 January 2014), abbreviated as Archick http://fpc.state.gov/documents/organization/58265.pdf (Date of use: 1 January 2014)

Arkko J "Diversity" https://www.ietf.org/blog/2013/04/diversity/ (Date of use: 4 January 2016), abbreviated as Arkko https://www.ietf.org/blog/2013/04/diversity/ (Date of use: 4 January 2016)

Ashford W "Cyber skills a top challenge, says UK police cyber crime unit" http://www.computerweekly.com/news/1280094331/Cyber-skills-a-top-challenge-says-UK-police-cyber-crime-unit (Date of use: 25 March 2013), abbreviated as Ashford http://www.computerweekly.com/news/1280094331/Cyber-skills-a-top-challenge-says-UK-police-cyber-crime-unit (Date of use: 25 March 2013)

Ashford W "Financial services sector attracts most cyber crime, says PwC study" http://www.computerweekly.com/news/2240215532/Financial-services-sector-attract-most-cyber-crime-says-PwC-study (Date of use: 21 March 2015), abbreviated as Ashford http://www.computerweekly.com/news/2240215532/Financial-services-sector-attract-most-cyber-crime-says-PwC-study (Date of use: 21 March 2015)

Baird Z and Verhulst S "A new model for global internet governance" http://www.markle.org/sites/default/files/ahs_global_internet_gov.pdf (Date of use: 17 September 2016), abbreviated as Baird and Verhulst http://www.markle.org/sites/default/files/ahs_global_internet_gov.pdf (Date of use: 17 September 2016)

Baldwin DA "Power of positive sanctions" http://www.princeton.edu/~dbaldwin/selected%20articles/Baldwin%20(1971)%20The%20Power%20of%20Positive%20Sanctions.pdf (Date of use: 4 April 2015), abbreviated as Baldwin http://www.princeton.edu/~dbaldwin/selected%20articles/Baldwin%20(1971)%20The%20Power%20of%20Positive%20Sanctions.pdf (Date of use: 4 April 2015)

Ballard "UN rejects international cybercrime treaty" http://www.computerweekly.com/news/1280092617/UN-rejects-international-cybercrime-treaty (Date of use: 10 October 2013), abbreviated as Ballard http://www.computerweekly.com/news/1280092617/UN-rejects-international-cybercrime-treaty (Date of use: 10 October 2013)

Bande LC "The making of cybercrime legislation in Malawi: A comparative analysis of Malawi's proposed cybercrime law against international standards and best practices" https://lirias.kuleuven.be/bitstream/123456789/404618/1/The+Making+of+Cybercrime+Legislation+in+Malawi+Pdf.pdf (Date of use: 12 September 2013), abbreviated as Bande https://lirias.kuleuven.be/bitstream/123456789/404618/1/The+Making+of+Cybercrime+Legislation+in+Malawi+Pdf.pdf (Date of use: 12 September 2013)

Barret A "NRO-NC / ASO-AC Address Council Report" https://internetsummitafrica.org/images/AIS14_slides/Alan_Barrett-nro-nc.afrinic20_201406.pdf (Date of use: 30 January 2016), abbreviated as Barret https://internetsummitafrica.org/images/AIS14_slides/Alan_Barrett-nro-nc.afrinic20_201406.pdf (Date of use: 30 January 2016)

Bartlett D "Talking points – Cyber crime: A growing threat to global companies" http://rsmi.com/publications/talking-points/691-talking-points-cyber-crime-a-growing-threat-to-global-companies.html (Date of use: 21 March 2015),

abbreviated as Bartlett http://rsmi.com/publications/talking-points/691-talking-points-cyber-crime-a-growing-threat-to-global-companies.html (Date of use: 21 March 2015)

Baryun A "Re: [Diversity] Diversity team wiki (was 'Re: Questions from USA Today" https://www.ietf.org/mail-archive/web/diversity/current/msg00598.html (Date of use: 4 January 2016), abbreviated as Baryun https://www.ietf.org/mail-archive/web/diversity/current/msg00598.html (Date of use: 4 January 2016)

Becker R "How many countries in Africa? How hard can the question be?" http://africacheck.org/reports/how-many-countries-in-africa-how-hard-can-the-question-be/ (Date of use: 29 August 2013), abbreviated as Becker http://africacheck.org/reports/how-many-countries-in-africa-how-hard-can-the-question-be/ (Date of use: 29 August 2013)

Belenko A "Breakthrough in password recovery: Thunder tables and GPUs" http://www.elcomsoft.com/presentations/elcomsoft_company_product_presentation_2009.pdf (Date of use: 11 February 2013), abbreviated as Belenko http://www.elcomsoft.com/presentations/elcomsoft_company_product_presentation_2009.pdf (Date of use: 11 February 2013)

Bellia PL "Chasing bits across borders" http://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1430&context=law_faculty_scholarship (Date of use: 15 February 2014), abbreviated as Bellia PL http://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1430&context=law_faculty_scholarship (Date of use: 15 February 2014)

Bellinger G, Castro D and Mills A "Data, information, knowledge, and wisdom" http://www.systems-thinking.org/dikw/dikw.htm (Date of use: 28 April 2012), abbreviated as Bellinger, Castro and Mills http://www.systems-thinking.org/dikw/dikw.htm (Date of use: 28 April 2012)

Bird JA "Addresses of W3C offices" https://www.w3.org/Consortium/Offices/staff (Date of use: 23 January 2016), abbreviated as Bird https://www.w3.org/Consortium/Offices/staff (Date of use: 23 January 2016)

Birkenbihl K "Roles of W3C offices" https://www.w3.org/Consortium/Offices/role.html (Date of use: 23 January 2016), abbreviated as Birkenbihl https://www.w3.org/Consortium/Offices/role.html (Date of use: 23 January 2016)

Bose SS "Nagpur rural police gets modern cyber cell" http://timesofindia.indiatimes.com/city/nagpur/Nagpur-rural-police-gets-modern-cyber-cell/articleshow/18466610.cms (Date of use: 15 February 2013), abbreviated as Bose http://timesofindia.indiatimes.com/city/nagpur/Nagpur-rural-police-gets-modern-cyber-cell/articleshow/18466610.cms (Date of use: 15 February 2013)

Brain M and Crawford S "How domain name servers work" http://computer.howstuffworks.com/dns.htm (Date of use: 26 September 2015), abbreviated as Brain and Crawford http://computer.howstuffworks.com/dns.htm (Date of use: 26 September 2015)

Brenner S "Cybercrime investigation and prosecution: the role of penal and procedural Law" http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan003073.pdf (Date of use: 25 March 2013), abbreviated as Brenner http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan003073.pdf (Date of use: 25 March 2013)

Brenner S and Goodman M "Cybercrime: The need to harmonize national penal and procedural laws" http://www.isrcl.org/Papers/Brenner.pdf (Date of use: 14 July 2013), abbreviated as Brenner and Goodman http://www.isrcl.org/Papers/Brenner.pdf (Date of use: 14 July 2013)

Brewster T "The rush to fix Britain's cyber police" http://www.techweekeurope.co.uk/news/fixing-cyber-police-security-pceu-soca-national-crime-agency-106466 (Date of use: 17 April 2013), abbreviated as Brewster http://www.techweekeurope.co.uk/news/fixing-cyber-police-security-pceu-soca-national-crime-agency-106466 (Date of use: 17 April 2013)

Briggs S "Important theories in criminology: why people commit crime" http://www.dummies.com/how-to/content/important-theories-in-criminology-why-people-commi.html (Date of use: 11 January 2015), abbreviated as Briggs http://www.dummies.com/how-to/content/important-theories-in-criminology-why-people-commi.html (Date of use: 11 January 2015)

Bugg D "Commonwealth Director of Public Prosecutions (2002-2003 Annual report)" http://www.cdpp.gov.au/wp-content/uploads/CDPP-Annual-Report-2002-2003.pdf (Date of use: 16 April 2014), abbreviated as Bugg http://www.cdpp.gov.au/wp-content/uploads/CDPP-Annual-Report-2002-2003.pdf (Date of use: 16 April 2014)

Bui S, Enyeart M and Luong J "Issues in computer forensics" http://www.cse.scu.edu/~jholliday/COEN150sp03/projects/Forensic%20Investigation.pdf (Date of use: 10 March 2013), abbreviated as Bui, Enyeart and Luong http://www.cse.scu.edu/~jholliday/COEN150sp03/projects/Forensic%20Investigation.pdf (Date of use: 10 March 2013)

Burrows T "SA fails on forensic readiness" http://www.itweb.co.za/?id=62964:SA-fails-on-forensic-readiness (Date of use: 16 April 2014), abbreviated as Burrows http://www.itweb.co.za/?id=62964:SA-fails-on-forensic-readiness (Date of use: 16 April 2014)

Butler S "Tesco and rivals turn against huge stores as internet shopping takes over" http://www.guardian.co.uk/business/2012/mar/04/online-shopping-changes-hypermarket-strategy (Date of use: 13 August 2012), abbreviated as Butler http://www.guardian.co.uk/business/2012/mar/04/online-shopping-changes-hypermarket-strategy (Date of use: 13 August 2012)

Calandro E, Gillwald A and Zingales N "Mapping multistakeholderism in internet governance: Implications for Africa" http://www.researchictafrica.net/docs/Mapping%20multistakeholderism%20in%20internet%20governance%20draft%20final%2004082013.pdf (Date of use: 28 December 2015), abbreviated as Calandro, Gillwald and Zingales http://www.researchictafrica.net/docs/Mapping%20multistakeholderism%20in%20internet%20governance%20draft%20final%2004082013.pdf (Date of use: 28 December 2015)

Carlson N "How many users does Twitter really have" http://articles.businessinsider.com/2011-03-31/tech/30049251_1_twitter-

accounts-active-twitter-user-simple-answer (Date of use: 13 April 2012), abbreviated as Carlson http://articles.businessinsider.com/2011-03-31/tech/30049251_1_twitter-accounts-active-twitter-user-simple-answer (Date of use: 13 April 2012)

Castro D and McQuinn A "Cross-border data flows enable growth in all industries" http://www2.itif.org/2015-cross-border-data-flows.pdf (Date of use: 17 May 2015), abbreviated as Castro and McQuinn http://www2.itif.org/2015-cross-border-data-flows.pdf (Date of use: 17 May 2015)

CBC Digital archives http://archives.cbc.ca/science_technology/computers/clips/4182/ (Date of use: 02 April 2012)

Centre for problem-oriented policing
http://www.popcenter.org/problems/child_pornography/2 (Date of use: 13 April 2012)

Chalfant M "Cyber crime costs global economy $600B annually"
http://thehill.com/policy/cybersecurity/374854-cybercrime-costs-global-economy-600-billion-annually-experts-estimate (Date of use: 14 September 2018), abbreviated as Chalfant http://thehill.com/policy/cybersecurity/374854-cybercrime-costs-global-economy-600-billion-annually-experts-estimate (Date of use: 14 September 2018)

Chapman C "South Africa welcomes new cybercrime legislation"
https://portswigger.net/daily-swig/south-africa-welcomes-new-cybercrime-legislation (Date of use: 5 October 2019), abbreviated as Chapman https://portswigger.net/daily-swig/south-africa-welcomes-new-cybercrime-legislation (Date of use: 5 October 2019)

Chawki M "A critical look at the regulation of cybercrime" http://www.droit-tic.com/pdf/chawki4.pdf (Date of use: 24 April 2012), Chawki http://www.droit-tic.com/pdf/chawki4.pdf (Date of use: 24 April 2012)

Chik WB "Challenges to criminal law making in the new global information society: A critical comparative study of the adequacies of computer-related criminal legislation in the United States, the United Kingdom and Singapore" www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc (Date of use: 6 November 2012), abbreviated as Chik www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc (Date of use: 6 November 2012)

Child exploitation and online protection Command http://ceop.police.uk/About-Us/ (Date of use: 05 February 2013)

Clarke R "The OECD data protection guidelines: A template for evaluating information privacy law and proposals for information privacy law" http://www.rogerclarke.com/DV/PaperOECD.html (Date of use: 17 March 2015), abbreviated as Clarke http://www.rogerclarke.com/DV/PaperOECD.html (Date of use: 17 March 2015)

Clayton R "UK law and the internet" http://www.cl.cam.ac.uk/~rnc1/notes/EL09_UKLaw.pdf (Date of use: 3 January 2013), abbreviated as Clayton http://www.cl.cam.ac.uk/~rnc1/notes/EL09_UKLaw.pdf (Date of use: 3 January 2013)

Cluley G "Facebook donates $250 000 to help fight cybercrime (using money acquired from spammers)" http://nakedsecurity.sophos.com/2012/10/23/facebook-fight-cybercrime/ (Date of use: 18 April 2013), abbreviated as Cluley http://nakedsecurity.sophos.com/2012/10/23/facebook-fight-cybercrime/ (Date of use: 18 April 2013)

Cobb M "International computer crime requires an international response" http://www.computerweekly.com/tip/International-computer-crime-requires-an-international-response (Date of use: 04 November 2012), abbreviated as Cobb http://www.computerweekly.com/tip/International-computer-crime-requires-an-international-response (Date of use: 04 November 2012)

Country Code Names Supporting Organisation http://ccnso.icann.org/about (Date of use: 5 October 2015)

Crossman A "Labelling theory" http://sociology.about.com/od/L_Index/g/Labeling-Theory.htm (Date of use: 11 January 2015), abbreviated as Crossman http://sociology.about.com/od/L_Index/g/Labeling-Theory.htm (Date of use: 11 January 2015)

Cunningham M "Economic inequality: Differences in developed and developing nations" http://study.com/academy/lesson/economic-inequality-differences-in-developed-and-developing-nations.html (Date of use: 27 November 2015), abbreviated as

Cunningham http://study.com/academy/lesson/economic-inequality-differences-in-developed-and-developing-nations.html (Date of use: 27 November 2015)

Cushing T "Abuse of India's Information Technology Act results in India's first arrested Twitter user" http://www.techdirt.com/articles/20121106/16174720954/abuse-indias-information-technology-act-results-indias-first-arrested-twitter-user.shtml (Date of use: 14 March 2013), abbreviated as Cushing http://www.techdirt.com/articles/20121106/16174720954/abuse-indias-information-technology-act-results-indias-first-arrested-twitter-user.shtml (Date of use: 14 March 2013)

Dahinden M "Democracy promotion at a local level: Experiences, perspectives and policy of Swiss international cooperation" http://poldev.revues.org/1517#tocfrom2n2 (Date of use: 29 May 2017), abbreviated as Dahinden http://poldev.revues.org/1517#tocfrom2n2 (Date of use: 29 May 2017)

Daily Times Newspaper http://www.dailytimes.com.ng/article/new-law-gives-life-jail-term-kidnappers (Date of use: 3 March 2013), abbreviated as http://www.dailytimes.com.ng/article/new-law-gives-life-jail-term-kidnappers (Date of use: 3 March 2013)

Dalton W "Cyber-crime policing completely inadequate, says ex-Scotland Yard detective" http://www.itproportal.com/2012/11/22/cyber-crime-policing-completely-inadequate-says-ex-scotland-yard-detective/ (Date of use: 25 March 2013), abbreviated as Dalton http://www.itproportal.com/2012/11/22/cyber-crime-policing-completely-inadequate-says-ex-scotland-yard-detective/ (Date of use: 25 March 2013)

DeBruin L "FBI, police go high-tech to fight crime" http://usatoday30.usatoday.com/news/nation/2011-07-30-police-fbi-digital-detectives_n.htm (Date of use: 11 February 2013), abbreviated as DeBruin http://usatoday30.usatoday.com/news/nation/2011-07-30-police-fbi-digital-detectives_n.htm (Date of use: 11 February 2013)

Doria A "The IETF and the multistakeholder model" https://docs.google.com/document/d/1x-WIVPfk3FZ9NKLeDJuQlk5WqG-HSVmm56c028D3xGg/edit?pref=2&pli=1# (Date of use: 4 January 2016), abbreviated as Doria https://docs.google.com/document/d/1x-

WlVPfk3FZ9NKLeDJuQlk5WqG-HSVmm56c028D3xGg/edit?pref=2&pli=1# (Date of use: 4 January 2016)

Doyle C "Cybercrime: An overview of 18 USC 1030 and related federal criminal laws" http://www.fas.org/sgp/crs/misc/97-1025.pdf (Date of use: 2 December 2012), abbreviated as Doyle http://www.fas.org/sgp/crs/misc/97-1025.pdf (Date of use: 2 December 2012)

Dunn M "A comparative analysis of cybersecurity initiatives worldwide" http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf (Date of use: 2 March 2012), abbreviated as Dunn http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf (Date of use: 2 March 2012)

Durch WJ "United Nations police evolution, present capacity and future tasks" http://www3.grips.ac.jp/~pinc/data/10-03.pdf (Date of use: 19 July 2014), abbreviated as Durch http://www3.grips.ac.jp/~pinc/data/10-03.pdf (Date of use: 19 July 2014)

Dybwad B "2 year-old finds iPad easy to use" http://mashable.com/2010/04/06/2-year-old-girl-uses-ipad/ (Date of use: 24 April 2012), abbreviated as Dybwad http://mashable.com/2010/04/06/2-year-old-girl-uses-ipad/ (Date of use: 24 April 2012)

Dzidonu C and Quaynor NN "Broadening and enhancing the capacity of developing countries to effectively participate in the Global ICT Policy for a and the ICT for development (ICTfDev) Process" https://archive.icann.org/en/meetings/carthage/conceptpaper-carthage-globalict.pdf (Date of use: 22 July 2017), abbreviated as Dzidonu and Quaynor https://archive.icann.org/en/meetings/carthage/conceptpaper-carthage-globalict.pdf (Date of use: 22 July 2017)

Eagle N "How to make the internet free in developing countries" https://techcrunch.com/2015/06/01/how-to-make-the-internet-truly-free-in-developing-countries/ (Date of use: 24 July 2016), abbreviated as Eagle https://techcrunch.com/2015/06/01/how-to-make-the-internet-truly-free-in-developing-countries/ (Date of use: 24 July 2016)

Emm D "Cybercrime and the law: A review of UK computer crime legislation" http://www.securelist.com/en/analysis/204792064/Cybercrime_and_the_law_a_review_of_UK_computer_crime_legislation (Date of use: 21 December 2012), abbreviated as Emm http://www.securelist.com/en/analysis/204792064/Cybercrime_and_the_law_a_review_of_UK_computer_crime_legislation (Date of use: 21 December 2012)

Evans M "Fraud and cyber crime are now the country's most common offences" http://www.telegraph.co.uk/news/2017/01/19/fraud-cyber-crime-now-countrys-common-offences/ (Date of use: 4 November 2017), abbreviated as Evans http://www.telegraph.co.uk/news/2017/01/19/fraud-cyber-crime-now-countrys-common-offences/ (Date of use: 4 November 2017)

Ewelukwa N "Non-passage of cybercrime Bill decried" http://www.thisdaylive.com/articles/non-passage-of- cyber-crime-bill-decried/88750/ (Date of use: 8 January 2013), abbreviated as Ewelukwa http://www.thisdaylive.com/articles/non-passage-of- cyber-crime-bill-decried/88750/ (Date of use: 8 January 2013)

Ezugwu BN "Law on kidnapping: Matters arising" http://www.gamji.com/article8000/NEWS8473.htm (Date of use: 8 January 2013), abbreviated as Ezugwu http://www.gamji.com/article8000/NEWS8473.htm (Date of use: 8 January 2013)

Fafinski S, Dutton B and Margetts H "Mapping and measuring cybercrime" www.law.leeds.ac.uk/assets/files/staff/FD18.pdf (Date of use: 31 March 2013), abbreviated as Fafinski, Dutton and Margetts www.law.leeds.ac.uk/assets/files/staff/FD18.pdf (Date of use: 31 March 2013)

Fakoya G "The police and the Nigerian public" *Sahara Reporters E-Newspaper* 16 February 2012 http://saharareporters.com/2012/02/16/police-and-nigerian-public (Date of use: 18 October 2014), abbreviated as Fakoya http://saharareporters.com/2012/02/16/police-and-nigerian-public (Date of use: 18 October 2014)

Finklea KM "The interplay of borders, turf, cyberspace, and jurisdiction: Issues confronting US law enforcement" http://www.fas.org/sgp/crs/misc/R41927.pdf (Date of use: 3 March 2014), abbreviated as Finklea http://www.fas.org/sgp/crs/misc/R41927.pdf (Date of use: 3 March 2014)

Foldvary FE “Ignorance, apathy, and greed” http://starbase.airweb.net/lifestyle/ignorance_apathy.html (Date of use: 31 May 2015), abbreviated as Foldvary http://starbase.airweb.net/lifestyle/ignorance_apathy.html (Date of use: 31 May 2015)

Friedman IN “National cyber security: FBI unveils next generation cyber initiative” http://www.examiner.com/article/national-cyber-security-fbi-unveils-next-generation-cyber-initiative (Date of use: 8 February 2013), abbreviated as Friedman http://www.examiner.com/article/national-cyber-security-fbi-unveils-next-generation-cyber-initiative (Date of use: 8 February 2013)

Galvin J “IAB and IESG selection, confirmation, and recall process: Operation of the nominating and recall committees” https://www.ietf.org/rfc/rfc2727.txt (Date of use: 2 January 2016), abbreviated as Galvin https://www.ietf.org/rfc/rfc2727.txt (Date of use: 2 January 2016)

Gann T “McAfee Executive on measuring the cost of cybercrime: Why it matters” http://www.hstoday.us/columns/critical-issues-in-national-cybersecurity/blog/mcafee-executive-on-measuring-the-cost-of-cybercrime-why-it-matters/c79246f8b6f0cf029edd2ff79348e349.html (Date of use: 18 April 2015), abbreviated as Gann http://www.hstoday.us/columns/critical-issues-in-national-cybersecurity/blog/mcafee-executive-on-measuring-the-cost-of-cybercrime-why-it-matters/c79246f8b6f0cf029edd2ff79348e349.html (Date of use: 18 April 2015)

Garson P “Cybercriminals find wonderland in developing countries” https://www.opendemocracy.net/opensecurity/philippa-garson/cybercriminals-find-wonderland-in-developing-countries (Date of use: 20 January 2015), abbreviated as Garson https://www.opendemocracy.net/opensecurity/philippa-garson/cybercriminals-find-wonderland-in-developing-countries (Date of use: 20 January 2015)

Ghaziri H “Information technology in the banking sector: Opportunities, threats and strategies” http://ddc.aub.edu.lb/projects/business/it-banking.html (Date of use: 13 April 2012), abbreviated as Ghaziri http://ddc.aub.edu.lb/projects/business/it-banking.html (Date of use: 13 April 2012)

Gilbert K and Sookram S “The socio-economic determinants of violent crime in Jamaica” www.sta.uwi.edu/conferences/09/salises/documents/K%20Gilbert.pdf (Date of use: 17 January 2015), abbreviated as Gilbert and Sookram

www.sta.uwi.edu/conferences/09/salises/documents/K%20Gilbert.pdf (Date of use: 17 January 2015)

Gilwald A "Strengthening participation by developing countries in international decision-making: Case study of South Africa" https://www.wits.ac.za/media/migration/files/SACTOP.pdf (Date of use: 4 July 2016), abbreviated as Gilwald https://www.wits.ac.za/media/migration/files/SACTOP.pdf (Date of use: 4 July 2016)

Girard F "What can companies do to prevent cyber crime?" http://www.ehow.com/info_8152903_can-do-prevent-cyber-crime.html (Date of use: 16 August 2012), abbreviated as Girard http://www.ehow.com/info_8152903_can-do-prevent-cyber-crime.html (Date of use: 16 August 2012)

Golubev V "International cooperation in fighting cybercrime" http://www.crime-research.org/articles/Golubev0405/ (Date of use: 15 February 2014), abbreviated as Golubev http://www.crime-research.org/articles/Golubev0405/ (Date of use: 15 February 2014)

Goodwin B "Hightech is put on trial" http://www.computerweekly.com/feature/High-tech-crime-is-put-on-trial (Date of use: 5 February 2013), abbreviated as Goodwin http://www.computerweekly.com/feature/High-tech-crime-is-put-on-trial (Date of use: 5 February 2013)

Gordon S and Ford R "On the definition and classification of cybercrime" http://profs.sci.univr.it/~giaco/download/Watermarking-Obfuscation/cybercrime%20classification.pdf (Date of use: 24 April 2012), abbreviated as Gordon and Ford http://profs.sci.univr.it/~giaco/download/Watermarking-Obfuscation/cybercrime%20classification.pdf (Date of use: 24 April 2012)

Graham L "Cybercrime costs the global economy $450 billion: CEO" https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html (Date of use: 4 November 2017), abbreviated as Graham https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html (Date of use: 4 November 2017)

Greenspun P “Mobile phone as home computer” http://philip.greenspun.com/business/mobile-phone-as-home-computer (Date of use: 7 April 2012), abbreviated as Greenspun P “Mobile phone as home computer” http://philip.greenspun.com/business/mobile-phone-as-home-computer (Date of use: 7 April 2012)

Hagy DW “Investigative uses of technology: Devices, tools, and techniques” https://www.ncjrs.gov/pdffiles1/nij/213030.pdf (Date of use: 11 February 2013), abbreviated as Hagy https://www.ncjrs.gov/pdffiles1/nij/213030.pdf (Date of use: 11 February 2013)

Hakim S “World’s smallest cyber crime investigation device released by ASCL & Data64” http://cyberforensicsindia.blogspot.com/2010/08/worlds-smallest-cyber-crime.html (Date of use: 16 February 2013), abbreviated as Hakim http://cyberforensicsindia.blogspot.com/2010/08/worlds-smallest-cyber-crime.html (Date of use: 16 February 2013)

Harley B “A global convention on cybercrime?” http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/ (Date of use: 14 July 2013), abbreviated as Harley http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/ (Date of use: 14 July 2013)

Hickson N “ICANN response to internet governance consultation” https://ec.europa.eu/digital-agenda/en/content/icann-response-internet-governance-consultation (Date of use: 15 November 2015), abbreviated as Hickson https://ec.europa.eu/digital-agenda/en/content/icann-response-internet-governance-consultation (Date of use: 15 November 2015)

Hofmann J “Internet Corporation for Assigned Names and Numbers (ICANN)” http://www.giswatch.org/sites/default/files/gisw_icann_0.pdf (Date of use: 30 May 2016), abbreviated as Hofmann http://www.giswatch.org/sites/default/files/gisw_icann_0.pdf (Date of use: 30 May 2016)

Hossain J “View from the desk of the Internet Governance Secretariat” http://www.internetsociety.org/ur/node/380526 (Date of use: 2 August 2016), abbreviated as Hossain http://www.internetsociety.org/ur/node/380526 (Date of use: 2 August 2016)

Howe W “A brief history of the internet” http://www.walthowe.com/navnet/history.html (Date of use: 24 April 2012), abbreviated as Howe http://www.walthowe.com/navnet/history.html (Date of use: 24 April 2012)

Hubbard K “Protect your financial data from cyber criminals” http://www.bbc.com/capital/story/20141007-avoid-cyber-crime-in-90-seconds (Date of use: 30 March 2015), abbreviated as Hubbard http://www.bbc.com/capital/story/20141007-avoid-cyber-crime-in-90-seconds (Date of use: 30 March 2015)

IBN News India http://ibnlive.in.com/news/cyber-crime-police-station-shortstaffed/255424-60-119.html (Date of use: 15 February 2013)

Iferi B “New law gives life jail term to kidnappers” http://www.dailytimes.com.ng/article/new-law-gives-life-jail-term-kidnappers (Date of use: 3 March 2013), abbreviated as Iferi http://www.dailytimes.com.ng/article/new-law-gives-life-jail-term-kidnappers (Date of use: 3 March 2013)

Indian Economic Times Newspaper http://articles.economictimes.indiatimes.com/2009-03-30/news/28401922_1_cyber-terrorism-cybercrime-convention (Date of use: 19 October 2014)

International Centre for Missing and Exploited Children http://www.icmec.org/missingkids/servlet/NewsEventServlet?LanguageCountry=en_X1&PageId=4877 (Date of use: 9 March 2014)

International Monetary Fund http://www.ioha2012.net/?page_id=1945 (Date of use: 7 March 2013)

Iredia T “Who is crippling the EFCC” http://www.vanguardngr.com/2012/12/who-is-crippling-the-efcc/ (Date of use: 23 February 2013), abbreviated as Iredia http://www.vanguardngr.com/2012/12/who-is-crippling-the-efcc/ (Date of use: 23 February 2013)

Jahnke A "Alexey Ivanov and Vasiliy Gorshkov: Russian hacker roulette" http://www.csoonline.com/article/2118241/malware-cybercrime/alexey-ivanov-and-vasiliy-gorshkov--russian-hacker-roulette.html (Date of use: 22 April 2014), abbreviated as Jahnke http://www.csoonline.com/article/2118241/malware-cybercrime/alexey-ivanov-and-vasiliy-gorshkov--russian-hacker-roulette.html (Date of use: 22 April 2014)

Jian GU "Strengthening international cooperation and joining hands in fighting against transnational cybercrime" http://www.china.org.cn/business/2010Internetforum/2010-11/09/content_21306503.htm (Date of use: 20 May 2017), abbreviated as Jian http://www.china.org.cn/business/2010Internetforum/2010-11/09/content_21306503.htm (Date of use: 20 May 2017)

Jones Telecommunications and Multimedia Encyclopaedia http://www.dia.eui.upm.es/asignatu/sis_op1/comp_hd/comp_hd.htm (Date of use: 2 April 2012)

Karsedt S "Inequality, power and morals: Criminality of elites and their impact in society" http://www.afp.gov.au/media-centre/publications/platypus/previous-editions/1998/march-1998/inequality.aspx (Date of use: 17 January 2015), abbreviated as Karsedt http://www.afp.gov.au/media-centre/publications/platypus/previous-editions/1998/march-1998/inequality.aspx (Date of use: 17 January 2015)

Kharouni L "Africa a new safe harbour for cybercriminals?" http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-africa.pdf (Date of use: 29 August 2013), abbreviated as Kharouni http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-africa.pdf (Date of use: 29 August 2013)

Kirk J "Private industry group boosts UK cybercrime fight" http://www.computerworlduk.com/news/security/3289753/private-industry-group-boosts-uk-cybercrime-fight/ (Date of use: 9 April 2012), Kirk http://www.computerworlduk.com/news/security/3289753/private-industry-group-boosts-uk-cybercrime-fight/ (Date of use: 9 April 2012)

Klasen S "Social exclusion, children, and education: Conceptual and measurement issues" http://www.oecd.org/edu/school/1855901.pdf (Date of use: 17 May

2015), abbreviated as Klasen http://www.oecd.org/edu/school/1855901.pdf (Date of use: 17 May 2015)

Klein H "ICANN and internet governance: Leveraging technical coordination to realize global public policy" http://indiana.edu/~tisj/readers/full-text/18-3%20Klein.pdf (Date of use: 28 September 2015), abbreviated as Klein http://indiana.edu/~tisj/readers/full-text/18-3%20Klein.pdf (Date of use: 28 September 2015)

Koenig D "Investigation of cybercrime and technology-related crime" http://www.neiassociates.org/cybercrime-and-technology/ (Date of use: 27 December 2013), abbreviated as Koenig http://www.neiassociates.org/cybercrime-and-technology/ (Date of use: 27 December 2013)

Kolodkin B "What are sanctions" http://usforeignpolicy.about.com/od/introtoforeignpolicy/a/what-are-sanctions.htm (Date of use: 4 April 2015), abbreviated as Kolodkin http://usforeignpolicy.about.com/od/introtoforeignpolicy/a/what-are-sanctions.htm (Date of use: 4 April 2015)

Kovacs E "Cybercriminals use patriotic Russians to revive Kelihos botnet" http://www.infosecisland.com/blogview/23951-Cybercriminals-Use-Patriotic-Russians-to-Revive-Kelihos-Botnet.html (Date of use: 19 October 2014), abbreviated as Kovacs http://www.infosecisland.com/blogview/23951-Cybercriminals-Use-Patriotic-Russians-to-Revive-Kelihos-Botnet.html (Date of use: 19 October 2014)

Kowalski M "Cyber-crime: Issues, data sources, and feasibility of collecting police-reported statistics" http://publications.gc.ca/Collection/Statcan/85-558-X/85-558-XIE2002001.pdf (Date of use: 1 March 2012), abbreviated as Kowalski http://publications.gc.ca/Collection/Statcan/85-558-X/85-558-XIE2002001.pdf (Date of use: 1 March 2012)

LaMance K "What Is the crime of false pretenses?" http://www.legalmatch.com/law-library/article/false-pretenses.html (Date of use: 19 October 2014), abbreviated as LaMance http://www.legalmatch.com/law-library/article/false-pretenses.html (Date of use: 19 October 2014)

LaMorte C and Lilly J “Computers: History and development” http://www.dia.eui.upm.es/asignatu/sis_op1/comp_hd/comp_hd.htm (Date of use: 2 April 2012), abbreviated as LaMorte and Lilly http://www.dia.eui.upm.es/asignatu/sis_op1/comp_hd/comp_hd.htm (Date of use: 2 April 2012)

Langseth P “Global programme against corruption” http://www.unodc.org/pdf/crime/gpacpublications/cicp2.pdf (Date of use: 18 April 2015), abbreviated as Langseth http://www.unodc.org/pdf/crime/gpacpublications/cicp2.pdf (Date of use: 18 April 2015)

Larok A “Different approaches, same goal? Civil society and the fight against corruption in Uganda” http://www.actionaid.org/sites/files/actionaid/different_approaches_same_goal_civil_society_and_corruption.pdf (Date of use: 18 April 2015), abbreviated as Larok http://www.actionaid.org/sites/files/actionaid/different_approaches_same_goal_civil_society_and_corruption.pdf (Date of use: 18 April 2015)

Laurie D “Report argues Somali piracy benefits, stabilizes economy” *Voice of America* 12 January 2012 http://www.voanews.com/content/report-argues-somali-piracy-benefits-stabilizes-economy-137287138/150635.html (Date of use: 12 January 2015), abbreviated as Laurie http://www.voanews.com/content/report-argues-somali-piracy-benefits-stabilizes-economy-137287138/150635.html (Date of use: 12 January 2015)

Leiner BM *et al.* “Brief history of the internet” https://arxiv.org/html/cs/9901011? (Date of use: 21 April 2012), abbreviated as Leiner (Date of use: 21 April 2012)

Lemos R “International cybercrime treaty finalized” http://news.cnet.com/2100-1001-268894.html (Date of use: 31 December 2013), abbreviated as Lemos http://news.cnet.com/2100-1001-268894.html (Date of use: 31 December 2013)

Lengfelder C “International cooperation as a stepping-stone to a world government” http://www.globalpolicyjournal.com/brookings-audit/international-cooperation-stepping-stone-world-government (Date of use: 19 April 2017), abbreviated as Lengfelder http://www.globalpolicyjournal.com/brookings-audit/international-cooperation-stepping-stone-world-government (Date of use: 19 April 2017)

Lewytzkyj M “Tactics in cybersecurity: Russia and US – Don’t forget the Council of Europe Cyber-Crime Convention” http://www.examiner.com/article/tactics-cybersecurity-russia-us-don-t-forget-the-council-of-europe-cyber-crime-convention (Date of use: 31 December 2013), abbreviated as Lewytzkyj http://www.examiner.com/article/tactics-cybersecurity-russia-us-don-t-forget-the-council-of-europe-cyber-crime-convention (Date of use: 31 December 2013)

Li X “International actions against cybercrime: Networking legal systems in the networked crime scene” http://www.webology.org/2007/v4n3/a45.html (Date of use: 14 July 2013), abbreviated as Li http://www.webology.org/2007/v4n3/a45.html (Date of use: 14 July 2013)

Lilley P and Basnett Y “10 ways the new EU trade chief can help reduce poverty in developing countries” https://www.devex.com/news/10-ways-the-new-eu-trade-chief-can-help-reduce-poverty-in-developing-countries-84458 (Date of use: 17 July 2015), abbreviated as Lilley and Basnett https://www.devex.com/news/10-ways-the-new-eu-trade-chief-can-help-reduce-poverty-in-developing-countries-84458 (Date of use: 17 July 2015)

Longley R “Federalism whose power is this?” http://usgovinfo.about.com/od/rightsandfreedoms/a/whatisfederalism.htm (Date of use: 6 November 2012), abbreviated as Longley http://usgovinfo.about.com/od/rightsandfreedoms/a/whatisfederalism.htm (Date of use: 6 November 2012)

Lubic P “FBI has lead in addressing cybercrime for US” http://paulsInternetsecurityblog.wordpress.com/2013/01/31/fbi-has-lead-in-addressing-cybercrime-for-us/ (Date of use: 8 February 2013), abbreviated as Lubic http://paulsInternetsecurityblog.wordpress.com/2013/01/31/fbi-has-lead-in-addressing-cybercrime-for-us/ (Date of use: 8 February 2013)

Maclean D “International Telecommunications Union (ITU)” https://www.giswatch.org/sites/default/files/gisw_itu_0.pdf (Date of use: 25 December 2015), abbreviated as Maclean

https://www.giswatch.org/sites/default/files/gisw_itu_0.pdf (Date of use: 25 December 2015)

Maclean D *et al* "Strengthening developing country participation in international ICT decision-making" http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 28 November 2015), abbreviated as Maclean http://unpan1.un.org/intradoc/groups/public/documents/un/unpan013242.pdf (Date of use: 28 November 2015)

Madziwa S and Snail S "Cyber crime in South Africa" http://www.hg.org/article.asp?id=5351 (Date of use: 19 October 2014), abbreviated as Madziwa and Snail http://www.hg.org/article.asp?id=5351 (Date of use: 19 October 2014)

Maidment M "Taxonomies in the public sector" http://www.nglis.org.uk/tips/tipsben.htm (Date of use: 14 July 2013), abbreviated as Maidment http://www.nglis.org.uk/tips/tipsben.htm (Date of use: 14 July 2013)

Makkar S "Who will tackle cyber crime: Delhi police debates" http://www.india-forums.com/news/sci-tech/45564-who-will-tackle-cyber-crime-delhi-police-debates.htm (Date of use: 15 February 2013), abbreviated as Makkar http://www.india-forums.com/news/sci-tech/45564-who-will-tackle-cyber-crime-delhi-police-debates.htm (Date of use: 15 February 2013)

Marais P and Ostwalt P "Cross-border investigations: Are you prepared for the challenge?" http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cross-border-investigations.pdf (Date of use: 21 April 2014), abbreviated as Marais and Ostwalt http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cross-border-investigations.pdf (Date of use: 21 April 2014)

Markus Funk T "Mutual legal assistance treaties and letters rogatory: A guide for judges" http://www.fjc.gov/public/pdf.nsf/lookup/mlat-lr-guide-funk-fjc-2014.pdf/$file/mlat-lr-guide-funk-fjc-2014.pdf (Date of use: 10 April 2014)

Marshall J "Unethical rationalizations" http://ethicsalarms.com/rule-book/unethical-rationalizations-and-misconceptions/ (Date of use: 8 March 2012), abbreviated

as Marshall http://ethicsalarms.com/rule-book/unethical-rationalizations-and-misconceptions/ (Date of use: 8 March 2012)

Martin W "The 25 richest, wealthiest, happiest and most advanced countries in the world" http://www.independent.co.uk/travel/the-25-richest-healthiest-happiest-and-most-advanced-countries-in-the-world-a7396051.html (Date of use: 4 November 2017), abbreviated as Martin http://www.independent.co.uk/travel/the-25-richest-healthiest-happiest-and-most-advanced-countries-in-the-world-a7396051.html (Date of use: 4 November 2017)

Martinez PA "Testimony of Pablo A Martinez, Deputy Special Agent in Charge, Criminal Investigative Division, US Secret Service, before the Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism" http://www.dhs.gov/news/2011/04/11/testimony-pablo-martinez-deputy-special-agent-charge-criminal-investigative-division (Date of use: 12 February 2013)

Mashabane P "Unit set to tackle cyber crime" http://www.citizen.co.za/citizen/content/en/citizen/local-news?oid=228630&sn=Detail&pid=334&Unit-set-to-tackle-cyber-crime (Date of use: 20 April 2013), abbreviated as Mashabane http://www.citizen.co.za/citizen/content/en/citizen/local-news?oid=228630&sn=Detail&pid=334&Unit-set-to-tackle-cyber-crime (Date of use: 20 April 2013)

Massari G "Internet as instrument to spring Nigeria into the millennium" http://www.isocnig.org.ng/News.html (Date of use: 3 March 2013), abbreviated as Massari http://www.isocnig.org.ng/News.html (Date of use: 3 March 2013)

Masters G “Global cybercrime treaty rejected at UN” http://www.scmagazine.com/global-cybercrime-treaty-rejected-at-un/article/168630/ (Date of use: 14 July 2013), abbreviated as Masters http://www.scmagazine.com/global-cybercrime-treaty-rejected-at-un/article/168630/ (Date of use: 14 July 2013)

Mathews L “Phishing scams cost American businesses half a billion dollars a year” https://www.forbes.com/sites/leemathews/2017/05/05/phishing-scams-cost-american-businesses-half-a-billion-dollars-a-year/#783faf393fa1 (Date of use: 4 November 2017), abbreviated as Mathews https://www.forbes.com/sites/leemathews/2017/05/05/phishing-scams-cost-american-businesses-half-a-billion-dollars-a-year/#783faf393fa1 (Date of use: 4 November 2017)

Mathur A “United Nation’s definition of cybercrime” http://cyber-law-web.blogspot.com/2009/07/united-nations-definition-of-cybercrime.html (Date of use: 3 March 2012), abbreviated as Mathur http://cyber-law-web.blogspot.com/2009/07/united-nations-definition-of-cybercrime.html (Date of use: 3 March 2012)

Mauree V “ICT standardization capabilities of developing countries: Bridging the standardization gap” https://www.itu.int/dms_pub/itu-t/oth/0B/1F/T0B1F0000013301PDFE.pdf (Date of use: 25 December 2015)

Megias A “Internetlaw - how cyber jurisdiction affects cybercrime prosecution” https://www.ibls.com/Internet_law_news_portal_view.aspx?s=articles&id=32E51BFD-F186-4DEB-B121-F49D060E8118 (Date of use: 28 February 2014)

Melnikov A, Saint-Andre P and Nottingham M “Recent collaboration between W3C and IETF” http://www.w3.org/2010/11/TPAC/W3C-IETF-Collaboration.pdf (Date of use: 2 January 2016)

Messmer E “Ineffective law enforcement, bad economy fueling cybercrime” http://www.pcworld.com/article/155178/cybercrime_increasing.html (Date of use: 3 March 2013), abbreviated as Messmer http://www.pcworld.com/article/155178/cybercrime_increasing.html (Date of use: 3 March 2013)

Ministry of Foreign Affairs of Japan http://www.mofa.go.jp/policy/i_crime/high_tec/conf0105-6.html (Date of use: 7 April 2012)

Mobbs P "The law on the misuse of computers and networks" http://www.Internetrights.org.uk/index.shtml?AA_SL_Session=8fa795873994ed10dd54938b98227a99&x=605 (Date of use: 1 January 2013), abbreviated as Mobbs http://www.Internetrights.org.uk/index.shtml?AA_SL_Session=8fa795873994ed10dd54938b98227a99&x=605 (Date of use: 1 January 2013)

Mohammed Y "Appoint experience person to head power ministry Ewenla tells Buhari" http://www.pmnewsnigeria.com/2016/04/27/appoint-experienced-person-to-head-power-ministry-ewenla-tells-buhari/ (Date of use: 25 September 2016)

Morgan S "Cyber crime cost projected to reach $2 trillion by 2019" https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#620937163a91 (Date of use: 4 November 2017)

Moscow Times Newspaper http://www.themoscowtimes.com/news/article/ex-soviet-hackers-dominate-cyber-crime-world/484999.html (Date of use: 29 August 2013)

Mueller RS "FBI budget for fiscal year 2012" http://www.fbi.gov/news/testimony/fbi-budget-for-fiscal-year-2012 (Date of use: 12 February 2013)

Musser R "The two main challenges facing African civil society organizations" http://www.cipe.org/blog/2014/08/15/the-two-main-challenges-facing-african-civil-society-organizations/#.VR82SMl0cdk (Date of use: 4 April 2015)

Mutai M "Trans-border data flow: Its advantages and disadvantages" https://www.mu.ac.ke/informationscience/index.php/research-publications/staff-research-and-publication-2/category/16-miriam-mutai?download=57:advantages-and-disadvantages-of-trans-border-dataflow (Date of use: 15 March 2015), abbreviated as Mutai https://www.mu.ac.ke/informationscience/index.php/research-publications/staff-research-and-publication-2/category/16-miriam-mutai?download=57:advantages-and-disadvantages-of-trans-border-dataflow (Date of use: 15 March 2015)

Mwaita P and Owor M "Workshop report on effective cybercrime legislation in Eastern Africa" http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/2571_EastAfrica_WS_Report.pdf (Date of use: 12 October 2014), abbreviated as Mwaita and Owor http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/2571_EastAfrica_WS_Report.pdf (Date of use: 12 October 2014)

Nahra KJ "Role of victims in criminal investigations and prosecutions" http://www.insurancefraud.org/downloads/Role_of_Victims.pdf (Date of use: 19 April 2014), abbreviated as Nahra http://www.insurancefraud.org/downloads/Role_of_Victims.pdf (Date of use: 19 April 2014)

Nevile CM "World wide web consortium process document" https://www.w3.org/2015/Process-20150901/ (Date of use: 5 November 2016), abbreviated as Nevile https://www.w3.org/2015/Process-20150901/ (Date of use: 5 November 2016)

New Indian Express http://newindianexpress.com/states/kerala/article562041.ece?service=print (Date of use: 15 February 2013)

Nguyen A "Government creates new cyber crime unit" http://www.csoonline.com/article/695079/government-creates-new-cyber-crime-unit (Date of use: 24 April 2012)

Nigerian Pilot Newspaper http://www.nigerianpilot.com/we-dont-know-exact-number-of-police-in-nigeria-psc/ (Date of use: 20 April 2013)

O'Driscoll A "100+ terrifying cybercrime and cybersecurity statistics and trends (2018 edition)" https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/#gref (Date of use: 29 September 2018).

Oates J "Operation Eagle Claw nets 18 Nigerian spammers" http://www.theregister.co.uk/2009/10/23/nigeria_police_success/ (Date of use: 23 February 2013), abbreviated as Oates http://www.theregister.co.uk/2009/10/23/nigeria_police_success/ (Date of use: 23 February 2013)

Ochman BL "Facebook silent as my account and 45 000 others are hacked: 600 000 Facebook logins are compromised daily. What to do if your Facebook account is hacked" http://www.whatsnextblog.com/2012/01/facebook-silent-as-my-account-and-45000-others-are-hacked-600000-facebook-logins-are-compromised-daily/ (Date of use: 24 April 2012)

Odiegwu M "Fighting kidnappers with death sentence" http://www.punchng.com/politics/fighting-kidnappers-with-death-sentence/ (Date of use: 20 January2015)

Odita S "For police, a forensic laboratory to fight financial crimes" http://www.ngrguardiannews.com/index.php?option=com_content&view=article&id=112349:for-police-a-forensic-laboratory-to-fight-financial-crimes&catid=3:metro&Itemid=558 (Date of use: 22 February 2013)

Ofosu-Appiah B "Making NGO's more effective and responsive in a globalised world" https://www.globalpolicy.org/component/content/article/177/31636.html (Date of use: 17 May 2015)

Okoli F "Starting a computer business centre in Nigeria" http://www.makemoneynigeria.net/cgi-bin/page.pl?b=small-business&bn=4&m=3 (Date of use: 16 April 2015)

Okoye SE "How to tackle corruption effectively in Nigeria" http://www.gamji.com/article4000/NEWS4930.htm (Date of use: 29 January 2015)

Okuttah M "EAC eyes trade growth with cyber laws" http://www.businessdailyafrica.com/EAC-eyes-trade-growth-with-cyber-laws/-/539444/945130/-/xd5eh7z/-/index.html (Date of use: 31 August 2013)

Omoh G "How government impoverished Nigerians, poverty on rampage" http://www.vanguardngr.com/2012/02/how-government-impoverished-nigerians-poverty-on-rampage/ (Date of use: 31 March 2013)

Oreweme IE "What's new about the 2011 Evidence Act" http://dx.doi.org/10.2139/ssrn.2111157 (Date of use: 16 March 2013)

Paganini P “The value of personal data in the criminal underground” http://securityaffairs.co/wordpress/33431/cyber-crime/personal-data-criminal-underground.html (Date of use: 1 April 2015)

Pearson C “Problems with the Computer Misuse Act” http://www.ehow.co.uk/list_7373521_problems-computer-misuse-act.html (Date of use: 3 January 2013)

Pei M “China's political evolution: Implications for Beijing's foreign relations” http://www.thefreelibrary.com/China%27s+political+evolution%3a+implications+for+Beijing%27s+foreign...-a0155824547 (Date of use: 18 August 2013), abbreviated as Pei http://www.thefreelibrary.com/China%27s+political+evolution%3a+implications+for+Beijing%27s+foreign...-a0155824547 (Date of use: 18 August 2013)

Peter I “The beginnings of the internet” http://www.nethistory.info/History%20of%20the%20Internet/beginnings.html (Date of use: 24 April 2012)

Pfeffermann G “Poverty reduction in developing countries: The role of private enterprise” http://www.imf.org/external/pubs/ft/fandd/2001/06/pfefferm.htm#author (Date of use: 17 July 2015)

Pickett K “Reducing inequality: An essential step for development and wellbeing” http://www.progressiveeconomy.eu/content/reducing-inequality-essential-step-development-and-en (Date of use: 17 January 2015), abbreviated as Pickett http://www.progressiveeconomy.eu/content/reducing-inequality-essential-step-development-and-en (Date of use: 17 January 2015)

Power R “Deadbolting the backdoors on your network” http://www.ssg-inc.net/cyber_crime/digital_crime.html (Date of use: 9 April 2012)

Prakash P “Short note on IT Amendment Act, 2008” http://cis-india.org/Internet-governance/publications/it-act/short-note-on-amendment-act-2008 (Date of use: 12 January 2013)

Premium Times Newspaper http://premiumtimesng.com/news/124330-nigerian-not-ready-to-fight-cyber-crime-ncc.html (Date of use: 1 January 2014)

Protalinski E "Internet fraud alert: One-stop service to report stolen data" http://arstechnica.com/tech-policy/2010/06/Internet-fraud-alert-one-stop-service-to-report-stolen-data/ (Date of use: 12 February 2013)

Punch Newspaper Nigeria http://www.punchng.com/business/technology/cyber-laws-necessary-to-protect-cash-less-system-fico-boss/ (Date of use: 24 April 2012)

Radebe J "Results beginning to show in fight againstcrime/corruption" http://www.politicsweb.co.za/politicsweb/view/politicsweb/en/page71656?oid=281004&sn=Detail (Date of use: 20 February 2013)

Rademeyer J "Conviction rates an unreliable benchmark of NPA success" http://africacheck.org/reports/conviction-rates-an-unreliable-benchmark-of-npa-success/ (Date of use: 29 December 2013)

Ragan S "UK unveils new cyber security strategy, will create new cybercrime unit" http://www.securityweek.com/uk-unveils-new-cyber-security-strategy-will-create-new-cybercrime-unit (Date of use: 13 April 2012)

Raja M "The dark face of the internet in India" http://atimes.com/atimes/South_Asia/II20Df01.html (Date of use: 16 February 2013)

Reed C "Taking sides on technology neutrality" http://www2.law.ed.ac.uk/ahrc/script-ed/vol4-3/reed.asp (Date of use: 03 January 2014), abbreviated as Reed http://www2.law.ed.ac.uk/ahrc/script-ed/vol4-3/reed.asp (Date of use: 03 January 2014

Richardson H "Aid – More strings attached?" http://www.una.org.uk/content/aid-more-strings-attached (Date of use: 3 April 2015), abbreviated as Richardson http://www.una.org.uk/content/aid-more-strings-attached (Date of use: 3 April 2015)

Ringwelski M "Effects of cybercrime" http://www.ehow.com/about_5052659_effects-cyber-crime.html (Date of use: 3 April 2015**)**

Robinson PH "Mensrea" https://www.law.upenn.edu/fac/phrobins/mensreaentry.pdf (Date of use: 28 September 2013)

Rodota S “Opinion 4/2001 on the Council of Europe’s draft Convention on Cyber-Crime” http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp41_en.pdf (Date of use: 18 August 2013)

Rosenberg M “Current USA population” http://geography.about.com/od/obtainpopulationdata/a/uspopulation.htm (Date of use: 13 April 2012)

Rosenburg M “Non-members of the United Nations” http://geography.about.com/od/politicalgeography/a/nun.htm (Date of use: 3 January 2014), abbreviated as Rosenburg http://geography.about.com/od/politicalgeography/a/nun.htm (Date of use: 3 January 2014)

Rosenblatt B “Principles of jurisdiction” http://cyber.law.harvard.edu/property99/domain/Betsy.html (Date of use: 4 October 2014)

Sabadash V “Victims of cybercrime” http://www.crime-research.org/news/04.17.2004/212/ (Date of use: 31 March 2012)

Sadiq S and Tiller S “The debate over UN sanctions” http://www.pbs.org/frontlineworld/stories/iraq/sanctions.html (Date of use: 4 April 2015), abbreviated as Sadiq and Tiller http://www.pbs.org/frontlineworld/stories/iraq/sanctions.html (Date of use: 4 April 2015)

Sadowsky G**,** Zambrano R and Dandjinou P **“**Internet governance: A discussion document” http://www.Internetsociety.org/sites/default/files/Internet%20Governance%20A%20Discussion%20Document%20%28George%20Sadowsky%29.pdf (Date of use: 20 September 2015)

Sainty K and Ailwood A “Managing compliance in the global space – Transborder data flow” http://www.aar.com.au/pubs/pdf/priv/pap30nov04.pdf (Date of use: 24 April 2012)

Sakal Times E-paper http://72.78.249.187/SakaalTimesBeta/20121227/5600265108256631975.htm (Date of use: 15 February 2013)

Sanou B “The world in 2015” https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf (Date of use: 23 July 2016), abbreviated as Sanou https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf (Date of use: 23 July 2016)

Schettino I “Is coercive diplomacy a viable means to achieve political objectives?” http://www.e-ir.info/2009/06/29/is-coercive-diplomacy-a-viable-means-to-achieve-political-objectives/ (Date of use: 3 April 2015), abbreviated as Schettino http://www.e-ir.info/2009/06/29/is-coercive-diplomacy-a-viable-means-to-achieve-political-objectives/ (Date of use: 3 April 2015)

Schiller J “Crime and criminality” http://www.des.ucdavis.edu/faculty/Richerson/BooksOnline/He16-95.pdf (Date of use: 11 January 2015), abbreviated as Schiller http://www.des.ucdavis.edu/faculty/Richerson/BooksOnline/He16-95.pdf (Date of use: 11 January 2015)

Schjølberg S “Computer-related offences” http://www.cybercrimelaw.net/documents/Strasbourg.pdf (Date of use: 13 August 2013), abbreviated as Schjølberg http://www.cybercrimelaw.net/documents/Strasbourg.pdf (Date of use: 13 August 2013)

Schøjlberg S “Potential new international legal mechanisms against global cyber-attacks and other global cybercrime” http://www.cybercrimelaw.net/documents/New_international_legal_mechanisms.pdf (Date of use: 15 February 2014), abbreviated as Schøjlberg http://www.cybercrimelaw.net/documents/New_international_legal_mechanisms.pdf (Date of use: 15 February 2014)

Schjølberg S “The history of global harmonization on cybercrime legislation – The road to Geneva” http://www.cybercrimelaw.net/documents/cybercrime_history.pdf (Date of use: 2 August 2013), abbreviated as Schjølberg http://www.cybercrimelaw.net/documents/cybercrime_history.pdf (Date of use: 2 August 2013

Schjølberg S and Ghernaouti-Helie S "A global protocol on Cybersecurity and Cybercrime" http://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf (Date of use: 3 June 2017), abbreviated as Schjølberg and Ghernaouti-Helie http://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf (Date of use: 3 June 2017)

Schjølberg S and Ghernaouti-Helie S "A global treaty on cybersecurity and cybercrime" http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf (Date of use: 2 August 2013), abbreviated as Schjølberg and Ghernaouti-Helie http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf (Date of use: 2 August 2013)

Schjølberg S and Hubbard AM "Harmonizing national legal approaches on cybercrime" http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf (Date of use: 13 August 2013), abbreviated as Schjølberg and Hubbard http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf (Date of use: 13 August 2013)

Schwartz MJ "FBI to get more cyber crime agents" http://www.informationweek.com/security/government/fbi-to-get-more-cyber-crime-agents/232300860 (Date of use: 12 February 2013), abbreviated as http://www.informationweek.com/security/government/fbi-to-get-more-cyber-crime-agents/232300860 (Date of use: 12 February 2013)

Scott BA "Effects of technology and high-tech gadgets in our lives" http://ezinearticles.com/?Effects-Of-Technology-And-High-Tech-Gadgets-In-Our-Lives&id=5859939 (Date of use: 13 April 2012)

Sembok TT "Ethics of information communication technology" http://www2.unescobkk.org/elib/publications/ethic_in_asia_pacific/239_325ETHICS.PDF (Date of use: 9 April 2012)

Serra D and Barr A "Culture and corruption" http://economics.ouls.ox.ac.uk/14043/1/gprg-wps-040.pdf (Date of use: 3 March 2013), abbreviated as Serra and Barr

http://economics.ouls.ox.ac.uk/14043/1/gprg-wps-040.pdf (Date of use: 3 March 2013)

Shah S "The Information Technology Act 2000: A legal framework for e-governance" http://www.sudhirlaw.com/cyberlaw-itact.htm (Date of use: 11 January 2013)

Shane Smith M "Sanctions: Diplomatic tool, or warfare by other means?" http://www.beyondintractability.org/essay/sanctions (Date of use: 4 April 2015), abbreviated as Shane Smith http://www.beyondintractability.org/essay/sanctions (Date of use: 4 April 2015)

Shears M "The road to Rio and beyond current status of internet governance discussions" https://www.ripe.net/participate/meetings/roundtable/september-2007/roadtorio.pdf (Date of use: 11 January 2016)

Sikuka K "Southern Africa: Region cracks down on cyber crime" http://allafrica.com/stories/201204120866.html (Date of use: 31 August 2013), abbreviated as Sikuka http://allafrica.com/stories/201204120866.html (Date of use: 31 August 2013)

Simonelis A "A concise guide to the major internet bodies" http://ubiquity.acm.org/article.cfm?id=1071915 (Date of use: 5 November 2016)

Sinha S "Indian police not capable of solving hi-tech cyber crimes" http://www.indianexpress.com/news/-indian-police-not-capable-of-solving-hitech-cyber-crimes-/1009410 (Date of use: 14 February 2013)

Sirothia A "Staff crunch cripple cyber crime cell" http://articles.timesofindia.indiatimes.com/2012-08-12/bhopal/33167201_1_cyber-cell-cyber-crime-crime-detection (Date of use: 15 February 2013), abbreviated as Sirothia http://articles.timesofindia.indiatimes.com/2012-08-12/bhopal/33167201_1_cyber-cell-cyber-crime-crime-detection (Date of use: 15 February 2013)

Sloan J "Fighting computer crime by combining federal and state law" http://www.uplink.com.au/lawlibrary/Documents/Docs/Doc121.html (Date of use: 2 December 2012), abbreviated as Sloan

http://www.uplink.com.au/lawlibrary/Documents/Docs/Doc121.html (Date of use: 2 December 2012)

Smith RG "Impediments to the successful investigation of transnational high tech crime" http://www.aic.gov.au/publications/current%20series/tandi/281-300/tandi285.html (Date of use: 15 February 2014), abbreviated as Smith http://www.aic.gov.au/publications/current%20series/tandi/281-300/tandi285.html (Date of use: 15 February 2014)

Sommer P "Malware and cyber-crime" http://www.publications.parliament.uk/pa/cm201012/cmselect/cmsctech/writev/mal/mal01.htm (Date of use: 24 April 2012)

Souter D "Phase 2 report: Mapping the information and participation practice of Internet governance entities" http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_Internet_governance/Internet_Governance_Report_Souter_May09.pdf (Date of use: 20 September 2015), abbreviated as Souter http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_Internet_governance/Internet_Governance_Report_Souter_May09.pdf (Date of use: 20 September 2015)

Southern Times Newspaper http://www.southerntimesafrica.com/news_article.php?id=8603&title=Wising%20Up%20to%20Cyber%20Security&type=80 (Date of use: 31 August 2013)

Spinellis D "Opportunité et Légitimité de l'Harmonisation" http://hal.archives-ouvertes.fr/docs/00/41/96/45/PDF/OPPORTUNITE_ET_LEGITIMITE_DE_L_HARMONISATION_-_Donysios_SPINELLIS.pdf (Date of use: 31 August 2013)

Stenson T "Inchoate crimes and criminal responsibility under International law" https://www.law.upenn.edu/journals/jil/jilp/articles/1-1_Stenson_Thomas.pdf (Date of use: 14 September 2013)

Suleiman S "Nigeria: Where thieves are rewarded" http://nigerianstalk.org/2014/01/15/nigeria-where-thieves-are-rewarded-salisu-suleiman/ (Date of use: 31 May 2015), abbreviated as Suleiman http://nigerianstalk.org/2014/01/15/nigeria-where-thieves-are-rewarded-salisu-suleiman/ (Date of use: 31 May 2015)

Surbhi S “Difference between developed countries and developing countries” http://keydifferences.com/difference-between-developed-countries-and-developing-countries.html (Date of use: 4 November 2017)

Taub EA “Deleting may be easy, but your hard drive still tells all” http://www.nytimes.com/2006/04/05/technology/techspecial4/05forensic.html?pagewanted=print&_r=0 (Date of use: 11 February 2013)

Teleanu S “Emerging IG issues from the perspective of regional and national IGF initiatives” https://www.Internetsociety.org/blog/2012/11/emerging-ig-issues-perspective-regional-and-national-igf-initiatives (Date of use: 9 December 2015)

The Economic Times http://articles.economictimes.indiatimes.com/2009-03-30/news/28401922_1_cyber-terrorism-cybercrime-convention (Date of use: 19 October 2014)

The Hindu Newspaper http://www.thehindu.com/news/states/tamil-nadu/validity-of-section-66a-of-it-act-challenged/article4116598.ece (Date of use: 12 January 2013)

The internet library of law and court decisions http://www.Internetlibrary.com/statuteitem.cfm?Num=10 (Date of use: 11 November 2012)

The New Indian Express http://newindianexpress.com/states/kerala/article562041.ece?service=print (Date of use: 15 February 2013)

The Times of India http://timesofindia.indiatimes.com/topic/cyber-crime/news/ (Date of visit: 16 February 2013)

Thomson I “Sony admits huge data leak after PlayStation network and Qriocity attacks” http://www.v3.co.uk/v3-uk/news/2046030/sony-admits-leak-playstation-network-qriocity-attacks (Date of use: 29 March 2015)

Touray KS “I had a dream: ICANN has 2 billion reasons to support developing countries” http://www.circleid.com/posts/20130901_icann_has_2_billion_reasons_to_support_developing_countries/ (Date of use: 24 November 2015)

Tylus K "Culture as a factor of social and economic development – The Polish experience" http://www.poieinkaiprattein.org/economy/culture-and-economy/culture-as-a-factor-of-social-and-economic-development---the-polish-experience-by-karolina-tylus/ (Date of use: 20 January 2015)

Urbas G "An overview of cybercrime legislation and cases in Singapore" http://law.nus.edu.sg/asli/pdf/WPS001.pdf (Date of use: 6 March 2012)

Van Der Westhuizen H "New Bill offers robust game plan against cybercrime in South Africa" https://saiia.org.za/research/new-bill-offers-robust-game-plan-against-cybercrime-in-south-africa/ (Date of use: 4 October 2019), abbreviated as Van Der Westhuizen https://saiia.org.za/research/new-bill-offers-robust-game-plan-against-cybercrime-in-south-africa/ (Date of use: 4 October 2019)

Vaughn S "Consumers prefer online banking to traditional branch banking: Rosetta retail banking survey reveals consumer trends and insights" http://www.prweb.com/releases/2012/5/prweb9524621.htm (Date of use: 13 August 2012)

Verton D "FBI chief: Lack of incident reporting slows cybercrime fight" http://www.computerworld.com/article/2578278/cybercrime-hacking/fbi-chief--lack-of-incident-reporting-slows-cybercrime-fight.html (Date of use: 19 October 2014)

Wang B "Poverty statistics and estimates and definitions" https://www.nextbigfuture.com/2011/02/poverty-statistics-and-estimates-and.html (Date of use: 12 October 2018).

Waghorne M "Cybercrime: The scourge of the digital economy" http://www.information-age.com/technology/security/123458137/cybercrime-scourge-digital-economy (Date of use: 17 January 2015)

Wagley J "Battling cybercrime across borders" http://www.securitymanagement.com/article/battling-cybercrime-across-borders-007995 (Date of use: 20 April 2014)

Ward M "Poverty and crime" http://www.nationaldialoguenetwork.org/poverty-and-crime/ (Date of use 17 January 2015)

Ware WH "RAND contributions to the development of computing" http://www.rand.org/about/history/ware.html (Date of use: 24 April 2012)

Wattanajantra A "Cybercrime: The challenges of the police central e-crime unit" http://www.itpro.co.uk/609968/cybercrime-the-challenges-of-the-police-central-e-crime-unit (Date of use: 17 April 2013.

Whittaker Z "Cybercrime costs $338bn to global economy: More lucrative than drugs trade" http://www.zdnet.com/blog/btl/cybercrime-costs-338bn-to-global-economy-more-lucrative-than-drugs-trade/57503 (Date of use: 13 April 2012), Whittaker http://www.zdnet.com/blog/btl/cybercrime-costs-338bn-to-global-economy-more-lucrative-than-drugs-trade/57503 (Date of use: 13 April 2012)

Wingfield B "Making sense of US foreign aid to Egypt and elsewhere" http://www.forbes.com/sites/brianwingfield/2011/01/29/making-sense-of-u-s-foreign-aid-to-egypt-and-elsewhere/ (Date of use: 3 April 2015), abbreviated as Wingfield http://www.forbes.com/sites/brianwingfield/2011/01/29/making-sense-of-u-s-foreign-aid-to-egypt-and-elsewhere/ (Date of use: 3 April 2015)

Wolf U "Cyber-crime: Law enforcement must keep pace with tech-savvy criminals" http://www.digitalcommunities.com/articles/Cyber-Crime-Law-Enforcement-Must-Keep-Pace.html (Date of use: 16 April 2014), abbreviated as Wolf http://www.digitalcommunities.com/articles/Cyber-Crime-Law-Enforcement-Must-Keep-Pace.html (Date of use: 16 April 2014)

Yamout S "Developing nations participation in internet governance" http://igcaucus.org/submission-cstd-working-group-improvements-igf (Date of use: 9 December 2015), abbreviated as Yamout http://igcaucus.org/submission-cstd-working-group-improvements-igf (Date of use: 9 December 2015)

Yanagihara T "Approach to poverty reduction in developing countries andJapan" s contribution" http://jica-ri.jica.go.jp/IFIC_and_JBICI-Studies/english/publications/reports/study/topical/articles/pdf/articles_02.pdf (Date of use: 17 July 2015), abbreviated as Yanagihara http://jica-ri.jica.go.jp/IFIC_and_JBICI-Studies/english/publications/reports/study/topical/articles/pdf/articles_02.pdf (Date of use: 17 July 2015)

Young-Mok K “Inequality – How to address Piketty on the global level” https://www.devex.com/news/inequality-how-to-address-piketty-on-the-global-level-84077 (Date of use: 17 May 2015), Young-Mok https://www.devex.com/news/inequality-how-to-address-piketty-on-the-global-level-84077 (Date of use: 17 May 2015)

Zimbabwe Independent Newspaper https://www.theindependent.co.zw/2017/01/13/cybercrimes-bill-flaws-remedies/ (Date of use: 14 August 2017)

Zintel M “Scotland Yard selects guidance software’s EnCase to combat UK’s computer crime” http://www.crime-research.org/news/2003/01/Mess1003.htm (Date of use: 7 February 2013), abbreviated as Zintel http://www.crime-research.org/news/2003/01/Mess1003.htm (Date of use: 7 February 2013)

http://afrinic.net/en/about-us/our-members (Date of use: 30 January 2016)

http://apt46.net/2013/01/18/thai-guy-convicted-of-insinuating-something-about-his-king/ (Date of use: 3 March 2013)

http://beta.congress.gov/bill/112th-congress/senate-bill/1469/text (Date of use: 13 April 2013)

http://cbi.nic.in/aboutus/cbiroles.php (Date of use: 14 February 2013)

http://cbi.nic.in/aboutus/div.php (Date of use: 16 February 2013)

http://cbi.nic.in/aboutus/manuals/Chapter_26.pdf (Date of use: 15 February 2013)

http://cidwestbengal.gov.in/ (Date of use: 14 February 2013)

http://clinton4.nara.gov/WH/New/Commerce/summary.html (Date of use: 20 September 2015)

http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG (Date of use: 13 August 2013)

http://conventions.coe.int/Treaty/Commun/print/ChercheSig.asp?NT=185&CL=ENG (Date of use: 31 December 2013)

http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm (Date of use: 13 August 2013)

http://da.co.la.ca.us/htcu.htm (Date of use: 12 February 2013)

http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/477/78/IMG/NR047778.pdf?OpenElement (Date of use: 24 July 2013)

http://delcode.delaware.gov/title11/c005/sc03/index.shtml#P1781_140437 (Date of use: 11 November 2012)

http://digitalreview.asia/content/sub-regional-perspectives/asia-pacific-economic-cooperation/ (Date of use: 10 August 2013)

http://docs.legis.wisconsin.gov/statutes/statutes/947/0125/1 (Date of use: 27 November 2012)

http://energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf (Date of use: 2 December 2012)

http://epic.org/privacy/intl/ccc.html (Date of use: 18 August 2013)

http://gidsigned.com/sites/gidsigned/documents/Document_0000024.odt (Date of use: 6 April 2012)

http://gilc.org/privacy/coe-letter-1000.html (Date of use: 18 August 2013

http://groups.itu.int/itu-t/StudyGroups.aspx (Date of use: 25 December 2015)

http://grprofessionals.org/about-lobbying/what-is-lobbying/ (Date of use: 21 March 2015)

http://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_%28CFAA%29 (Date of use: 2 December 2012)

http://investors.guidancesoftware.com/releasedetail.cfm?releaseid=560712 (Date of use: 11 February 2013)

http://law.jrank.org/pages/818/Crime-Causation-Sociological-Theories-Social-disorganization-theory.html (Date of use: 11 January 2015)

http://law.justia.com/codes/florida/2004/TitleXLVI/chapter847/847_0135.html (Date of use: 1 December 2012)

http://law.onecle.com/new-jersey/2c-the-new-jersey-code-of-criminal-justice/20-25.html (Date of use: 11 November 2012)

http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.7 (Date of use: 27 November 2012)

http://legal-dictionary.thefreedictionary.com/Uniform+Acts (Date of use: 11 November 2012)

http://library.thinkquest.org/28787/developm1.htm (Date of use: 2 April 2012)

http://mac-antivirus-software-review.toptenreviews.com/the-geography-of-cybercrime.html (Date of use: 19 October 2014)

http://newsdiaryonline.com/house_speak.htm (Date of use: 22 February 2013)

http://oklegal.onenet.net/oklegal-cgi/ifetch?Oklahoma_Statutes.99+845214534629+F (Date of use: 1 December 2012)

http://pirateparty.org.au/2013/03/05/cybercrime-convention-ratification-leaves-lingering-concerns/ (Date of use: 18 August 2013)

http://recoverytoolsrus.com/forensic-data-recovery-news/news-11-27.html (Date of use: 20 February 2013)

http://sheltersuites.net/why-are-hotels-in-nigeria-so-expensive/ (Date of use: 29 January 2015)

http://specialfraudunit.org.ng/about.html (Date of use: 22 February 2013)

http://specialfraudunit.org.ng/fraud.html (Date of use: 22 February 2013)

http://unmiss.unmissions.org/Default.aspx?tabid=4307&language=en-US (Date of use: 22 July 2014)

http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan002107.pdf (Date of use: 20 March 2012)

http://us.norton.com/cybercrime/prevention.jsp (Date of use: 24 April 2012)

http://www.419eater.com/html/419faq.htm (Date of use: 24 April 2012)

http://www.accessdata.com/products/digital-forensics (Date of use: 7 February 2013)

http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf (Date of use: 7 February 2013)

http://www.actionfraud.police.uk/fraud-az-advance-fee-fraud (Date of use: 9 October 2014)

http://www.afp.gov.au/~/media/afp/pdf/f/fighting-the-invisible.ashx (Date of use: 14 July 2013)

http://www.ag.gov.au/Internationalrelations/Internationalcrimecooperationarrangements/Extradition/Documents/Factsheet%20Provisional%20Arrest%20Requests.pdf (Date of use: 12 April 2014)

http://www.alertindian.com/node/5 (Date of use: 14 March 2013)

http://www.apec.org/About-Us/About-APEC/Member-Economies.aspx (Date of use: 10 August 2013)

http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2012_tel.aspx (Date of use: 10 August 2013)

http://www.asianlii.org/apec/other/agrmt/fammotaiisc819/ (Date of use: 10 August 2013)

http://www.atf.gov/about/mission/# (Date of use: 8 February 2013)

http://www.balancingact-africa.com/news/en/issue-no-177/internet/nigerian-police-exto/en (Date of use: 9 October 2014)

http://www.balancingact-africa.com/news/telecoms_en/7072/icann-asks-for-more-african-input-in-generic-names-supporting-organisation (Date of use: 5 October 2015)

http://www.bluechipjournal.co.za/articles/cyber-crime (Date of use: 20 February 2013)

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf (Date of use: 01 August 2014)

http://www.college.police.uk/cps/rde/xchg/cop/root.xsl/16732.htm (Date of use: 7 February 2013)

http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/ (Date of use: 20 March 2012)

http://www.cps.gov.uk/legal/l_to_o/obscene_publications/ (Date of use: 1 January 2013)

http://www.cyanre.co.za/national-cybersecurity-policy.pdf (Date of use: 19 February 2013)

http://www.cyanre.co.za/what-sets-us-apart.html (Date of use: 20 February 2013)

http://www.cybercitizenship.org/crime/crime.html (Date of use: 31 March 2012)

http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf (Date of use: 4 August 2013)

http://www.cybersecuritycooperation.org/moredocuments/International%20Agreements/Cybersec%20Strategy%20TEL%20final.htm (Date of use: 10 August 2013)

http://www.data64.in/about-us.php (Date of use: 16 February 2013)

http://www.dibsforensics.com/equipment.html (Date of use: 16 February 2013)

http://www.dsci.in/cyber-labs (Date of use: 16 February 2013)

http://www.duhaime.org/LegalDictionary/D/DualCriminality.aspx (Date of use: 17 March 2014)

http://www.eac.int/ (Date of use: 31 August 2013)

http://www.efccnigeria.org/efcc/index.php/about-efcc (Date of use: 21 February 2013)

http://www.efccnigeria.org/efcc/index.php/about-efcc/efcc-academy (Date of use: 23 February 2013)

http://www.efccnigeria.org/efcc/index.php/about-efcc/operations (Date of use: 21 February 2013)

http://www.encyclopedia.com/topic/Computer_Crime.aspx#2 (Date of use: 11 November 2012)

http://www.fbi.gov/about-us/itb/news-features/cyber-one-stop-shopping-and-real-time-tracking (Date of use: 11 February 2013)

http://www.fbi.gov/news/testimony/oversight-of-the-federal-bureau-of-investigation-4 (Date of use: 10 February 2013)

http://www.fd.uc.pt/CI/CEE/OI/INTERPOL/interpol-constitution.htm (Date of use: 23 July 2014)

http://www.fletc.gov/about-fletc (Date of use: 12 February 2013)

http://www.fraudwatchers.org/forums/showthread.php?t=15076 (Date of use: 23 February 2013)

http://www.gaicac.us/Statutes_Georgia.htm# ComputerCrime (Date of use: 11 November 2012)

http://www.globalpartnership.org/education (Date of use: 17 July 2015)

http://www.gov.za/documents/national-crime-prevention-strategy-summary#P3 (Date of use: 18 April 2015)

http://www.gpo.gov/fdsys/pkg/CHRG-106shrg69335/html/CHRG-106shrg69335.htm (Date of use: 5 February 2013)

http://www.hg.org/cyber-space.html (Date of use: 8 March 2013)

http://www.homeoffice.gov.uk/about-us/freedom-of-information/released-information1/foi-archive-crime/21981-cyber-crime-funding/ (Date of use: 7 February 2013)

http://www.homeoffice.gov.uk/crime/nca/ (Date of use: 5 February 2013)

http://www.hrw.org/world-report/2013/country-chapters/nigeria (Date of use: 19 October 2014)

http://www.huffingtonpost.com/2010/06/22/internet-usage-statistics_n_620946.html (Date of use: 13 April 2012)

http://www.icc-cpi.int/en_menus/icc/structure%20of%20the%20court/Pages/structure%20of%20the%20court.aspx (Date of use: 11 August 2014)

http://www.icc-cpi.int/en_menus/icc/structure%20of%20the%20court/chambers/pre%20trial%20division/Pages/pre%20trial%20division.aspx (Date of use: 16 August 2014)

http://www.icc-cpi.int/en_menus/icc/structure%20of%20the%20court/chambers/appeals%20division/Pages/appeals%20division.aspx (Date of use: 20 September 2014)

http://www.icc-cpi.int/en_menus/icc/structure%20of%20the%20court/office%20of%20the%20prosecutor/faq/Pages/faq.aspx (Date of use: 16 August 2014)

http://www.icc-cpi.int/iccdocs/doc/doc1405819.pdf (Date of use: 16 March 2014)

http://www.icc-cpi.int/iccdocs/PIDS/publications/RomeStatutEng.pdf (Date of use: 16 August 2014)

http://www.ice.gov/cyber-crimes/# (Date of use: 8 February 2013)

http://www.ictparliament.org/legislationlibrary/Cybercrime (Date of use: 29 August 2013)

http://www.ideafinder.com/history/inventions/comeniac.htm (Date of use: 2 April 2012)

http://www.ietf.org/iesg/past-members.html (Date of use: 4 January 2016)

http://www.info.gov.za/speech/DynamicAction?pageid=461&sid=25751&tid=59794 (Date of use: 19 February 2013)

http://www.info.gov.za/view/DownloadFileAction?id=127117 (Date of use: 19 February 2013)

http://www.informationweek.com/security/government/fbi-to-get-more-cyber-crime-agents/232300860 (Date of use: 12 February 2013)

http://www.infosecurity-magazine.com/view/13346/uk-to-spend-650m-on-new-national-cyber-security-programme/ (Date of use: 7 February 2013)

http://www.Internetsociety.org/deploy360/resources/number-resource-organization/ (Date of use: 30 January 2016)

http://www.Internetsociety.org/what-we-do/grants-awards (Date of use: 7 September 2016)

http://www.Internetsociety.org/who-we-are/board-trustees (Date of use: 11 January 2016)

http://www.Internetsociety.org/who-we-are/board-trustees (Date of use: 9 January 2016)

http://www.Internetsociety.org/who-we-are/chapters (Date of use: 7 September 2016)

http://www.Internetsociety.org/who-we-are/mission (Date of use: 9 January 2016)

http://www.interpol.int/About-INTERPOL/International-partners/United-Nations (Date of use: 23 July 2014)

http://www.interpol.int/About-INTERPOL/Structure-and-governance (Date of use: 23 July 2014)

http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime (Date of use: 23 July 2014)

http://www.interpol.int/Member-countries/World (Date of use: 22 July 2014)

http://www.intgovforum.org/cms/aboutigf (Date of use: 11 December 2015)

http://www.intgovforum.org/cms/athensmeeting (Date of use: 12 December 2015)

http://www.intgovforum.org/cms/component/content/article?id=2102:mag-2015 (Date of use: 12 December 2015)

http://www.intgovforum.org/cms/home-36966/77-igf-regional-events/igf-regional-and-national/2160-list-of-national-and-regional-igf-initiatives-2015 (Date of use: 12 December 2015)

http://www.intgovforum.org/cms/igf-initiatives (Date of use: 12 December 2015)

http://www.intgovforum.org/cms/mag/45-mag-membership/3030-mag-2016-membership-2 (Date of use: 10 September 2016)

http://www.intgovforum.org/cms/magabout (Date of use: 5 December 2015)

http://www.intgovforum.org/cms/wks2014/index.php/proposal/view_public/103 (Date of use: 11 January 2016)

http://www.intgovforum.org/cmsold/Contributions2009/Synthesis_Contribution_RPWG.doc (Date of use: 12 December 2015)

http://www.itu.int/en/events/Pages/Calendar-Events.aspx?sector=ITU-T (Date of use: 28 December 2015)

http://www.itu.int/en/ITU-T/about/Pages/default.aspx (Date of use: 26 December 2015)

http://www.itu.int/en/ITU-T/info/tsb/Pages/geninfo.aspx (Date of use: 25 December 2015)

http://www.itu.int/en/ITU-T/membership/Pages/Categories-and-Fees.aspx (Date of use: 23 October 2016)

http://www.itu.int/en/ITU-T/membership/Pages/default.aspx (Date of use: 26 December 2015)

http://www.itu.int/en/ITU-T/membership/Pages/Members.aspx (Date of use: 25 December 2015)

http://www.itu.int/en/ITU-T/regional-groups/Pages/default.aspx (Date of use: 28 December 2015)

http://www.itu.int/en/ITU-T/studygroups/2013-2016/02/Pages/mgmt.aspx (Date of use: 18 September 2016)

http://www.itu.int/en/ITU-T/studygroups/2013-2016/11/Pages/mgmt.aspx (Date of use: 18 September 2016)

http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf (Date of use: 24 April 2012)

http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf (Date of use: 21 July 2013)

http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf (Date of use: 21 July 2013)

http://www.itu.int/itunews/manager/display.asp?lang=en&year=2005&issue=05&ipage=internet&ext=html (Date of use: 13 November 2016)

http://www.itu.int/net/pressoffice/press_releases/2013/05.aspx#.VESyyVPlxnY (Date of use: 19 October 2014)

http://www.itu.int/net/wsis/docs/geneva/official/dop.html (Date of use: 26 December 2016)

http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/chapter_1.html (Date of use: 4 August 2013)

http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/foreword_chair.html (Date of use: 3 August 2013)

http://www.jesc.co.za/downloads/products/1%20AccessData/10%20FTK%20Information.pdf (Date of use: 20 February 2013)

http://www.justice.gov/archive/crs/pubs/principlesofgoodpolicingfinal092003.pdf (Date of use: 31 May 2015)

http://www.justice.gov/criminal/cybercrime/reporting.html (Date of use: 8 February 2013)

http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00602.htm (Date of use: 11 April 2014)

http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf (Date of use: 23 March 2013)

http://www.labsystems.co.in/drac.html (Date of use: 16 February 2013)

http://www.law.cornell.edu/uscode/text/18/1343 (Date of use: 14 December 2012)

http://www.legis.state.ak.us/basis/folioproxy.asp?url=http://wwwjnu01.legis.state.ak.us/cgi-bin/folioisa.dll/stattx99/query=*/doc/{t3744}/pageitems={body} (Date of use: 27 November 2012)

http://www.legis.state.wv.us/wvcode/code.cfm?chap=61&art=3C (Date of use: 12 November 2012)

http://www.merriam-webster.com/dictionary/fiscal (Date of use: 30 March 2015)

http://www.mext.go.jp/english/unesco/1304525.htm (Date of use: 14 August 2016)

http://www.michigan.gov/msp/0,1607,7-123-1589_3493_4602-143714--,00.html (Date of use: 8 February 2013)

http://www.mscode.com/free/statutes/97/045/0007.htm (Date of use: 18 November 2012)

http://www.nasa.gov/centers/ames/about/overview.html (Date of use: 24 April 2012)

http://www.nass.gov.ng/nass/legislation.php?id=103 (Date of use: 10 January 2013)

http://www.nationmaster.com/country/ni-nigeria/int-Internet (Date of use: 13 April 2012)

http://www.ndtv.com/article/south/hands-on-training-to-andhra-pradesh-police-officers-to-probe- cyber-crimes-318057 (Date of use: 5 February 2013)

http://www.net-security.org/article.php?id=34&p=1 (Date of use: 12 February 2013)

http://www.nij.gov/topics/crime/Internet-electronic/welcome.htm (Date of use: 8 February 2013)

http://www.npa.gov.za/UploadedFiles/NPA%20Strategic%20Plan%202012%20-%202017.pdf (Date of use: 19 February 2013)

http://www.npf.gov.ng/departments/d-department/crime-investigation (Date of use: 22 February 2013)

http://www.npia.police.uk/en/16761.htm (Date of use: 7 February 2013)

http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Date of use: 17 March 2015)

http://www.osdata.com/kind/history.htm (Date of use: 2 April 2012)

http://www.panix.com/~eck/computer-fraud-act.html (Date of use: 2 December 2012)

http://www.parliament.uk/documents/post/postpn271.pdf (Date of use: 5 February 2013)

http://www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html (Date of use: 8 December 2012)

http://www.pctools.com/security-news/cybercrime-international-concerns/ (Date of use: 8 March 2012)

http://www.publicservice.co.uk/news_story.asp?id=19047 (Date of use: 7 February 2013)

http://www.reportcybercrime.com/classification.php (Date of use: 24 April 2012)

http://www.sacw.net/article606.html (Date of use: 12 January 2013)

http://www.sadc.int/about-sadc/overview/history-and-treaty/ (Date of use: 31 August 2013)

http://www.salvationdata.com/data-recovery-examples/data-recovery-flow.htm (Date of use: 20 February 2013)

http://www.saps.gov.za/_dynamicModules/InternetSite/faqBuild.asp?myURL=273 (Date of use: 20 February 2013)

http://www.saps.gov.za/_dynamicModules/InternetSite/HOnewsBuild.asp?myURL=33 (Date of use: 20 February 2013)

http://www.saps.gov.za/docs_publs/legislation/country_report/part_two.pdf (Date of use: 19 February 2013)

http://www.scholarsworks.com/origin-problem-curb-kidnapping-problem-nigeria/#sthash.8dYOjJfQ.dpbs (Date of use: 20 January 2015)

http://www.scoop.it/t/governance-by-dr-lendy-spires-foundation?page=4 (Date of use: 12 December 2015)

http://www.scribd.com/doc/15938005/Cyber-Crime-Investigation-and-Cyber-forensic (Date of use: 21 March 2012)

http://www.secretservice.gov/ectf.shtml (Date of use: 8 February 2013)

http://www.shareyouressays.com/84485/short-essay-on-poverty-and-crime (Date of use: 17 January 2015)

http://www.sida.se/contentassets/21d3b77fac2844fd89779048c8b3cfe7/no-10.-methods-for-capacity-develpoment_2645.pdf (Date of use: 1 August 2017)

http://www.sophos.com/sophos/docs/eng/comviru/viru_ben.pdf (Date of use: 8 March 2012)

http://www.spamlaws.com/fraud-effects.html (Date of use: 9 April 2012)

http://www.ssr.org/DevelopingCountries (Date of use: 4 November 2017)

http://www.state.gov/r/pa/prs/ps/2012/12/201786.htm (Date of use: 18 April 2013)

http://www.state.tn.us/tccy/tnchild/39/39-13-528.htm (Date of use: 1 December 2012)

http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02 (Date of use: 29 December 2013)

http://www.thefreedictionary.com/taxonomy (Date of use: 27 September 2014)

http://www.un.org/cyberschoolbus/untour/subgen.htm (Date of use: 21 July 2013)

http://www.un.org/en/peacekeeping/sites/police/work.shtml (Date of use: 19 July 2014)

http://www.un.org/en/sc/ctc/docs/bestprac-interpol.pdf (Date of use: 16 April 2014)

http://www.uncitral.org/pdf/english/texts/electcom/computerrecords-e.pdf (Date of use: 2 August 2013)

http://www.unisys.com/unisys/about/company/history.jsp?id=209 (Date of use: 24 April 2012)

http://www.unodc.org/documents/human-trafficking/Toolkit-files/08-58296_tool_9-8.pdf (Date of use: 18 April 2015)

http://www.unodc.org/nigeria/en/eu-funded-project-sponsors-forensic-workshop.html (Date of use: 23 February 2013)

http://www.wgig.org/docs/WGIGpaperStakeholders.pdf (Date of use: 26 September 2015)

http://www.which.co.uk/news/2011/02/government-allocates-63m-to-fight-cybercrime-245078/ (Date of use: 13 April 2012)

http://www.wisegeek.com/what-is-information-technology.htm (Date of use: 6 April 2012)

http://www.wsfa.com/story/16555968/ala-gets-funding-to-fight-cyber-crime (Date of use: 18 April 2013)

https://aso.icann.org/documents/memorandums-of-understanding/memorandum-of-understanding/ (Date of use: 5 October 2015)

https://community.icann.org/download/attachments/5996930/AFRALO%20AfrICANN%20-%20Singapore%20.pdf?version=1&modificationDate=1373407641000&api=v2 (Date of use: 15 November 2015)

https://joinup.ec.europa.eu/sites/default/files/document/2014-12/United%20Kingdom%20Country%20Report.pdf (Date of use: 5 February 2013)

https://mandreptla.org/CalifPenalCode502.htm (Date of use: 11 November 2012)

https://meetings.icann.org/en/calendar (Date of use: 8 November 2015)

https://postalinspectors.uspis.gov/aboutus/lab.aspx (Date of use: 8 February 2013)

https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c344b (Date of use: 11 December 2015)

https://web.archive.org/web/20050511011954/http://unstats.un.org/unsd/mi/developed_new.htm (Date of use: 4 November 2017)

https://www.afnic.fr/medias/documents/afnic-internet-governance-guide-06-2008.pdf (Date of use: 2 December 2015)

https://www.afrinic.net/en/about-us/our-structure/bod (Date of use: 30 January 2016)

https://www.amsl.com/index.html (Date of use: 4 January 2016)

https://www.arin.net/about_us/membership/overview.html (Date of use: 30 January 2016)

https://www.arin.net/participate/governance/icann.html (Date of use: 3 October 2015)

https://www.arin.net/participate/how_to_participate.html (Date of use: 30 January 2016)

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=BuwzWQYv (Date of use: 11 November 2012)

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (Date of use: 22 July 2017)

https://www.fic.gov.za/SiteContent/ContentPage.aspx?id=1 (Date of use: 20 January 2013)

https://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00548.html (Date of use: 6 March 2015)

https://www.icann.org/community/explore?profile_search[badge_filters][]=staff_badge (Date of use: 28 November 2015)

https://www.icann.org/en/system/files/files/acct-trans-frameworks-principles-17oct07-en.pdf (Date of use: 13 March 2016)

https://www.icann.org/en/system/files/files/drd-ui-09sep13-en.pdf (Date of use: 10 October 2015)

https://www.icann.org/profiles/cherine-chalaby (Date of use: 10 September 2016)

https://www.icann.org/public-comments/dns-underserved-2014-05-14-en (Date of use: 28 November 2015)

https://www.icann.org/resources/pages/board-of-directors (Date of use: 10 September 2016)

https://www.icann.org/resources/pages/governance/bylaws-en#VI (Date of use: 8 November 2015)

https://www.icann.org/resources/pages/providers-6d-2012-02-25-en (Date of use: 28 September 2015)

https://www.icann.org/resources/pages/welcome-2012-02-25-en (Date of use: 26 September 2015)

https://www.ietf.org/iesg/ (Date of use: 2 January 2016)

https://www.ietf.org/iesg/members.html (Date of use: 10 September 2016)

https://www.ietf.org/iesg/members.html (Date of use: 4 January 2016)

https://www.ietf.org/list/ (Date of use: 2 January 2016)

https://www.ietf.org/meeting/past.html (Date of use: 4 January 2016)

https://www.ietf.org/newcomers.html (Date of use: 2 January 2016)

https://www.infosecurity-magazine.com/news/uk-government-cyber-security-operations-centre/ (Date of use: 5 February 2013)

https://www.intgovforum.org/cms/2011/Proposed%20Improvements%20to%20the%20IGF.PDF (Date of use: 6 December 2015)

https://www.intgovforum.org/cms/mag/45-mag-membership (Date of use: 5 November 2016)

https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf (Date of use: 28 April 2012)

https://www.itu.int/online/mm/scripts/gensel11 (Date of use: 19 September 2016)

https://www.itu.int/online/mm/scripts/mm.list?_search=ITU-T&_languageid=1&_foto=y (Date of use: 28 December 2015)

https://www.nro.net/ (Date of use: 30 January 2016)

https://www.nro.net/about-the-nro (Date of use: 30 January 2016)

https://www.nro.net/about-the-nro/nro-faq (Date of use: 30 January 2016)

https://www.nro.net/about-the-nro/regional-Internet-registries (Date of use: 30 January 2016)

https://www.nro.net/about-the-nro/the-nro-number-council (Date of use: 30 January 2016)

https://www.revisor.mn.gov/statutes/?id=609.891 (Date of use: 27 November 2012)

https://www.techopedia.com/definition/2432/Internet-society-isoc (Date of use: 9 January 2016)

https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/publication/ldc_list.pdf (Date of use: 12 October 2018)

https://www.unngls.org/index.php/engage-with-the-un/un-civil-society-contact-points/120-the-international-telecommunication-union-itu (Date of use: 23 December 2015)

https://www.unodc.org/documents/justice-and-prison-reform/Handbook_on_Effective_police_responses_to_violence_against_women_English.pdf (Date of use: 31 May 2015)

https://www.unodc.org/documents/southeastasiaandpacific/2012/05/cyber-crime/Bangkok_intro_presentation.pdf (Date of use: 4 November 2012)

https://www.unpei.org/sites/default/files/PDF/institutioncapacity/Ways-to-increase-effectiveness-SD.pdf (Date of use: 30 July 2017)

https://www.uschamber.com/issue-brief/safeguard-cross-border-data-flows (Date of use: 17 May 2015)

https://www.w3.org/2002/ab/ (Date of use: 10 September 2016)

https://www.w3.org/2010/04/w3c-vision-public/wiki/Newstd (Date of use: 1 May 2016)

https://www.w3.org/Consortium/facts (Date of use: 23 January 2016)

https://www.w3.org/Consortium/membership-faq (Date of use: 23 January 2016)

https://www.w3.org/Consortium/membership-faq#who (Date of use: 23 January 2016)

https://www.w3.org/Consortium/mission (Date of use: 17 January 2016)

https://www.w3.org/People/ (Date of use: 23 January 2016)

DOCUMENTS ISSUED BY INTERNATIONAL ORGANISATIONS, INTERNET GOVERNANCE BODIES, CONVENTIONS, DIRECTIVES, REPORTS, ETC

International Organisations

APEC

Recommendation by the APEC telecommunications and information working group (TEL) to APEC senior officials (SOM) for an APEC Cybersecurity strategy

AFRICAN UNION

African Union convention on Cyber Security and Personal Data Protection, 2014

Council of Europe

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, 2006 (ETS No. 189)

Council of Europe Convention on Cybercrime, 2001 (ETS No 185)

Explanatory Report on Council of Europe Cybercrime Convention (ETS No 185)

European Union Directive on Data Protection (Directive 95/46/EC)

United Nations

Tenth United Nation Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, April 2000

United Nations General Assembly Resolution 55/63 of 4 December 2000 on Combating the Criminal Misuse of Information Technologies

United Nations Resolution 56/121 of 19 December 2001 on Combating the Criminal Misuse of Information Technologies

United Nations Resolution 40/71 of 1985 on Legal Value of Computer Records

Internet Corporation for Assigned Names and Numbers (ICANN)

Bylaws for Internet Corporation for Assigned Names and Numbers (ICANN)

International Telecommunication Union

Constitution of the International Telecommunication Union, 1992

Convention of the International Telecommunication Union,1992

INTERPOL
INTERPOL Constitution

International Criminal Court
Rome Statute of the International Criminal Court

Rules of Procedure and Evidence

Organisation for Economic Co-operation and Development
OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

UNITED STATES OF AMERICA
Senate Bill S.1469 International Cybercrime Reporting and Cooperation Act, 2011

United States Congressional Serial Set, Serial No 15006, Senate Treaty Documents No 9-12 (United States Government Printing Office Washington 2006) 333-335

TABLE OF CASES

LIBYA

The Prosecutor v Saif al-Islam Gaddafi and Abdullah al-Ssenussi ICC-01/11-01/11

NIGERIA

Aoko v. Fagbemi (1961) 1 All NLR 400
FRN v. Ifegwu (2003) 15 NWLR Pt. 842 Pg. 113

SOUTH AFRICA

S v Mashiyi 2002 (2) SACR 387
S v Harper 1981 (1) SA 88
Narlis v South African Bank of Athens 1976 (2) SA 573
Nissan v Marnitz NO &Ors 2005 (1) SA 441 (SCA)

UNITED KINGDOM

DPP v Jones [1997] 2Cr App R, 155, HL163
R v Gold [1988] 2 WLR 984
R v Smith (Wallace Duncan) (No4) [2004] 3 WLR 229
R v Waddon 6 April 2000 (unreported)
R v Bedworth (1991)
DPP v Bignell [1998] 1 Cr App R8
Sweet v Parsley (1970) AC 132
DPP v Stonehouse [1978] AC 55

UNITED STATES OF AMERICA

United States v Riggs 739 F. Supp 414 (N.D. Ill. 1990)
United States v Schreier 908 F.2d645 (10th Cir. 1990)
US v SACCOCCIA 18 F. 3d 795 (1994)

TABLE OF STATUTES

AUSTRALIA

Australian Cybercrime Act, 2001

INDIA

Indian Copyright Act of 1957 (as amended)
Indian Information Technology Act of 2000
Information Technology Act of India, 2000
Information Technology Amendment Act of India, 2008

LIBYA

Libyan Criminal Procedure Code

NIGERIA

Advance Fee Fraud and Other Fraud Related Offences Act of Nigeria, 2006
Child Right Act (Nigeria), 2003
Constitution of the Federal Republic of Nigeria, 1999
Constitution of the Federal Republic of Nigeria, 1999 (as amended)
Criminal Code Act, Laws of the Federation, 2004
Nigerian Child's Right Act of 2003
Nigerian Copyright Act; Laws of the Federation of Nigeria 1990 (as amended)
Nigerian Cybercrime Act of 2015
Nigerian Economic and Financial Crime Commission (Establishment) Act of 2004
Nigerian Evidence Act Laws of the Federation, 2011
Nigerian Evidence Act, Laws of the Federation, 2004

SINGAPORE

Computer Misuse Act of Singapore, 1993

SOUTH AFRICA

Constitution of the Republic of South Africa, 1996
Copyright Act of South Africa, 1978

Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of South Africa, 2007 (as amended by the Judicial Matters Amendment Act 66 of 2008)
Electronic Communications and Transactions Act of South Africa, 2002
Films and Publications Act 65 of South Africa, 1996
Financial Intelligence Centre Act of South Africa, 2001
Interception and Monitoring Prohibition Act 127 of South Africa, 1992.
Judicial Matters Amendment Act 66 of 2008
Lotteries Act of South Africa, 1997
National Gambling Act of South Africa, 2004
Prevention of Organized Crime Act of South Africa, 1998
Regulation of Interception of Communications and Provision of Communication Related Information Act (RICPCRIA) of South Africa, 2002
South African Copyright Act 98 of 1978 (as amended)
South African Criminal Procedure Act 51 of 1977 (as amended)
South African Cybercrime Bill
South African Electronic Communications and Transactions Act of 2002
South African Judicial Matters Amendment Act 66 of 2008

THAILAND

Constitution of the Kingdom of Thailand, 2007
Criminal Code of Thailand, 1956
Thailand Penal Code

UNITED ARAB EMIRATES

United Arab Emirates Federal Law No 2 The Prevention of Information Technology Crimes, 2006

UNITED KINGDOM

Communications Act (UK) of 2003
Communications Act C.21 of United Kingdom, 2003
Computer Misuse Act, 1990
Copyright and Related Rights Regulations (UK), 2003
Copyright, Designs and Patent Act of United Kingdom, 1988
Criminal Justice Act C.33 of United Kingdom, 1994
Criminal Justice Act of 1988
Criminal Justice and Public Order Act c. 33, 1994
Data Protection Act, 1998

United Kingdom Data Protection Act of 1998
Forgery and Counterfeiting Act C.45 of United Kingdom, 1981
Fraud Act C.35 of United Kingdom, 2006
Police and Justice Act (UK), 2006
Protection of Children Act C.37 of United Kingdom, 1978.
Public Order Act C.64 of United Kingdom, 1986
Regulation of Investigatory Powers Act C.23 of United Kingdom, 2000
Serious and Organised Crime Act of United Kingdom, 2005
Serious Crime Act of United Kingdom, 2007
United Kingdom Coroners and Justice Act, 2009
United Kingdom Forgery and Counterfeiting Act c.45, 1981
United Kingdom Fraud Act c.35, 2006
United Kingdom Theft Act c. 60, 1968

UNITED STATES OF AMERICA

18 USC 1030 – Crimes and Criminal Procedure – Fraud and Related Activity in Connection with Computers
Alabama Computer crime Act, 1985
Alaska Statute
Code of Criminal Justice of New Jersey, 1995
Computer Crime and Abuse Act of West Virginia
Computer Fraud snd Abuse Act 18 United States Code Section 1030
Computer Systems Protection Act of Georgia State, 1991
Criminal Code of Alabama
Criminal Code of Delaware State
Criminal Code of Mississippi, 1972(as amended)
Criminal Code of Utah State
Florida Statutes
General Laws of Rhode Island, 2000
Minnesota Statutes 2012
Oklahoma Statutes
Penal Code of California State
Revised Statutes of Louisiana, 2011
Section 402 Restatement (Third) of Foreign Relations Law of the United States Section of 1987
Tennessee Code Annotated Section 39-13-528
Texas Penal Code
Title 17 USC Section 506
Title 18 Pennsylvania Statutes Section 6318

Title 18 USC Section 2319
Title 18 United States Code Section 1028
Title 18 United States Code Section 1030
Title 18 United States Code Section 1343
Title 18 United States Code Section 1343
Title 18 United States Code Section 1462
Title 18 United States Code Section 1463
Title 18 United States Code Section 2251
Title 18 United States Code Section 2252
Title 18 United States Code Section 2314
Title 18 United States Code Section 2319
Title 18 United States Code Section 2510-2522
United States of America Computer fraud and Abuse Act, 1986
United States of America Constitution
United States of America Electronic Communications Privacy Act of 1986
Virginia Code
West Virginia Code
Wisconsin Statute