AN APPRAISAL OF THE LEGAL REGIME FOR INFORMATION TECHNOLOGY AND CYBERSECURITY IN NIGERIA

BY

Dimson Diffiwuka DIMAS,

DEPARTMENT OF PUBLIC LAW,
AHMADU BELLO UNIVERSITY,
ZARIA

JANUARY, 2020

AN APPRAISAL OF THE LEGAL REGIME FOR INFORMATION TECHNOLOGY AND CYBERSECURITY IN NIGERIA

BY

Dimson Diffiwuka DIMAS,
LLM/LAW/103946/2014-2015.

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

DEPARTMENT OF PUBLIC LAW,
AHMADU BELLO UNIVERSITY,
ZARIA

JANUARY, 2020.

DECLARATION

I, declare that this dissertation titled an Appraisal of the Legal Regime for Information Technology and Cybersecurity in Nigeria has been carried out by me in the Department of Public Law, Ahmadu Bello University, Zaria, Nigeria. All information derived from the various literatures has been duly acknowledged in the text and a list of references provided. No part of this dissertation was previously presented for another degree or Diploma at this or any other institutions.

_____

Dimson Diffiwuka DIMAS,
January, 2020

CERTIFICATION

This dissertation titled An Appraisal of the Legal Regime for Information Technology and Cybersecurity in Nigeria, by Dimson Diffiwuka Dimas, meets the regulations governing

the award of the degree of Master of Laws-LLM of the Ahmadu Bello University, and is approved for its contribution to knowledge and literary presentation.

_____	_____	_____
Chairman, Supervisory Committee Prof. B. Babaji	(Signature)	(Date)
_____	_____	_____
Member, Supervisory Committee Prof. D. C. John	(Signature)	(Date)
_____	_____	_____
Head of Department, Public Law Prof. A. I. Bappah	(Signature)	(Date)
_____	_____	_____
Dean, School of Postgraduate Studies Prof. Sani Abdullahi	(Signature)	(Date)

DEDICATION

This research work is dedicated to my late mother Patricia Y. Dimas who inspired and taught me to work hard, prayed for me and assured me of a greater future. Her memories are ever cherished.

ACKNOWLEDGEMENT

I am profoundly grateful to the Almighty God for his guidance and protection throughout this sojourn of learning. My special gratitude to my amiable, caring, loving and ever supportive wife, Abigail Dimson, and to my parents, Mr. & Mrs. Dimas D. Jamare Jen, for their combined prayers and admonition which have made a responsible, hardworking and visionary personality out of me.

I deeply appreciate my inspiring and amiable supervisors, Professor. B. Babaji (Dean, Faculty of Law, ABU) and Professor. D.C. John, erudite scholars of great distinction. I

appreciate them for their thorough insights, guidance, directives and tremendous efforts, notwithstanding their rigorous schedules, which ensured the success of this work. Their arms were always open whenever I needed assistance.

Special appreciation to Professor A. I.Bappah, the Head of Department, Public Law, ABU, my lecturer and examiner; his comments, criticisms and suggestions added depth to this work. I appreciate the sincere commitment of the following lecturers in the Faculty of Law, Ahmadu Bello University, Zaria, Professor, M.T. Ladan, Professor Y. Aboki, and Zainab Haruna (Mrs.) for their dedication and diligence towards mentoring and nurturing me, it is my prayer that God Almighty will reward them mightily. I am greatly indebted to Dr. Onuh Paul Igoche for his in-depth and insightful criticism and guidance that has produced this piece, he is truly a mentor.

This work will be incomplete without appreciating my friends and colleagues, Salawu John Onipe, Esq., Ogana Eteya, Esq., and Elisha Oloruntoba, Esq., for their moral and material supports towards the successful completion of this noble programme.

My Amiable and indefatigable General Manager, MTN Nigeria Communications Plc, Mrs. Ifeoma Utah, my former Principal Joe Kyari Gadzama, SAN, and my entire colleagues at J-K Gadzama LLP, I appreciate them all. I am also indebted in gratitude to all who contributed in diverse ways to the success of this programme whose names are not mentioned for several reasons.

ABSTRACT

The increasing dependence upon the convergent Technology and network infrastructure has given rise to new and multifarious risks to national security, governance and business processes. Information and its attendant infrastructure has come under persistent threat of attack and sophisticated information warfare. Owing to the economic, political and social risks associated with a concerted cyber-attack on a nation, various governments globally have introduced regulations aimed at protecting and defending information of national importance. As a result of these perilous circumstances, securing the cyberspace has become a shared responsibility of governments, business, organizations, and individual users who develop, own, provide, manage, service and use these information systems and network. The startling growth of the internet and its wide acceptance has led to increase in security threats. In Nigeria, several internet assisted crimes known as cybercrimes are committed daily in various forms. There is the rise of politically motivated attacks; the rapid adoption of cloud services and the application programming interface (API) and its attendant cybersecurity threat; the prevalence of phishing attacks and the increasing malware attacks. According to the Nigerian Communications Commission in 2017, Nigeria ranked third globally in cybercrimes behind the United Kingdom and the United States. The realization of these challenges explains the several efforts made by Nigeria from the early 1960s to grapple with this social malaise through the enactment of appropriate legislations. This work seeks to appraise, the possibility of properly regulating the provision and usage of ICT and other services in Nigerian cyberspace; the adequacy of established Institutional Framework for cyber laws; the degree of international cooperation; enforcement mechanisms on criminal activities in the cyberspace; and the efficiency in handling the burden of multiple regulations of similar activities in the Nigerian cyberspace. The researcher adopted the doctrinal research method in the gathering of information. The findings of the research revealed essentially that, though several efforts have been made by the government and private sector in Nigeria to tackle cyber threats, these are not sufficient, given the dynamic and evolving nature of the cyber and ICT regime. It is therefore recommended that legislations in Nigeria need to keep pace with changes in the cyberspace. This can be achieved through amendments and enactments of new legislations. Reforms are needed to meet the prevalent and sophisticated cyber challenges. Additionally, adequate awareness and security measures need to be in place and enforced, as part of the solutions to cyber threats.

TABLE OF CONTENT

TABLE OF CASES

TABLE OF STATUTES

LIST OF ABBREVIATIONS

ACPO -Association of Chief Police Officers

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

JHA	-Justice and Home Affairs Council (EU)
LEA	-Law Enforcement Authority
MLAT	-Mutual Legal Assistance Treaty
MoU	-Memorandum of Understanding
MSSP	-Managed Security Service Provider
n/g CERT	-National/Governmental CERT
NHTCU	-National High Tech Crime Unit (NL)
NIS	-Network and Information Security
NWLR	-Nigerian Weekly Law Report
OCSIA	-Office for Cyber Security and Information Assurance (UK)
PCSIRT	-Product CSIRT
PPP	-Public Private Partnership
RAT	-Remote Access Tool
Rf.C	-Request for Comments
SC	-Supreme Court
TRANSITS	-Training programme for CERTs

CHAPTER ONE

GENERAL INTRODUCTION

1.1 Background to the Study

The continuous dependence on the internet and network infrastructure has given rise to new and multiple threats to national security, governance and business undertakings. Information and its attendant infrastructure has come under persistent threat of attacks and information warfare, owing to the economic, political and social risks associated with intensive cyber-attack on a nation. Various Governments globally have introduced Risk Management Framework by way of regulations aimed at protecting and defending information of serious national importance. Managing the inherent risks requires that the various players and stakeholders in the cyber industry act concertedly to address cybersecurity issues appropriately.

Our nation's critical infrastructure comprises public and private institutions in the agriculture, water, public health, emergency services, government, defence, industrial base, information and communications, energy, transportation, banking and finance, postal and shipping sectors. The Cyberspace is their nervous system-the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fibre optic cables that allow our critical infrastructures to work. Therefore the healthy functioning of our cyberspace is essential to our economy and national wellbeing.[1]

In the words of Jeffrey Walker "Because the entire law of war regime has been built upon a West phalian foundation, the transformative properties of cyber warfare are just as breath-taking. We are left pondering some fundamental questions - what constitutes force? What is a hostile act? When is self-defense justified in response to a cyber-attack? Is the use of traditional means of force ever justified in response to a cyber-attack? These are not easy questions and the international legal regime is lagging far behind the problems presented by the increasingly sophisticated technological possibilities in this area".[2]

Cyberspace, as the fifth common domain – after land, sea, air and outer space, is in great need for coordination, cooperation and legal measures among all nations. A cyberspace treaty or a set of treaties at the United Nations level should be the framework for peace, justice and security in the cyberspace. According to a survey by the Pew Research Centre exploring the future of cyber-attacks, some 61% of the respondents said that a major attack causing widespread harm would occur by 2025. Cross, the chief scientist at Internet Time Group, said: "Connectedness begets vulnerability." Livingston, author and president

[1]Official website of the Department of Homeland Security, *National Strategy to Secure Cyberspace*www.dhs.gov/national-strategy-secure-cyberspace accessed on the 13-05-16 10:40 am

[2] Walker J. K. (2001) 'The Demise of the Nation-State, the Dawn of new Paradigm Warfare, and a future for the profession of arms*, Air Force Law Review* (51:2001pdf available at www.dhs.gov/national-startegy-secure-cyberspace accessed on the 25-04-2016 10:40 am

of Tenacity Media, responded, "Cyberwar is the battlefield of now. Don't kid yourself. Battlefields in Sudan, Afghanistan, and Syria are real, but there is a new battlefield and every day wars are won and lost between individuals, businesses, and countries." He added that the Pentagon is regularly engaged in "digital spats". "We really have no idea how deep this goes, but we are much closer to Gibson's vision in the seminal cyberpunk novel Neuromancer than any of us would like to admit."[3]

The information technology revolution associated with the internet in Nigeria has brought about a new wave of crime. A very few criminally minded youth in the country are stealing and committing atrocity with the aid of internet online business transactions. The internet online business services, which ordinarily ought to be an advantage to the nation, because of the numerous opportunities associated with, is fast becoming a source of discomfort and worry due to the atrocities being perpetrated using the internet platform.

Cybercrime has come as a surprise and a strange phenomenon that for now lives with us in Nigeria. Nigeria was recently identified as the innocent and ignorant passive player in cyberspace knowledge Olympiad. The capture of Al Qaeda's operative, Muhammad Naeem Noor Khan, provided the Pakistani and American Intelligence Authority with some of Al Qaeda's Internet Communication Strategy. It also identified that Nigerian Websites and Email System were used by Al Qaeda to disseminate internet information[4]. This has once again brought up the pertinent questions of the safety and security of Nigeria's national cyberspace. The availability of cyberspace and the integrity, authenticity and confidentiality of data in cyberspace have become vital questions of the 21st century.

[3] Lee R., Janna A. and Jennifer C. (2014) Internet & Technology: Cyber Attacks Likely to Increase, *Pew Research Center*.http://clapway.com/2015/08/02/is-the-fbi-ready-to-ward-off-cybersecurity-attacks432/#ixzz3hjvCQWWH accessed on 23/05/2018 11:00am

[4]Aladesanmi T, Afolabi B., Oyebisi, T. (2012), Assessing Network Services and Security in Nigeria Universities, *Journal of Computer Science and Its Application* V. 19 p.2

Ensuring cybersecurity has thus turned into a central challenge for the state, business and society at national and international levels.[5]

1.2 Statement of the Problem and Research Question

The startling growth of the internet and its wide acceptance has led to increase in security threats. In Nigeria on a daily basis, several internet assisted crimes known as cybercrimes are committed in various forms. There is the rise of politically motivated attacks; the rapid adoption of cloud services and the application programming interface (API) and its attendant cybersecurity threat; the prevalence of phishing attacks and the increasing malware attacks. According to the Nigerian Communications Commission in 2017, Nigeria ranked third globally in cybercrimes behind the United Kingdom and the United States.

Cyber criminality is a well-established trend, and the Nigerian Cyberspace is constantly under pressure by malicious activities, especially those targeted at the financial sector and unsuspecting users. The Central Bank of Nigeria (CBN), asserted that in 2007 alone, the financial industry lost N7.3Billion to cybercrime[6]. From global perspective, Nigerian Cyberspace is a conduit for growing cyber-criminality where cybercrimes are flourishing[7]

The availability and integrity, authenticity and confidentiality of data in cyberspace have become vital questions of the 21st century. Ensuring cybersecurity has thus turned into a central challenge for the state, business and society at national and international levels. Consequently, cybersecurity has become a national concern. The exponential increase in cyber threats has become a strong issue that should not be overlooked. The impact of

---

[5] Celeb I. *etal* (2015)*Regulating Cyber Security: Cyber security and law* , ER p.1, https://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1 Accessed on 20/08/2016:10:30am

[6] I. Nnadozie (2013), *Nigeria will lose $15million to Cyber theft related cases by 202* http://www.thenigerianvoice.com/nvnews/126855/50/nigeria-will-lose-15million-to-cyber-theft-related.html. [Accessed March 2020].

[7]Balancing Act Africa, "Nigeria Ranked Third in the World for Cyber-Crime," http://www.balancingact-africa.com/news/en/issue-no-302/computing/nigeria-ranked-third/en#sthash.v598OgZB.dpuf.

illegal activities in the cyberspace can be felt on the lives, economy and the international reputation of the nation. Therefore, this research focuses on the various efforts made and steps taken to regulate the cyberspace in Nigeria.

This research has therefore outlined the under mentioned issues as clearly representing the special legal problems which the ICT regime has created beyond the comprehension of traditional criminal laws, law of contract, tax law, and commercial law. This research seeks answers to the following issues:

1. Whether it is possible to properly regulate the provision and usage of ICT services and other activities in Nigerian cyberspace.

2. Whether Nigeria has adequate established legal and institutional framework for coordination and implementation of cyber laws.

3. Whether Nigeria has harnessed sufficiently degree of International Cooperation in its fight to secure the cyberspace.
4. Whether Nigeria has adequate specialised enforcement mechanisms on criminal activities in the cyberspace; if there is any anybody, organization or entity set up by the government to investigate, monitor and to enforce cyber laws for the purpose of punishing cyber criminals in Nigeria.
5. Whether the government of Nigeria has tackled the challenges posed by Multiple-regulations (of the same aspects of telecommunications operations) by two or more government Ministries, Departments and Agencies ("MDAs"), which presents the hazard of regulatory intervention by these entities working at cross purposes to the detriment of the affected operator?

1.3 Aim and Objectives

The aim of this research is to appraise the regulatory framework for cybersecurity and information technology in Nigeria in order to assess the existence, adequacy and efficiency of the legal and regulatory framework underpinning the cybersecurity and the information technology regime in Nigeria. The specific objectives of this research are:

1. To examine whether it is possible to properly regulate the provision and usage of ICT services and other activities in Nigerian cyberspace.
2. To appraise whether Nigeria has adequate established legal and institutional framework for coordination and implementation of cyber laws, in order to abate the apparent vulnerability of the cyberspace, and the likely devastating effect to the whole nation.
3. To appraise the degree of international cooperation Nigeria has garnered in its fight to secure its cyberspace.
4. To appraise the various efforts Nigeria has made to regulate its cyberspace with a view to finding out if Nigeria has adequate specialised enforcement mechanisms on criminal activities in the cyberspace
5. To appraise the extent to which the Government of Nigeria has properly tackled the challenges posed by multiple regulations of similar activities in the cyberspace by two or more government agencies in Nigeria.

1.4 Justification

With Nigeria being at a critical moment in cybersecurity and information technology policy formulation, this research work would be relevant in providing useful and important information as well as serve as a depository of knowledge for stakeholders in the cyber industry. This information would be helpful in assessing the present cybersecurity posture of Nigeria, and making contributions and recommendations which would guide

cybersecurity strategy implementation in Nigeria. The knowledge provided by this research would provide legal experts/researchers, academicians, students of law and users of information, with the necessary competencies and skills to function effectively in the institutions of higher learning, and in both the public and private sectors of the Nigerian economy. It would also provide necessary information as to the viability of the policies and strategy frameworks with respect to the Nigerian cyberspace. The work would also provide insight to the legislature in terms of making further legislation, amending or consolidation the present ones by way of other policy frame work.

Finally, this research work would contribute to existing knowledge by unveiling the efforts made at securing the cyberspace as well sustaining the information technology regime in Nigeria, the adequacies or otherwise of these measures as well as expose *lacunas* where identified. This work would also form the basis for further research in the cyberspace and information technology related fields in Nigeria, as build-up from the findings made from the research work.

1.5 Scope of the Research

The scope of this work is delimited to the legal and policy frameworks on cybersecurity and information technology in Nigeria. This research particularly glances at international trends and best practices in cybersecurity by reviewing global, regional, sub-regional and national treaties, protocols, conventions, laws, policies, regulations and other instruments that will serve as yardstick for evaluating the legal and policy readiness of Nigeria in respect of the cyberspace and related matters.

1.6 Research Methodology

This work seeks to appraise the legal and regulatory framework for ensuring cybersecurity and advancing information technology in Nigeria, hence, this research shall be carried out on the basis of the doctrinal research methodology; by placing reliance on the review and analysis of existing literatures, articles, international, regional, sub-regional and national conventions, protocols, treaties and other textual materials on the subject matter. The Nigerian legislations, cases and policies that relate to this research subject would also be considered.

1.7 Literature Review

This is an emerging field of research, especially academic research, in Nigeria. Few scholars and researchers have ventured into research on cyberspace related matters. This is largely either because they are yet to come to terms with the operations of the cyberspace or they are not able to separate activities in the cyber and human space. This research work reviews legislations, cases, books, articles, journals as well as global and regional treaties, protocols, conventions that border on the cyberspace.

The term "cyberspace" first appeared in the 1980s in the work of science fiction author William Gibson, first in his 1982 short story "Burning Chrome" and later in his 1984 novel "Neuromancer".[8] Shortly thereafter, the word became prominently identified with online computer networks. Gibson asserted that "Cyberspace is a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity, lines of light ranged in the non-space of the mind, clusters and constellations of data, like city lights, receding."[9]

[8] Scott T.William G. (1948), *Father of Cyberspace*. Ace Books, New York p.72
[9] Gibson, W. (1984) *Neuromancer*. Ace Books, New York p.69.

Drastler Jr.[10] has this to say about the cyberspace, "Much of the hoopla about 'cyberspace law' relates more to climbing the steep learning curve of [the internet's] technological complexities than to changes in fundamental legal principles. To the extent there was 'new' law, it was almost entirely case-by-case development, in accordance with the accepted and well understood basic legal principles, albeit applied to new technology and new circumstances". This author addresses generally the issue of conventional crimes as it relates to the advent of the technological regime, this research goes further by looking at the peculiarity of the Nigerian situation in regards to the protection of the cyberspace and information technology.

Akuta[11] asserted that there is increasing reliance on computers to perform key functions that makes every day living more convenient. Computers have spurred economic and business growth and improvements. Critical infrastructures depend on computers. This situation has given rise to legislations in many countries to criminalize computer-assisted crimes and/or crimes against computer systems. Computer or cybercrimes are particularly relevant to Nigeria because it seems that out of the top ten countries in the world with a high level of cybercrime prevalence, Sub-Sahara Africa is host to four of these countries (Nigeria, Cameroon, Ghana and South Africa). This author focuses on the rise of crimes perpetrated through the use of computers, this research work however considers holistically the rise of both computer and all cyber related threats in Nigeria, and efforts made to secure Nigeria's cyberspace.

Chukkol[12] states that "crimes committed by a person or group of persons via cyberspace and computers are cybercrimes or computer crimes. Dealing with crimes that affect the

[10]Drasler. Jr., (2001) Cyberlaws. *Law Journal Press*; Lslf edition p.1-3
[11]Akuta, E.A., (2011) CombatingCybercrime in Sub Sahara Africa: A discourse on law, policy and practice *Journal of Peace, Gender and Development Studies*, Vol.1 No.4 pp 129-137 at p. 129 print pdf retrieved on 12/05/2016
[12]Chukkol, K.S(2010) *The Law of Crimes in Nigeria*, (Revised ed)., ABU Press, Zaria

cyberspace, he further observed that, they are limitless if stock of them is to be taken. Hence cybercrimes and computer related offences include, fraud, theft of computer processor of central processing unit (CPU), theft of handsets, mobile or cellular phones, hacking and distribution of viruses and worms, credit card fraud, software piracy, conspiracy, forgery, obscenity and pornography and advance fee fraud (ie.419). This author focuses on the various threats to the cyberspace by pointing out what cyber and computer crimes are. This research work takes a further look at Nigerian cyberspace vulnerability, and the efforts made towards safeguarding the cyberspace in Nigeria.

Ladan[13] asserted that cybersecurity is not only a framework or a set of on-time actions, but it is also a set of on-going efforts focused on performing periodic assessments and monitoring of aforementioned policies, as well as enforcing compliance with existing regulations and laws, and applying sanctions in the case of violations. He further stated that cyber laws prevent or reduce large scale damage from cybercriminal activities by protecting information access, privacy, communications, intellectual property and freedom of speech related to the use of the internet, websites, emails, computers, cell phones, software and hardware, such as data storage devices. This author looks critically at the global, regional and national efforts towards enacting cyber laws and policies as well as securing the cyber security. This research work however does not only look the various efforts made globally towards cyber laws and cybersecurity but uses the global efforts as guage to assess how Nigeria has fared in its drive towards cybersecurity.

Onoja[14] postulated that Nigeria and Nigerians have been accused of internet-based advance fee fraud and other cybercrimes. The country is alleged to be the origin of a high volume of

[13]Ladan M.T (2015) *Cyber Law and Policy on Information and Communications Technology in Nigeria and ECOWAS*, ABU Press Zaria.
[14]Onoja E.O(2015) *Fundamental Principles of Nigerian law*, Green World Publishing Company, Akwanga, Nasarawa State, p.605

such crimes, while Nigerians have been linked with such crimes in various parts of the globe. Some embassies have gone to the extent of warning their citizens that, they can shake the hands of Nigerians, but they should count their fingers after the handshake.[15] This author aimed at exposing the menace of cyber related crimes in Nigeria and how it has affected the image of Nigerians abroad. This work goes a step further to consider the efforts made over time by Nigerian government to combat cybercrimes and secure the cyberspace.

Oluwafemi & Agada[16] posited that Nigeria is interestingly at a defining moment in the establishment of a cybersecurity policy and strategy framework. This is only an aspect of the numerous processes in their developmental stages concerning national security. In June, 2014, the National Cyber Security Policy and Strategy drafts were officially presented at a symposium held in Lagos. In 2015, the Nigerian President assented to the Nigerian Cyber Crime bill. The cyberspace, characterized by an unrestricted borderless nature, the importance of security policy implementation through standardized and functional strategies cannot be overemphasized. This explains why the government of Nigeria has continued to solicit for the active support, participation and contributions of stakeholders from relevant sectors towards achieving increased national cybersecurity.[17] These authors examined the efforts the Nigerian government has made in securing the cyberspace as a national security prerogative, however this work examines, not only the efforts made overtime, but the adequacy or otherwise of these efforts.

Chuks[18]posited that cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing business security and revenue at risk. It can harm

[15]ibid
[16]Oluwafemi O.&Agada D. O. (2015) National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis**:** *International Journal of Cyber Criminology*. Vol. 9 (1): 120–143. pdf retrieved on 15/05/2016
[17]*ibid*
[18]Chuks O. (2014) *Examining Industry "Cybersecurity Governance and Corporate Leadership*. Paper presented at the 1st National Cybersecurity forum June18-19 2014, Eko Hotel and Suites, Lagos

an organization's ability to innovate and to gain and maintain customers. This author examines the risk associated with cybersecurity vulnerability while this work considers the efforts made towards curbing these risks.

Ifeanyi, and Obalum,[19] stated that presently, many factories, hospitals, schools, governments, and business offices are totally dependent on computer programs, and any slight anomaly can cause grave havoc which may shut down entire systems or cause problems that may not be solved for a long time. In addition to this, a huge amount of money is spent on preventing hacking attacks or clearing problems created by hacking. The effect of computer hacking is quite detrimental in exploiting information like personal data, social security numbers, credit card numbers, bank account data and personal photographs. That is why the law has become very interested in tackling hacking. Hacking has become an issue in legal systems because of its new-face when compared to other traditional offences.[20]These authors look at the potential risks associated with dependence on computer regime, this work however looks at both potential and apparent risks associated with the computer regime and the various efforts made towards tackling these risks.

Natalie and Carolina [21] talking about cybersecurity postulated that; in practice, outward expressions of cybersecurity include domestic public policy and laws (creation of cybersecurity agencies, such as the United States' Cyber Command), international public policy discussions (talks around creating an International Telecommunication Union(ITU)/United Nations(UN) cybersecurity treaty), private business practices (anti-virus software, notification programs by internet Service providers (ISPs), firewalls), online surveillance (often by governments), and technical community practices aimed at

[19]Ifeanyi, A. N and Obalum, D. C (2015) Hacking: The New Face of Cybercrime in Nigeria. *African Journal of Law and Criminology,* V, 5 (1), p. 48
[20]*ibid*
[21] Natalie G. and Carolina R. (2015) *Cyber Security and Human rights (*1**)_4.pdf** retrieved from https://www.uhd.edu/computing/helpdesk/documents/virusfacts.pdfon 12/3/16 10:20am

maintaining the critical infrastructure of the Internet (Internet Engineering Task Force is one of these independent technical agencies)[22]. They further stated that the understandings of these are essentials to the understanding of the basics of cybersecurity: Cybersecurity; Internet security; Information security; Critical infrastructure; Cyber space; Cybercrime; Cyberwarfare; Cyber threat.[23] Here the authors pay particular attention to the cyberspace in relation to the US approach; this research work however shall focus attention on the Nigerian cyberspace.

Abraham, [24] asserts that society has become dependent on cyber systems across the full range of human activities, including commerce, finance, health care, energy, entertainment, communications, and national defence. "The globally-interconnected digital information and communications infrastructure known as 'cyberspace' underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security."[25] The author focuses on the US cyberspace; however, this research work would focus on the Nigerian cyberspace borrowing from the US experience.

Richard, (2009)[26] asserted that the vast majority of the computers that make up cyberspace are owned and operated by private organizations. Within the Federal Government, most agencies manage their own cybersecurity more or less independently. Even the research, development and production of computer technology are mostly handled by private companies, for purposes unrelated to national security. When computer networks connect across national boundaries, questions of sovereignty and jurisdiction become complex

[22] *Ibid*
[23] *ibid*
[24] Abraham D. Sofaer, David Clark, and Whitfield Diffie (2009) *Cyber Security and International Agreements,* Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy retrieved from http://www.nap.edu/catalog/12997.html accessed 2/2/2018 10:20am
[25] The White House (2009), *Cyberspace Policy Review*: Assuring a Trusted and Resilient Information and Communications Infrastructure, p.III
[26] Richard, M. (2009) Securing the Cyberspace; Guarding the new frontier: *National Security Watch,* 25 August 2009 pdf retrieved 20/2/2018 10:20am

indeed. All these make it very difficult to secure the cyberspace. Much of cybersecurity focuses on defence: protecting computers, data and networks from attackers. This is necessary, but not sufficient. Information technology evolves quickly, and cyber defenders are always playing catch-up with attackers. Computer security experts say that staying ahead of the constantly adapting enemy is simply not possible. Trying to find vulnerabilities in advance and predict methods of attack does not provide an effective defence. Ideally, the United States would deter attacks with the threat of punishment or retribution. But going on offense—taking the fight to the enemy—is highly problematic.[27] The Author in this text lays more emphasis on the US cyberspace; however this research work lays emphasis on the Nigerian situation.

1.8 Organizational layout.

This work is structured in five chapters. Chapter one comprises matters such as General background to the study, aims and objectives of the study, research methodology, scope of the study, literature review, justification, and organizational Layout.

Chapter two deals with conceptual clarification of key terms related to the topic. Chapter three covers the analysis of the international legal responses on cybersecurity threats to information technology development.

Chapter four deals with the analysis of legislative and policy responses to the development of information technology and cybersecurity challenges in Nigeria. Chapter five, being the last chapter, captures the concise summary of the research work, findings and recommendation on the findings in the research.

[27] *ibid*

CHAPTER TWO
CONCEPTUAL CLARIFICATION OF KEY TERMS

2.1 Introduction

Criminal activities in the cyberspace like network outages, data compromised by hackers, computer viruses and other incidents threaten our existence in several ways. As the number of mobile users, digital applications and data networks increases, so do the opportunities for exploitation. This chapter of the research seeks to clarify both the technical and literal meaning of concepts associated with the cybersecurity and related matters, particularly as it affect the information technology regime.

2.2 Cyberspace

Cyberspace is the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship[1]Cyberspace is "the notional environment in which communication over computer networks occurs."[2] The word became popular in the 1990s when the uses of the Internet, networking, and digital communication were all growing dramatically and the term "cyberspace" was able to represent the many new ideas and phenomena that were emerging.[3]

The parent term of cyberspace is "cybernetics", derived from the Ancient Greek *κυβερνήτης* (*kybernētēs*, steersman, governor, pilot, or rudder), a word introduced by

[1]2010, Canada's Cyber Security Strategy p. 20, at: www.c-a-n-a-d-a-c-y-b-e-r-s-e-c-ur-i-t-y-s-t-r-a-t-e-g-y accessed 25/2/2016
[2]Lexico US Dictionary online version retrieved from: http://www.oxforddictionaries.com/us/definition/american_english/cyberspace accessed on 20/08/2016 10:15
[3]Strate, L. (1999). The varieties of cyberspace: Problems in definition and delimitation. *Western Journal of Communication.* 63 (3): 382–3.http://www.carriaghen.com/2011/02/what-exactly-is-cyberspace-and-cybersecirity-accessed on 22/08/2016 7:20 pm

Norbert Wiener for his pioneering work in electronic communication and control science. The term *cyberspace* has become a conventional means to describe anything associated with the Internet and the diverse Internet culture.

According to Morningstar and Farmer, cyberspace is defined more by the social interactions involved rather than its technical implementation.[4]In their views, the computational medium in cyberspace is an augmentation of the communication channel between real people; the core characteristic of cyberspace is that it offers an environment that consists of many participants with the ability to affect and influence each other. They derive this concept from the observation that people seek richness, complexity, and depth within a virtual world.

The term "cyberspace" first appeared in the visual arts in the late 1960s, when Danish artist Ussing (1940-1998) and her partner Hoff (b. 1934) constituted themselves as Atelier Cyberspace. Under this name the two made a series of installations and images entitled "sensory spaces" that were based on the principle of open systems adaptable to various influences, such as human movement and the behaviour of new materials.[5]

The term "cyberspace" first appeared in fiction in the 1980s in the work of cyberpunk science fiction author William Gibson, in his 1982 short story "Burning Chrome", and later in his 1984 novel *Neuromancer.*[6] In the next few years, the word became prominently

[4] Morningstar, C. and Farmer F. R. (2003) The Lessons of Lucas film's Habitat In: Wardrip-F. and Nick M. (Ed.) *The New Media Reader*. The MIT Press. PP. 664-667. Printhttp://www.carriaghen.com/2011/02/what-exactly-is-cyberspace-and-cybersecirity-accessed on 22/08/2016, 7:40pm

[5]Jacob Lillemose, Mathias Kryger (2015). *The (Re)invention of Cyberspace*. Nordic Art Review. http://www.kunstkritikk.com/kommentar/the-reinvention-of-cyberspace/accessed on 20/08/2016 10:30 am

[6] Scott T. (2009), (1948). William Gibson, Father of Cyberspace. Retrieved from www.willian-gibson-father-of-cyber-space on 23/03/2016, 10:00 am

identified with online computer networks. The portion of *Neuromancer* cited in this respect is usually the following:[7]

> Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding.

Cyberspace subsequently became a *de facto* synonym for the Internet, and later the World Wide Web, during the 1990s, especially in academic circles[8] and activist communities. Author Bruce Sterling, who popularized this meaning,[9]credits John Perry Barlow as the first to use it to refer to "the present-day nexus of computer and telecommunications networks." Barlow describes it thus in his essay to announce the formation of the Electronic Frontier Foundation in June, 1990:[10]

> In this silent world, all conversation is typed. To enter it, one forsakes both body and place and becomes a thing of words alone. You can see what your neighbors are saying (or recently said), but not what either they or their physical surroundings look like. Town meetings are continuous and discussions rage on everything from sexual kinks to depreciation schedules. Whether by one telephonic tendril or millions, they are all connected to one another. Collectively, they form what their inhabitants call the Net. It extends across that immense region of electron states, microwaves, magnetic fields, light pulses and thought which sci-fi writer William Gibson named Cyberspace.[11]

The concept cyberspace does not lend to itself a singular meaning; rather many definitions abound, both in scientific literature and other sources. There is no fully agreed official

---

[7] Gibson, W. (1984). *Neuromancer*. Ace Books, New York: p. 69. http://www.carriaghen.com/2011/02/what-exactly-is-cyberspace-and-cybersecirity-accessed on 22/08/2016 12:01pm

[8] Vanderbilt University,(1996) *Postmodernism and the Culture of Cyberspace* Fall 1996 course syllabus retrieved from http://www.carriaghen.com/2011/02/what-exactly-is-cyberspace-and-cybersecirity-accessed on 22/08/2016 10:20 pm

[9]Heylighen *(1994)* Cyberspace. *Principia Cybernetica*https://en. wikipedia.org/wiki/cyberspacehttp://www.carriaghen.com /2011/02/ what-exactly-is-cyberspace-and-cybersecirity-accessed on 22/08/2016 11:02am

[10] John, P. B. (1990) *Crime and Puzzlement*, http://www.carriaghen.com/2011/02/what-exactly-is-cyberspace-and-cybersecirity-accessed on 22/08/2018 10: 00 am

[11] *ibid*

definition yet. According to F. D. Kramer there are 28 different definitions of the term cyberspace.[12]. The most recent draft definition is the following:

> Cyberspace is a global and dynamic domain (subject to constant change) characterized by the combined use of electrons and electromagnetic spectrum, whose purpose is to create, store, modify, exchange, share and extract, use, eliminate information and disrupt physical resources. Cyberspace includes: a) physical infrastructures and telecommunications devices that allow for the connection of technological and communication system networks, understood in the broadest sense (SCADA devices, smartphones/tablets, computers, servers, etc.); b) computer systems (see point a) and the related (sometimes embedded) software that guarantee the domain's basic operational functioning and connectivity; c) networks between computer systems; d) networks of networks that connect computer systems (the distinction between networks and networks of networks is mainly organizational); e) the access nodes of users and intermediaries routing nodes; f) constituent data (or resident data). Often, in common parlance (and sometimes in commercial language), networks of networks are called Internet (with a lowercase i), while networks between computers are called intranet. Internet (with a capital I, in journalistic language sometimes called the Net) can be considered a part of the system a). A distinctive and constitutive feature of cyberspace is that no central entity exercises control over all the networks that make up this new domain.[13]

While cyberspace should not be confused with the Internet, the term is often used to refer to objects and identities that exist largely within the communication network, so that a website, for example, might be metaphorically said to "exist in cyberspace".[14] According to this interpretation, events taking place on the internet are not happening in the locations where participants or servers are physically located, but "in cyberspace".

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

[12]Kramer, F.D, Starr S. and Wentz L.K. (ed.) (2009),*Cyberpower and National Security*, National Defense University Press, Washington https://www.academia.edu/14336129/InternationalPoliticsintheDigital_Agehttp://www.carriaghen.com/2011/02/what-exactly-is-cyberspace-and-cybersecirity-accessed on 22/08/20168 11:25am

[13] Marco M., *etal* (2014). *How would you define Cyberspace*. Draft Pisa, https://www.academia.edu/7096442/ How would _you_ define_ Cyber space accessed on 20/08/2018 12:05 pm

[14]Graham M. (2011) Geography/Internet: Ethereal Alternate Dimensions of Cyberspace or Grounded Augmented Realities. *The Geographical Journal*, 179(2): pp. 177-188.http://www.carriaghen.com/2011/02/what-exactly-is-cyberspace-and-cybersecirity-accessed on 22/08/2016 11:15pm

online identity were enacted, raising important questions about the social psychology of internet use, the relationship between "online" and "offline" forms of life and interaction, and the relationship between the "real" and the virtual. Cyberspace draws attention to remediation of culture through new media technologies: it is not just a communication tool but a social destination, and is culturally significant in its own right. Finally, cyberspace can be seen as providing new opportunities to reshape society and culture through "hidden" identities, or it can be seen as borderless communication and culture.[15]

Cyberspace is the "place" where a telephone conversation appears to occur. Not inside your actual phone, the plastic device on your desk. Not inside the other person's phone, in some other city. The place between the phones. [...] in the past twenty years, this electrical "space," which was once thin and dark and one-dimensional—little more than a narrow speaking-tube, stretching from phone to phone—has flung itself open like a gigantic jack-in-the-box. Light has flooded upon it, the eerie light of the glowing computer screen. This dark electric netherworld has become a vast flowering electronic landscape. Since the 1960s, the world of the telephone has cross-bred itself with computers and television, and though there is still no substance to cyberspace, nothing you can handle, it has a strange kind of physicality now. It makes good sense today to talk of cyberspace as a domain on its own.[16]

2.3 The Concept of Cybersecurity

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a

[15]Flew, T.(2011) *New Media: an Introduction* http://www.carriaghen.com/2011/02/what-exactly-is-cyberspace-and-cybersecirity-accessed on 22/08/2018 10:20 am

[16] Bruce S., (2013) *Introduction to The Hacker Crackdown retrieved from www.cnn.com/2013/08/26/opinion/olson-mobile-hackers/index.html* accessed on 23/08/2016 7:10pm

computing context, the term security implies cybersecurity.[17]Cybersecurity, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.[18]

Cybersecurity involves protecting information and systems from major cyber threats, such as cyber terrorism, cyber warfare, and cyber espionage. [19]Cybersecurity is also the state of being protected against the criminal or unauthorised use of electronic data, or the measures taken to achieve this.[20]

Cybersecurity is not only a framework or a set of on-time actions, but it is also a set of on-going efforts focused on performing periodic assessments and monitoring of aforementioned policies, as well as enforcing compliance with existing regulations and laws and applying sanctions in the case of violations. Cyber laws prevent or reduce large scale damage from cybercriminal activities by protecting information access, privacy, communications, intellectual property and freedom of speech related to the use of the internet, websites, emails, computers, cell phones, software and hardware, such as data storage devices[21]

In practice, outward expressions of cybersecurity include domestic public policy and laws (creation of cybersecurity agencies, such as the United States' Cyber Command), international public policy discussions (talks around creating an ITU/UN cybersecurity treaty), private business practices (anti-virus software, notification programs by Internet Service Providers and firewalls), online surveillance (often by governments), and technical community practices aimed at maintaining the critical infrastructure of the Internet

[17]*ibid*
[18]Management Association, Information Resources (2018) *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications*http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm accessed on 20/08/2016 10: 20 am
[19]*ibid*
[20]Oxford Dictionaries (2013) Online available at http://oxforddictionaries.com
[21]Ladan M.T (2015), *Cyber law and Policy on Information and communications Technology in Nigeria and ECOWAS*, ABU Press p. 104

(Internet Engineering Task Force is one of these independent technical agencies). The understanding of these are essentials to the understanding of the basics of cybersecurity: Cybersecurity; Internet security; Information security; Critical infrastructure; Cyberspace; Cybercrime; Cyber warfare; and Cyber threat.[22]

2.4 Mobile Security or Mobile Device Security

Mobile security involves protecting both personal and business information stored on and transmitted from smartphones, tablets, laptops and other mobile devices. The term mobile security is a broad one that covers everything from protecting mobile devices from malware threats to reducing risks and securing mobile devices and their data in the case of theft, unauthorized access or accidental loss of the mobile device.[23]

Mobile security also refers to the means by which a mobile device can authenticate users and protect or restrict access to data stored on the device through the use of passwords, Personal Identification Numbers (PINs), pattern screen locks or more advanced forms of authentication such as fingerprint readers, eye scanners and other forms of biometric readers.[24]

Mobile device security means the security measures designed to protect the sensitive information stored on and transmitted by smartphones, tablets, laptops and other mobile devices. Mobile device security spans the gamut from user authentication measures and mobile security best practices for protecting against compromised data in the event of

[22]Natalie G. and Carolina R.***opcit p.10***
[23]Forrest S. (2019), *Mobile Computing*. Webopedia retrieved from https://www.webopedia.com /TERM/M/mobile_security.html
[24]*Ibid.*

unauthorized access or accidental loss of the mobile device to combat malware, spyware and other mobile security threats that can expose a mobile device's data to hackers.[25]

Most mobile devices feature mobile operating systems with built-in mobile device security features, including iphone operating system (iOS) for iPhones and iPads, Google's Android platform and Microsoft's Windows Phone. Additionally, a variety of third-party mobile device security solutions are available for providing an additional layer of protection for mobile devices.

Mobile security refers to the different security counter-measures being developed and applied to smart phones; from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable apps. Mobile security or mobile phone security has become increasingly important in mobile computing; of particular concern is the security of personal and business information now stored on smartphones.

Smartphones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company. All smartphones, as computers, are preferred targets of attacks. These attacks exploit weaknesses related to smartphones that can come from means of communication like Short Message Service (SMS, aka text messaging), Multimedia Messaging Service (MMS), Wi-Fi networks, Bluetooth and GSM, the de facto global standard for mobile communications. There are also attacks that exploit software vulnerabilities from both the web browser and operating system. Finally, there are forms of malicious software that rely on the weak knowledge of average users.

[25] *ibid*

Different security counter-measures are being developed and applied to smartphones, from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable apps.

2.4.1 Threats to Mobile Security

A smartphone user is exposed to various threats when they use their phone. In just the last two quarters of 2012, the number of unique mobile threats grew by 261%, according to ABI Research.[26] These threats can disrupt the operation of the smartphone, and transmit or modify user data. For these reasons, the applications deployed there must guarantee privacy and integrity of the information they handle. In addition, since some apps could themselves be malware, their functionality and activities should be limited (for example, restricting the apps from accessing location information via GPS, blocking access to the user's address book, preventing the transmission of data on the network, sending SMS messages that are billed to the user). There are three prime targets for attackers: data, identity and availability.[27]

The sources of these attacks are the same actors found in the non-mobile computing space: professionals, whether commercial or military, who focus on the three targets mentioned above. They steal sensitive data from the general public, as well as undertake industrial espionage. They will also use the identity of those attacked to achieve other attacks; thieves who want to gain income through data or identities they have stolen. The thieves will attack many people to increase their potential income; Black hat hackers who specifically attack

[26] Olson P. (2013) *Your Smartphone is Hackers' next big target* www.cnn.com/2013/08/26/opinion/olson-mobile-hackers/index.html accessed on 21/08/2016 10:45am
[27] Ibid.

availability.[28] Their goal is to develop viruses, and cause damage to the device.[29] In some cases, hackers have an interest in stealing data on devices. Grey hat hackers who reveal vulnerabilities.[30] Their goal is to expose vulnerabilities of the device.[31] Grey hat hackers do not intend on damaging the device or stealing data.[32]

2.4.2 Consequences

When a smartphone is infected by an attacker, the attacker can attempt several things: the attacker can manipulate the smartphone as a zombie machine, that is to say, a machine with which the attacker can communicate and send commands which will be used to send unsolicited messages (spam) through short messages (sms) or email;[33]

The attacker can easily force the smartphone to make phone calls. For example, one can use the Application Programming Interface (API)[34], which collects telephone numbers from any source such as yellow pages, and then call them. The attacker can also use this method to call paid services, resulting in a charge to the owner of the smartphone. It is also very dangerous because the smartphone could call emergency services and thus disrupt those services;[35]

A compromised smartphone can record conversations between the user and others and send them to a third party. This can cause user privacy and industrial security problems; an

[28]Ibid.
[29] Ibid.
[30]Creutzburg, R. (2016) *Wikipedia Handbook of Computer Security and Digital Forensics*: *Computer Security* retrieved from http://www.gov.mu/portal/sites/cert/files/Guide%20on%20Protection%20Against%20Hacking.pdf. accessed on 21/08/2016 1:20pm
[31]Lemos, R. (2002) *New laws make hacking a black-and-white choice*. CNET News.com. Retrieved September 23, 2018. 12:40 pm
[32]McCaney, K. (2013) *Unknowns hack NASA, Air Force, saying 'We're here to help*. Retrieved from. https:/ www.cnn.com/2013 /08/26/opinion/olson-mobile-hackers/index.html accessed on 21/08/2016. 1o:40am
[33]Khosrow-Pour, D.B.A., Mehdi (2018) https://en. www.cnn.com/2013/08/26/opinion/olson-mobile-hackers/index.html August 26, 2018. 2:30pm
[34] A documented set of commands that software developers can use to access specific functionality of the underlying operating system (OS) or hardware device.
[35] Olson, P. (2013) op. cit. 23

attacker can also steal a user's identity, usurp their identity (with a copy of the user's sim card or even the telephone itself), and thus impersonate the owner. This raises security concerns in countries where smartphones can be used to place orders, view bank accounts or are used as an identity card;[36]

The attacker can reduce the utility of the smartphone, by discharging the battery.[37] For example, they can launch an application that will run continuously on the smartphone processor, requiring a lot of energy and draining the battery. The attacker can prevent the operation and/or starting of the smartphone by making it unusable. This attack can either delete the boot scripts, resulting in a phone without a functioning operating system (OS), or modify certain files to make it unusable. The attacker can remove the personal (photos, music or videos) or professional data (contacts, calendars, notes) of the user.[38]

2.5 Information Security

Information security, sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).[39]

The definitions of InfoSec suggested in different sources are summarized below.[40]

"Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can

[36] *ibid*
[37] *ibid*
[38] *ibid*
[39] 44 U.S.C. § 3542(b)(1)
[40] Cherdantseva Y. and Hilton J. (2013). Information Security and Information Assurance: The Discussion about the Meaning, Scope and Goals. In:Almeida F. and Portela, I. (eds.) *Organizational, Legal, and Technological Dimensions of Information System Administrator*. IGI Global Publishing. Retrieved from www.cnn.com/2013/08/26/opinion/olson-mobile-hackers/index.html accessed on 20/08/20168 12:20am

also be involved."[41]"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."[42]"Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)."[43] "Information Security is the process of protecting the intellectual property of an organisation."[44] "...information security is a risk management discipline, whose job is to manage the cost of information risk to the business."[45]"A well-informed sense of assurance that information risks and controls are in balance."[46]

"Information security is the protection of information and minimises the risk of exposing information to unauthorised parties."[47]"Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organisational, human-oriented and legal) in order to keep information in all its locations (within and outside the organisation's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats.

Another concept associated with computer security is, information technology security, which is information security applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home

[41]ISO/IEC 27000:2018(en) Information technology - Security techniques - Information security management systems - *Overview and vocabulary*. Retrieved fromwww.cnn.com/2013/08/26/opinion/olson-mobile-hackers/index.html accessed on 20/08/2016
[42]*ibid*
[43]ISACA.(2008).Glossary of terms, 2008. Retrieved from http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf on 12/3/16 10:20am
[44]Pipkin, D. (2000) *Information security: Protecting the global enterprise*. New York: Hewlett-Packard Company.
[45] Jump up B., McDermott, E., & Geer, D. (2001). Information security is information risk management. In: *Proceedings of the 2001 Workshop on New Security Paradigms* pp. 97 – 104 www.cnn.com/2013/08/26/opinion/olson-mobile-hackers/index.html August 26, 2018 2:30pm
[46]Anderson, J. M. (2003). Why we need a new definition of information security. *Computers& Security*, 22(4), 308–313. www.cnn.com/2013/08/26/opinion/olson-mobile-hackers/index.html August 26, 2016. 2:30pm
[47]Venter, H. S., &Eloff, J. H. P. (2003). A taxonomy for information security technologies. *Computers & Security*, 22(4): 299–307. www.cnn.com/2013/08/26/opinion/olson-mobile-hackers/index.html August 26, 2016. 2:30pm

desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within.[48]

The major aim of information security is information assurance; the act of providing trust of the information, that the Confidentiality, Integrity and Availability (CIA) of the information are not violated. e.g., ensuring that data is not lost when critical issues arise. These issues include, but are not limited to: natural disasters, computer/server malfunction or physical theft. Since most information is stored on computers in our modern era, information assurance is typically dealt with by IT security specialists. A common method of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arise[49]

2.5.1 Threats to Information Security

Threats to computer systems come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Most people have experienced software attacks of some sort. Viruses, worms, phishing attacks, and Trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the IT field.

[48] *ibid*
[49] *ibid*

Intellectual property is the ownership of property usually consisting of some form of protection. Identity theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information. Theft of equipment or information is becoming more prevalent today due to the fact that most devices today are mobile. Cell phones are prone to theft and have also become far more desirable as the amount of data capacity increases. Sabotage usually consists of the destruction of an organization′s website in an attempt to cause loss of confidence to its customers. Information extortion consists of theft of a company′s property or information as an attempt to receive a payment in exchange for returning the information or property back to its owner.

Governments,military,corporations,financialinstitutions,hospitals and private businesses collect a great deal of confidential information about their employees, customers, products, research and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers. Should such confidential information about a business' customers or finances or new product line fall into the hands of a competitor or a black hat hacker, a business and its customers could suffer widespread, irreparable financial loss, as well as damage to the company's reputation. Protecting confidential information is a business requirement and in many cases also an ethical and legal requirement. Hence a key concern for organizations today is to derive the optimal information security investment.[50]For the individual, information security has a significant effect on privacy, which is viewed very differently in different cultures.

[50]Gordon, L., Loeb, M. (2002). *The Economics of Information Security Investment: ACM Transactions on Information and System Security*. 5 (4): 438–457 retrieved from www.cnn.com/2013/08/26/opinion/olson-mobile-hackers/index.html on 20/08/2018 10:45am

Threats to information and information systems may be categorized, and a corresponding security goal may be defined for each category of threats. A set of security goals, identified as a result of a threat analysis, should be revised periodically to ensure its adequacy and conformity with the evolving environment. The currently relevant set of security goals may include: confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability and audit ability."[51]

2.6 Internet Security

Internet security is a branch of computer security specifically related to the internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole. Its objective is to establish rules and measures to use against attacks over the internet.[52] The internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing.[53] Different methods have been used to protect the transfer of data, including encryption and from-the-ground-up engineering.[54]

2.6.1 Threats to Internet security

a. **Malware,** short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to

[51]Cherdantseva, Y. and Hilton, J. (2013). Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals. In:Almeida F., Portela, I. (eds.) *Organizational, Legal, and Technological Dimensions of Information System Administrator*. IGI Global Publishing. (2013)
[52]ibid
[53] Gordon, L. Loeb, M. (2002). *The Economics of Information Security Investment. ACM Transactions on Information and System Security*. 5 (4)
[54] *ibid*

some deficiency. The term bad ware is sometimes used, and applied to both true (malicious) malware and unintentionally harmful software.

b. **A botnet** is a network of zombie computers that have been taken over by a robot or bot that performs large-scale malicious acts for the creator of the bot net.

c. **Computer Viruses** are programs that can replicate their structures or effects by infecting other files or structures on a computer. The common use of a virus is to take over a computer to steal data.

d. **Computer worms** are programs that can replicate themselves throughout a computer network, performing malicious tasks throughout.

e. **Ransom ware** is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed.

f. **Scareware** is scam software with malicious payloads, usually of limited or no benefit that are sold to consumers through certain unethical marketing practices. The selling approach uses social engineering to cause shock, anxiety, or the perception of a threat, generally directed at an unsuspecting user.

g. **Spyware** refers to programs that surreptitiously monitor activity on a computer system and report that information to others without the user's consent.

h. **A Trojan horse**, commonly known as a *Trojan*, is a general term for malicious software that pretends to be harmless, so that a user willingly allows it to be downloaded onto the computer.

i. **Denial-of-service attacks**, (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts to prevent

an internet site or service from functioning efficiently or at all, temporarily or indefinitely.[55]

j. **Phishing**, Phishing occurs when the attacker pretends to be a trustworthy entity, either via email or web page. Victims are directed to fake web pages, which are dressed to look legitimate, via spoof emails, instant messenger/social media or other avenues. Often tactics such as email spoofing are used to make emails appear to be from legitimate senders, or long complex sub-domains hide the real website host.[56]

2.7 Critical Infrastructure Security

Critical infrastructure protection (CIP) is a concept that relates to the preparedness and response to serious incidents that involve the critical infrastructure of a region or nation.[57] Take for example, a computer virus that disrupts the distribution of natural gas across a region. This could lead to a consequential reduction in electrical power generation, which in turn leads to the forced shutdown of computerized controls and communications. Road traffic, air traffic, and rail transportation might then become affected. Emergency services might also be hampered.

An entire region can become debilitated because some critical elements in the infrastructure become disabled through natural disaster. While potentially in contravention of the Geneva Conventions,[58]military forces have also recognized that it can cripple an enemy's ability to resist by attacking key elements of its civilian and military infrastructure.

[55]ISO/IEC 15408-1:2009. (2009) *Information technology - Security techniques: Evaluation criteria for IT security: introduction and general model*. ISO/IEC.
[56] ibid
[57] Ibid
[58] Article 52 and 54 of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts ("Geneva Conventions")

2.8 Information Technology

Information technology (IT) is a term which encompasses all forms of technology used to create, store, exchange, and use information in its various forms (business data, voice conversations, still images, motion pictures, multimedia presentations, and other forms, including those not yet conceived). It is a convenient term for including both telephony and computer technology in the same word. It is the technology which is driving what has often been called "the information revolution"[59]Information and Communication Technology (ICT) refers to a broad spectrum of technologies that allows users to get, produce, and share ideas and resources. It is any technology, which enables communication and the electronic capture, processing and transmission of information[60].

Information technology (IT) is the acquisition, processing, storage and dissemination of vocal, pictorial, textual and numerical information by a micro-electronic-based combination of computing and telecommunication. The term in its modern sense first appeared in 1958 article published in the Harvard Business Review, in which authors Leavit and whistler commented that "the new Technology does not yet have a single established name. We call it information technology"[61]It spans a wide variety of areas that include but are not limited to things such as process, computer software, computer hardware, programming languages and data construct. In short, anything that renders data, information or perceived knowledge in any visual format whatsoever, via any multimedia distribution mechanism, is considered part of the domain space known as information technology.

[59]Pipkin, D. (2000). *Information Security: Protecting the global enterprise*. New York: Hewlett-Packard Company
[60]Adomi, E. (2006). *Application of Information and Communication Technologies (ICTs) in Nigerian High Schools.* Warri: Nigerian Library Association, Delta State Chapter. AGM. Retrieved 02/2/2016 10:20am
[61]Dipti B. (2020)*The Concept of Information, Communication and Educational Technology and Communication Technology*. M.A Education (part II) Group B-Paper-VII. Institute of Distance and Open learning, University of Mumbai.

Information-Technology consists of two words, Information and Technology. The term "information" refers to "any communication or representation of knowledge such as facts, data or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audio visual forms"[62]"Technology is the practical form of scientific knowledge or the science of application of knowledge to practical"[63]

Information Technology is any equipment or interconnected system or sub system of equipment that is used in the acquisition, storage, manipulation, management, transmission or reception of data or information.[64]Information Technology is a scientific, technological and engineering discipline and management technique used in handling the information, its application, and association with social, economic and cultural matters.[65]

From the foregoing we can conclude that information technology refers to the information processing of the software applications that includes computers, videos, telephones and related equipment of telecommunications.[66]The characteristics of Information Technology include:-acquisition, storage, manipulation, management, transmission, or reception of data or information; real time access to information; easy availability of updated data; connecting geographically dispersed regions; wider range of communication media.[67]

In this chapter, the researcher attempted to explore key concepts necessary for proper understanding of this research work. The chapter clarified the concepts of cyberspace, cybersecurity, mobile security, internet security, information security and information technology.

[62]See ***Oxford Advance Learner's Dictionary***, (7th Ed.), (2006) Oxford University Press, UK, at p.765
[63]Ibid, at p.1520.
[64]Ibid, at p.765
[65]Ibid.
[66]Ladan M.T. (2015), *op cit* p. 8
[67]Ibid

CHAPTER THREE

AN ANALYSIS OF INTERNATIONAL LEGAL RESPONSES TO CYBERSECURITY AND INFORMATION TECHNOLOGYTHREATS

3.1 Introduction

The last decade had witnessed significant developments in the promulgation of international and regional instruments aimed at securing the global cyberspace. These include binding and nonbinding instruments. The genesis, legal status, geographic scope, substantive focus, and mechanisms of such instruments vary significantly. The following possible 'clusters' of instruments may be identified – (i) instruments developed in the context of, or inspired by, the United Nations, Council of Europe or the European Union; (ii) instruments developed in the context of the Commonwealth of Independent States or other regional arrangements.

The current picture of cybersecurity legislation is a dynamic one – indicating ongoing legal reforms and increasing recognition that cybersecurity requires a legal response across multiple areas: criminal, civil and administrative.[1]

This chapter therefore seeks to appraise the various efforts across the globe meant to address cybersecurity challenges. These efforts are discussed below:

3.2 International/Global Responses to Cyber Threats

In recent times, the convergence of some distinct but interconnected trends in international relations necessitated the need for urgent formal intervention by governments and international organisations. First, Internet usage continued to rise, coupled with an expansion in forms of use. Second, many governments recognized that cyber vulnerabilities continued to threaten not only the security of their own networks, but also those of their

[1]Gertjan B. (2013) Study cybercrime questionnaire. Q14:*United Nations Comprehensive Study on the Problem of Cybercrime mandated by General Assembly resolution 65/230 (2010)*.

citizens involved in routine activities on a daily basis. Third, a noted absence of coordinated industry response or efforts to develop cooperative threat reduction strategies reinforced an unambiguous gap-in-governance. Finally, a growing set of cyber incidents, large and small, signalled to governments the potential impact of their failure to address the emerging threats. In response to these trends, governments, in various ways, mobilized significant national and international resources toward the creation of a broad cybersecurity framework some of which are highlighted below:

3.2.1 The G8 (Group of Eight)

The Group of Eight Industrialised States, otherwise known as the 'G8', comprises Canada, France, Italy, Germany, Japan, Russia, the UK, and the US. Statistically, the G8 is reputed to jointly hold 48 per cent of the entire wealth of the world,[2]a fact that identifies the G8 as an iconic organisation that could lead the formulation of global collaborative legal agenda against cybercrimes. The G8 has commendably been active in initiating a transnational arrangement for computer experts, establishing forensic and ethical principles for computer usage in situations where digital evidence obtained from one state requires authentication in the courts of another State, and making proposals for tracking cross-border criminal communications[3]

However, apart from technical initiatives, the G8 has not been able to come up with any legal framework specifically addressing cybercrimes, even among its members. The G8's initiatives appears promising, but, the organisation's capacity is greatly limited by its inability to enlist the participation of the weaker and poorer States which are often safe

[2] G8 Information Centre, 'What is the G8?' http://www.g7.utoronto.ca/what_is_g8.html accessed 09/08/2019 at 4:38pm
[3]Nykodym N., Taylor R. (2004), World's Current Legislation Efforts Against Cybercrime: *Computer and Security Review* v. 20 p. 91

havens for all sorts of cybercrimes.[4]The G8 countries were reduced to G7 countries in 2014, when Russia was excluded following its annexation of Crimea.

At G7 level there have been important developments especially for what concerns informal cooperation among the G7 network. In particular, during the Japan presidency of the group, G7 leaders launched, in 2016, the Ise-Shima Cyber Group (ISCG), entirely dedicated to cyber issues.[5]During the Italian presidency, the meeting of G7 foreign ministers approved the Declaration on Responsible State Behaviour in Cyberspace, otherwise known as the Lucca Declaration. The declaration is particularly important as it recognized the centrality of states' authority in the cyberspace, and urged all countries to develop laws, policies and practices that effectively combat cybercrime, including, if possible, becoming party to the 2001 Budapest Convention on Cybercrime. Moreover, the G7 created several task forces that work on several issues. One of these, the Roma-Lyon Group's High-Tech Crime Subgroup operates the G7 24/7 Cybercrime Network, which focuses mainly on preserving digital evidence for subsequent transfer through legal channels. This network is open to non G7 countries.

3.2.2 United Nations and United Nations Office on Drugs and Crimes[6]

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

[4]Dejo O. (2009) Cyber-Crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa, *Journal of Information Law & Technology v.1* retrieved at https:// warwick.ac.uk/ fac/ soc/ law/ elj/ jilt/ 2009_1/olowu/on 09/08/2019 at 4:38pm

[5]Luigi M. (2018), Cyber Diplomacy e relazioniinternazionali: le iniziativediplomatiche per mitigareilrischio di escalation militarenelcyberspazio, In Valerio De Luca, Giulio Terzi di Sant'Agata e *Francesca Voce (eds)..IlRuolodell'ItalianellaSicurezzaCibernetica*. Milano: Franco Angeli

[6] The United Nations (UN) is an international organization founded in 1945. It had 192 Member States in 2010

The United Nations Office on Drugs and Crimes (UNODC) Global Programme on Cybercrime provides focused technical assistance for capacity building, prevention and awareness raising, international cooperation and analysis on the phenomenon, principally in developing countries. The Programme is based within the UNODC Organized Crime Branch, part of the Division for Treaty Affairs.[7]

The UNODC developed the Cybercrime Repository, a part of the Global Programme on Cybercrime, as a central data repository of cybercrime laws and lessons learned for the purposes of facilitating the continued assessment of needs and criminal justice capabilities and the delivery and coordination of technical assistance.[8]

3.2.3 UN Convention on the Rights of the Child

The United Nations Convention on the Rights of the Child, adopted in 1989,[9] contains several instruments aiming to protect children. It does not define child pornography, nor does it contain provisions that harmonize the criminalization of the distribution of online child pornography. However, Article 34 calls upon Member States to prevent the exploitative use of children in pornographic performances.

3.2.4 UN General Assembly Resolution 45/121

After the eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (held in Havana, Cuba, 27 August – 7 September 1990), the UN General Assembly adopted a resolution dealing with computer-crime legislation.[10] Based on its

[7]Summer Walker (2019), *the Global Initiative Against Transnational Organized Crime: Cyber-Insecurities, a Guide to the UN Cybercrime Debate*https://www.unodc.org/unodc/en/cybercrime/index.html accessed 02/08/2019.
[8]*ibid*
[9] A/RES/44/25, adopted by the UN General Assembly on 12 December 1989.
[10] Saint (2017) *Comparative Analysis of Incentivized Cooperative and Regulatory Processes in Cybersecurity*. Retrieved from www.un.org/documents/ga/res/45/a45r121.htm. 10/6/2018 10:30 am

Resolution 45/121 (1990), the UN published a manual in 1994 on the prevention and control of computer-related crime.[11]

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

The Optional Protocol not only addresses the issue of child pornography in general, but explicitly refers to the role of the Internet in distributing such material. [12]Child pornography is defined as any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.[13] Article 3 requires the parties to criminalize certain conduct, including acts related to child pornography.

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

During the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held in Vienna in 2000, the impact of computer related crimes was discussed in a specific workshop. The debate focused especially on the categories of crime and transnational investigation, as well as legal response to the phenomenon.[14] The conclusions of the workshop contain major elements of the debate that is still ongoing: criminalization is required; legislation needs to include procedural instruments, international cooperation is crucial, and public-private partnership should be strengthened.[15] In addition, the importance of capacity building was highlighted – an issue that was picked up again in subsequent

[11] UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication, Sales No. E.94.IV.5), see www.uncjin.org/Documents/EighthCongress.html accessed 20/7/2018 10:20am
[12] The Preface to the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography
[13] Art. 2.Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography
[14] Report of the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.185/15, No. 165. Retrieved from www.uncjin.org/Documents/congr10/15e.pdf. on 12/3/16 10:20am
[15] Report of the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.185/15, No. 174, Retrieved on 12/3/16 10:20am fromwww.uncjin.org/Documents/congr10/15e.pdf.

years. The Vienna Declaration called upon the Commission on Crime Prevention and Criminal Justice to undertake work in this regard:

3.3.7 UN General Assembly Resolution 55/63

In the year 2000, the UN General Assembly adopted a resolution on combating the criminal misuse of information technologies which displays a number of similarities with the G8's Ten-Point Action Plan from 1997.[16] In its resolution, the General Assembly identified a number of measures to prevent the misuse of information technology, including:

> States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies; Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States; Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies;

Resolution 55/63 invites States to take the necessary steps to combat cybercrime on the regional and international stage. This includes the development of domestic legislation to eliminate safe havens for criminal misuse of technologies, improving law-enforcement capacities to cooperate across borders in the investigation and prosecution of international cases of criminal misuse of information technologies, improving information exchange, enhancing the security of data and computer systems, training law enforcement to deal specifically with the challenges associated with cybercrime, building mutual assistance regimes and raising public awareness of the threat of cybercrime.

3.2.8 UN General Assembly Resolution 56/121

In 2002, the UN General Assembly adopted another resolution on combating the criminal

[16] A/RES/55/63. Retrieved on 12/3/16 10:20am www.unodc.org/pdf/crime/a_res_55/res5563e.pdf.

misuse of information technology.[17] The resolution refers to the existing international approaches in fighting cybercrime and highlights various solutions, noting the work of international and regional organizations in combating high-technology crime, including the work of the Council of Europe in elaborating the Convention on Cybercrime as well as the work of those organizations in promoting dialogue between government and the private sector on safety and confidence in cyberspace.

Resolution 56/121 underlines the need for cooperation among states in combating the criminal misuse of information technologies. It highlights the role that can be played by the United Nations and other international and regional organizations. The resolution further invites states to take into account the direction provided by the Commission on Crime Prevention and Criminal Justice when developing national legislation.

3.2.9 UN General Assembly Resolutions 57/239 and 58/199

Resolutions 57/239 and 58/199 are the two main UN General Assembly resolutions dealing with cybersecurity. Without going into detail with regard to cybercrime, they recall Resolutions 55/06 and 56/121. Both resolutions furthermore emphasize the need for international cooperation in fighting Cybercrime by recognizing that gaps in states' access to and use of information technologies can diminish the effectiveness of international cooperation in combating the criminal misuse of information technology.[18]

3.2.10 Eleventh UN Congress on Crime Prevention and Criminal Justice

Cybercrime was discussed during the eleventh UN Congress on Crime Prevention and Criminal Justice (the "UN Crime Congress") in Bangkok, Thailand, in 2005. Several challenges associated with the emerging use of computer systems in committing offences

[17] A/RES/56/121. See http://daccessdds.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf. accessed on 12/3/16 10:20am

[18] A/RES/57/239, on Creation of a Global Culture of Cybersecurity; A/RES/58/199, on Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructure. Retrieved from www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf accessed 23/06/2016 10:40am

and the transnational dimension were addressed both in the background paper and in workshops. Within the framework of the preparatory meetings in advance of the congress, some member countries such as Egypt called for a new UN convention against cybercrime, and the Western Asian regional preparatory meeting called for the negotiation of such convention.

The possibility of negotiating a convention was included in the discussion guide for the eleventh UN Crime Congress. However, the Member States could not at this time decide to initiate a harmonization of legislation.

3.2.11 UN General Assembly Resolution 60/177

After the eleventh UN Congress on Crime Prevention and Criminal Justice in Bangkok, Thailand, in 2005, a declaration was adopted that highlighted the need for harmonization in the fight against cybercrime,[19] addressing, among others, the following issues: UN General Assembly Resolution 60/177 endorsed the 2005 Bangkok Declaration, wherein the international community's efforts to enhance and supplement existing cooperation to prevent computer related crime were encouraged, inviting further exploration of the feasibility of providing assistance to Member States in addressing computer-related crime under the aegis of the United Nations, and in partnership with other similarly focused organizations.

3.2.12 Twelfth UN Congress on Crime Prevention and Criminal Justice

The topic of cybercrime was also discussed at the twelfth UN Congress on Crime Prevention and Criminal Justice held in Brazil in 2010. Within the four regional

[19]25 April 2005 Bangkok Declaration Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice retrieved from www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf 23/06/2016 10:40am

preparatory meetings for the congress, for Latin America and Caribbean,[20] Western Asia,[21] Asia and the Pacific[22]and Africa, the countries called for the development of an international convention on cybercrime. Similar calls were made within academia. At the congress itself, Member States took a major step toward more active involvement of the United Nations in the debate on the issue of computer crime and cybercrime.

The fact that the delegations discussed the topics for two days and that additional side events were organized, highlights the importance of the topic, which was more intensively discussed than during the previous crime congresses. The deliberations focused on two main issues: how can harmonization of legal standards be achieved, and how can developing countries be supported in fighting cybercrime? The first point is especially relevant if the UN develops comprehensive legal standards or suggests that Member States implement the Council of Europe Convention on Cybercrime. In preparation of the UN Crime Congress, the Council of Europe had expressed concerns regarding a UN approach and had called for support for its Convention on Cybercrime. After an intensive debate, where the limited reach of the Convention on Cybercrime was discussed in particular, the Member States decided not to suggest the ratification of the Convention on Cybercrime but to strengthen the UN's role in two important areas, which are reflected in the Salvador Declaration:

> 41. We recommend that the United Nations Office on Drugs and Crime, upon request, provide, in cooperation with Member States, relevant international organizations and the private sector, technical assistance and training to States to

[20]Report of the Latin American and Caribbean Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10). www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf accessed 23/o6/2016 10:40am

[21]Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10). www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf accessed 23/o6/2016 10:40am

[22] Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10). www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf accessed 23/o6/2016 10:40am

> improve national legislation and build the capacity of national authorities, in order to deal with cybercrime, including the prevention, detection, investigation and prosecution of such crime in all its forms, and to enhance the security of computer networks.
> 42. We invite the Commission on Crime Prevention and Criminal Justice to consider convening an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.

The Member States thus recommended a strong mandate for the United Nations Office on Drugs and Crimes (UNODC) to provide global capacity building upon request.

3.2.13 UN General Assembly Resolution 64/211

In March 2010, the UN General Assembly passed a new resolution as part of the "Creation of a global culture of cybersecurity" initiative. Resolution 64/211 refers to the two major resolutions on cybercrime[23] as well as the two main resolutions on cybersecurity.[24] The voluntary self-assessment tool for national efforts to protect critical information infrastructures provided as an annex to the resolution calls for countries to review and update legal authorities (including those related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption) that may be outdated or obsolete as a result of the rapid uptake of, and dependence upon, new information and communication technologies. The resolution further calls on states to use regional international conventions, arrangements and precedents in these reviews.

> 13. Review and update legal authorities (including those related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption) that may be outdated or obsolete as a result of the rapid uptake of and dependence upon new information and communications technologies, and use regional and

[23] Resolutions 55/63 and 56/121.
[24] Resolutions 57/239 and 58/199.

international conventions, arrangements and precedents in these reviews. Ascertain whether your country has developed necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, General Assembly resolutions 55/63 and 56/121 on combating the criminal misuse of information technologies, and regional initiatives, including the Council of Europe Convention on Cybercrime.

14. Determine the current status of national cybercrime authorities and procedures, including legal authorities and national cybercrime units, and the level of understanding among prosecutors, judges and legislators of cybercrime issues.

15. Assess the adequacy of current legal codes and authorities in addressing the current and future challenges of cybercrime, and of cyberspace more generally.

16. Examine national participation in international efforts to combat cybercrime, such as the round-the clock Cybercrime Point of Contact Network.

17. Determine the requirements for national law enforcement agencies to cooperate with international counterparts to investigate translational cybercrime in those instances in which infrastructure is situated or perpetrators reside in national territory, but victims reside elsewhere.

The fact that four out of 18 subjects of the self-assessment tool are related to cybercrime highlights the importance of the ability of law enforcement to combat cybercrime effectively for maintaining cybersecurity.

3.2.14 Intergovernmental Expert Group on Cybercrime

Following the decision of the Member States to call upon UNODC to set up an intergovernmental working group, the first meeting of the group was held in Vienna in January 2011.[25] The expert group included representatives of Member States, intergovernmental and international organizations, specialized agencies, private sector and academia. During the meeting the members of the expert group discussed a draft structure for a comprehensive study analysing the issue of cybercrime, as well as the response.[26] With regard to the legal response, a number of members underline the usefulness of existing international legal instruments, including the United Nations Convention against

[25] The Report on the Meeting of the Open-ended Working Group (UNODC/CCPCJ/EG.4/2011/3) retrieved at www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_3/UNODC_C CPCJ_EG4_2011_3_E.pdf. 25/08/2016 10:30 am

[26] Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, 27 August-7 September 1990: Report prepared by the Secretariat (United Nations publication) Sales No. E.91.IV.2), chap. I, sect. B.1, annex. www.unodc .org/documents/treaties/organizedcrime/EGM cybercrime 2011/UNODC CCPCJ_EG4_2011_2/UNODC_CCPCJ_EG4_2011_2_E.pdf. accessed 29/07/2016 2:30pm

Transnational Organized Crime (UNTOC) and the Council of Europe Convention on Cybercrime, and the desirability of elaborating a global legal instrument to address specifically the problem of cybercrime. It was agreed that the decision on whether a global instrument should be developed will be made after the study was conducted.

3.2.15 Other Resolutions and Activities

In addition, a number of United Nations system decisions, resolutions and recommendations address issues related to cybercrime, the most important being the following: the United Nations Office for Drugs and Crime (UNODC) and the Commission on Crime Prevention and Criminal Justice's resolution on effective crime prevention and criminal justice responses to combat sexual exploitation of children.[27] In 2004, the United Nations Economic and Social Council's resolution on international cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes. A working group was established in 2005. A core group of experts on identity-related crime was created to undertake a comprehensive study on the issue. In 2007, the ECOSOC adopted a resolution on international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime.[28] Neither of these two resolutions explicitly addresses the challenges of Internet-related crimes, but they are applicable to those offences as well. Based on ECOSOC Resolution 2004/26 and ECOSOC Resolution 2007/20, UNODC in 2007 established a core group of experts to exchange views on the best course of action.[29] The core group has undertaken several studies that included aspects of Internet-related crimes.

[27] Ladan M.T. (2015) *op cit* P.8

[28] ECOSOC Resolution 2007/20, on International Cooperation in the Prevention, Investigation, Prosecution and Punishment of Economic Fraud and Identity-Related Crime, retrieved from www.un.org/ecosoc/docs/2007/Resolution%202007-20.pdf. 10:50am

[29] Marco G. (2011*) Legal Approaches to Criminalize Identity Theft: in UNDC Handbook on Identity- Related Crime* p.1 retrieved at www.unodc.org/documents/organized-crime/Courmayeur_report.pdf 20/06/2016 11:00pm

In 2004, ECOSOC had adopted a resolution on the sale of licit drugs via the Internet that explicitly took account of a phenomenon related to a computer crime.

3.2.16 UNODC/ITU Memorandum of Understanding

In 2011 UNODC and the International Telecommunication Union (ITU) signed a memorandum of understanding related to cybercrime. The MoU covers cooperation (especially capacity building and technical assistance for developing countries), training and joint workshops. With regard to the capacity building activities the two organizations can refer to a wide network of field offices in all continents. Furthermore, the organizations agreed to a joint dissemination of information, and knowledge and data analysis.

3.2.17 International Telecommunication Union[30]

The International Telecommunication Union (ITU), as a specialized agency within the United Nations, plays a leading role in the standardization and development of telecommunications as well as cybersecurity issues.A fundamental role of ITU, based on the guidance of the World Summit on the Information Society (WSIS) and the ITU Plenipotentiary Conference, is to build confidence and security in the use of Information and Communication Technologies (ICTs).

At WSIS, Heads of States and world leaders entrusted ITU to be the Facilitator of Action Line C5, "Building confidence and security in the use of ICTs", in response to which ITU launched, in 2007, the Global Cybersecurity Agenda (GCA), as a framework for international cooperation in the area of cybersecurity.

3.2.18 World Summit on the Information Society

The World Summit on the Information Society (WSIS) took place in two phases in Geneva, Switzerland (2003) and in Tunis, Tunisia (2005). Governments, policy-makers and experts

[30]Understanding cybercrime: Phenomena, Challenges and Legal Response Retrieved 10/08/2016 10:10am from www.itu.int.

from around the world shared ideas and experiences about how best to address the emerging issues associated with the development of a global information society, including the development of compatible standards and laws. The outputs of the summit are contained in the *Geneva Declaration of Principles*, the *Geneva Plan of Action*; the *Tunis Commitment* and the *Tunis Agenda for the Information Society*. The Geneva Plan of Action highlights the importance of measures in the fight against cybercrime:[31]

Cybercrime was also addressed at the second phase of WSIS in Tunis in 2005. The Tunis Agenda for the Information Society[32]highlights the need for international cooperation in the fight against cybercrime and refers to the existing legislative approaches such as the UN General Assembly resolutions and the Council of Europe Convention on Cybercrime:

3.2.19 Global Cybersecurity Agenda

As an outcome of WSIS, ITU was nominated as the sole facilitator for Action Line C5 dedicated to building of confidence and security in the use of information and communication technology.[33] At the second Facilitation Meeting for WSIS Action Line C5 in 2007, the ITU Secretary-General highlighted the importance of international cooperation in the fight against cybercrime and announced the launch of the ITU Global Cybersecurity Agenda.[34] The Agenda is made up of seven key goals,[35] and built upon five strategic pillars: legal measures, technical and procedural measures, organizational structures,

[31]2003 WSIS Geneva Plan of Action. Retrieved at www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0. On 20/05/2016
[32]Roxana R, Jean-Marie C, Rolf H. Weber (2014) *the Evolution of Global Internet Governance: Principles and Policies in the Making*. Retrieved at www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0. On 20/06/2016 12:40pm
[33]Meeting Report of the Second Facilitation Meeting for WSIS Action Line C5, 2007, page 1, retrieved at www.itu.int/osg/csd/cybersecurity/pgc/2007/events/docs/meetingreport.pdf, and the meeting report of the third Facilitation Meeting for WSIS Action Line C5, 2008, www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/WSIS_Action_Line_C5_Meeting_Report_June_2008.pdf. accessed 29/08/2016 11:20am
[34]Adil D, (2012) *Analysing Different Dimensions and New Threats in Defence Against Terrorism,*IOS Press, United States.
[35]*Ibid.*

capacity building, international cooperation[36], including the elaboration of strategies for the development of model cybercrime legislation. The seven goals are: 1) Elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures; 2)elaboration of strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime; 3) development of a strategy for the establishment of globally accepted minimum security criteria and accreditation schemes for software applications and systems; 4) development of strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives; 5) development of strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organizational structures to ensure the recognition of digital credentials for individuals across geographical boundaries; 6) development of a global strategy to facilitate human and institutional capacity-building to enhance knowledge and know-how across sectors and in all the above-mentioned areas; and 7) advice on potential framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas.

In order to analyse and develop measure and strategies with regard to the seven goals of the GCA, the ITU Secretary-General created a high-level expert group (HLEG) bringing together representatives from member states, industry as well as the scientific field.[37] In 2008, the expert group concluded negotiations and published the "Global Strategic Report".[38] Most relevant with regard to cybercrime are the legal measures contained in Chapter 1. In addition to an overview of different regional and international approaches in

[36]*Ibid.*
[37]John G. V. (2008) *Wiley Handbook of Science and Technology for Homeland Security*. Retrieved at www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html. 20/07/2018
[38]Gercke, Z. Fuer U. andMedienrecht, (2009), *Global Strategic Report*, *Issue 7*, page 533. Retrieved on 20/07/2018 10:40am from www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html;

fighting cybercrime,[39] the chapter provides an overview of criminal law provisions, procedural instruments, regulations governing the responsibility of internet service providers and safeguards to protect fundamental rights of Internet users.

3.2.21 Resolutions

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

1. ITU Plenipotentiary Conference Resolution 130 (Rev. Guadalajara, 2010), on Strengthening the role of ITU in building confidence and security in the use of information and communication technologies.
2. ITU Plenipotentiary Conference Resolution 149 (Antalya, 2006), on Study of definitions and terminology relating to building confidence and security in the use of information and communication technologies.
3. Resolution 45 (Doha, 2006) of the World Telecommunication Development Conference (WTDC), on Mechanisms for enhancing cooperation on cybersecurity, including combating spam and the report from *Meeting on Mechanisms for Cooperation on Cybersecurity and Combating Spam* (31 August – 1 September 2006).
4. Resolution 50 (Rev. Johannesburg, 2008) of the World Telecommunication Standardization Assembly (WTSA), on Cybersecurity.
5. Resolution 52 (Rev. Johannesburg, 2008) of the World Telecommunication Standardization Assembly (WTSA), on Countering and combating spam.
6. Resolution 58 (Johannesburg, 2008) of the World Telecommunication Standardization Assembly (WTSA), on Encouraging the creation of national computer incident response teams, particularly for developing countries.

[39]Gercke (2008), National, Regional and International Approaches in the Fight against Cybercrime, *Computer Law Review International*, (Issue 1), page 7.

3.3 Regional Response to Cyber Threats

In addition to the international organizations that are globally active, a number of regional organizations have made substantial efforts to curb illegal activities in the cyber space; they have developed instruments to further harmonize laws in order to tackle the incessant threats to the cyber space. Some of these regional responses are highlighted below:

3.3.1 Europe's Responses to Cybersecurity

a. Council of Europe[40]

The Council of Europe is playing an active role in addressing the challenges of cybercrime. The Council of Europe highlighted the international nature of computer-related crimes and discussed the topic at a conference dealing with aspects of economic crimes. This topic has since remained on its agenda. The Council of Europe appointed an Expert Committee to discuss the legal aspects of computer crimes. The European Committee on Crime Problems adopted the Expert Report on Computer-Related Crime,[41] analysing the substantive criminal legal provisions necessary to fight new forms of electronic crimes, including computer fraud and forgery.The Council of Europe has come up with several other conventions and protocol as highlighted hereunder;

b. Council of Europe Convention on Cybercrime and the Additional Protocol

The Convention on Cybercrime is today recognized as an important regional instrument in the fight against cybercrime and is supported by different international organizations. The Convention on Cybercrime was followed by the First Additional Protocol to the Convention on Cybercrime. During the negotiations on the text of the Convention on

[40] *ibid*

[41] 2005 United Nations Conference on Trade and Development, Information Economy Report, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, retrieved 10/06/2016 10:45am from www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

Cybercrime, it turned out that the criminalization of racism and the distribution of xenophobic material were particularly controversial matters. Some countries in which the principle of freedom of expression was strongly protected expressed their concern that if provisions are included in the Convention on Cybercrime that violate freedom of expression they would be unable to sign the Convention. To avoid a situation where countries would not be able to sign the Convention because of freedom of expression concerns, those issues were removed from the Convention on Cybercrime during the drafting process and integrated into a separate protocol.

Currently, the Council of Europe Convention on Cybercrime is still the instrument with the broadest reach supported by different international organizations.[42]Several countries such as Argentina,[43] Pakistan,[44] Philippines,[45] Egypt,[46] Botswana and Nigeria[47] have used the Convention as a model and drafted parts of their legislation in accordance with the Convention on Cybercrime. One of the key intentions of the Convention was to provide a comprehensive legal approach that addresses all relevant areas of cybercrime.

c. Council Decision to combat child pornography on the Internet

In 2000, the Council of the European Union undertook an approach to address child pornography on the Internet. The Decision that was adopted is a follow-up to the 1996 communication on illegal and harmful content on the Internet and the related 1999 action plan on promoting safer use of the Internet and combating illegal and harmful content on global networks. However, the Decision does not contain obligations with regard to the adoption of specific criminal law provisions.

[42]Ibid.
[43] Draft Electronic Crime Act 2006.
[44]Draft Act Defining Cybercrime, Providing for Prevention, Suppression and Imposition of Penalties therefore and for other Purposes, House Bill No. 3777.
[45] Draft Law Regulating the Protection of Electronic Data and Information and Combating Crimes of Information, 2006.
[46] Draft Cybercrime and Computer related Crimes Bill 2007, Bill No. 17 of 2007.
[47] Draft Computer Security and Critical Information Infrastructure Protection Bill 2005.

d. E-Commerce Directive (2000)

The EU Directive on Electronic Commerce[48] addresses, among other issues, the liability of Internet service provider (ISP) for acts committed by third parties (Article 12 *et seq.*). Taking into account the challenges stemming from the international dimension of the network, the drafters decided to develop legal standards to provide a framework for the overall development of the information society and to support overall economic development as well as the work of law-enforcement agencies.[49] It is based on the consideration that development of information-society services is hampered by a number of legal obstacles to the proper functioning of the internal market, which gives the European Community its mandate. The regulation of liability is based on the principle of graduated responsibility. Although the Directive highlights that there is no intention to harmonize the field of criminal law as such, it does however regulate liability under criminal law.[50]

e. European Union Council Framework Decision on combating fraud (2001)

In 2001, the EU adopted the first legal framework directly addressing aspects of cybercrime. The EU Framework Decision on combating fraud and counterfeiting of non-cash means of payment[51] contains obligations to harmonize criminal law legislation with regard to specific aspects of computer-related fraud and the production of instruments, such as computer programs, that are specifically adopted for the purpose of committing an offence mentioned in the Framework Decision.[52]

---

[48] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') *Official Journal* L 178, 17/07/2000 P. 0001 – 0016. http://db.consilium.eu.int/de/Info/eurocouncil/index.htm..accessed 05/08/2016 12:00pm

[49] Lindholm/Maennel (2000), *Computer Law Review International*, 65. http://db.consilium.eu.int/de/Info/eurocouncil/index.htm.. accessed 05/08/2016 12:00pm

[50] Gercke (2010), Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, *Computer Law Review International*. 75

[51] Decision No. 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (276/1999/EC)..

[52] Council Framework Decision of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment(2001/413/JHA)

Article 3 – Offences related to computers
Each Member State shall take the necessary measures to ensure that the following conduct is a criminal offence when committed intentionally: performing or causing a transfer of money or monetary value and thereby causing an unauthorised loss of property for another person, with the intention of procuring an unauthorised economic benefit for the person committing the offence or for a third party, by:
- without right introducing, altering, deleting or suppressing computer data, in particular identification data, or
- without right interfering with the functioning of a computer programme or system.

In line with the prevailing opinion at that time and as a consequence of the lack of a mandate in the first pillar, the instrument was developed under the third pillar, thereby highlighting that in view of the international dimension of the phenomena involved, such issues cannot be adequately addressed by the Member States themselves.

f. European Union Council Framework Decision on attacks against information systems (2005)

After the publication of the general policy in 2001, the European Union Council presented a proposal for a framework decision on attacks against information systems.[53] It was modified and adopted by the Council in 2005.[54] Although it takes note of the Council of Europe Convention on Cybercrime, it concentrates on the harmonization of substantive criminal law provisions that are designed to protect infrastructure elements. Aspects of criminal procedural law (especially the harmonization of the instruments necessary to investigate and prosecute cybercrime) and instruments related to the international cooperation were not integrated into the framework decision. It highlights the gaps and differences in the legal frameworks of the Member States and effective police and judicial cooperation in the area of attacks against information systems.[55]

[53] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. The legal basis for the Framework Decision, Indicated in the Preamble of the Proposal for the Framework Decision is Articles 29, 30(a), 31 and 34(2)(b) of the Treaty on European Union. See http://db.consilium.eu.int/de/Info/eurocouncil/index.htm..accessed 05/08/2016 12:00pm
[54] *ibid*
[55] The Explanation of the Framework Decision in the Proposal for a Council Framework Decision on Combating Serious Attacks Against Information Systems, No. 1.6. Accessed at http://db.consilium.eu.int/de/Info/eurocouncil/index.htm. 05/08/2016 12:00pm

h. Data Retention Directive (2005)

In 2005, the Council adopted the European Union Data Retention Directive. It contains an obligation for Internet Service Providers to store certain traffic data that are necessary for the identification of criminal offenders in cyberspace. Article 3(1) and (2) of the directive provides for obligation to retain data, it provides that:

> 1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.
> 2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the pro- cess of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.

The Directive was based on the European Community's mandate for the internal market (Article 95).

j. Amendment of the European Union Council Framework Decision on combating Terrorism (2007)

In 2007, the European Union started discussion on a draft amendment of the Framework Decision on combating terrorism. In the introduction to the draft amendment, the EU highlights that the existing legal framework criminalizes aiding or abetting and inciting but does not criminalize the dissemination of terrorist expertise through the Internet.[56] With the amendment, the EU is aiming to take measures to close the gap and bring the legislation throughout the EU closer to the Council of Europe Convention on the Prevention of Terrorism. The amendment introduced article 3(2) which deals with offences linked to terrorist activities. The article provides:

[56] Council Framework Decision 2008/919/JHA of 28 November 2008 Amending Framework Decision 2002/475/JHA on Combating Terrorism. See http://db.consilium.eu.int/de/Info/eurocouncil/index.htm..accessed 05/08/2016 12:00pm

2. Each Member State shall take the necessary measures to ensure that terrorist-linked offences include the following intentional acts:
(a) public provocation to commit a terrorist offence;
(b) recruitment for terrorism;
(c) training for terrorism;
(d) aggravated theft with a view to committing one of the acts listed in Article 1(1);
(e) extortion with a view to the perpetration of one of the acts listed in Article 1(1);
(f) drawing up false administrative documents with a view to committing one of the acts listed in Article 1(1)(a) to (h) and Article 2(2)(b).
3. For an act to be punishable as set forth in paragraph 2, it shall not be necessary that a terrorist offence be actually committed."

Based on Article 3(1)(c)[57] of the framework decision, the member states are, for example, obliged to criminalize the publication of instructions on how to use explosives, knowing that this information is intended to be used for terrorist-related purposes. The need for evidence that the information is intended to be used for terrorist-related purposes very likely limits the application of the provision with regard to the majority of instructions on how to use weapons that are available online, as their publication does not directly link them to terrorist attacks. As most of the weapons and explosives can be used to commit "regular" crimes as well as terrorist-related offences (dual use), the information itself can hardly be used to prove that the person who published them had knowledge about the way such information is used afterwards. Therefore, the context of the publication (e.g. on a website operated by a terrorist organization) needs to be taken into consideration.

c. Convention on the Protection of Children

Within its approach to improve the protection of minors against sexual exploitation, the Council of Europe introduced a new Convention in 2007.[58] One of the key aims of the Convention on the Protection of Children is the harmonization of criminal law provisions aimed at protecting children from sexual exploitation. To achieve this aim, the Convention

[57] Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism.
[58] ibid

contains a set of criminal law provisions. Apart from criminalization of the sexual abuse of children (Article 18), the Convention contains provisions dealing with the exchange of child pornography (Article 20) and the solicitation of children for sexual purposes (Article 23).

d. Directive on child pornography2011

The first cybercrime-related draft legal framework presented after the ratification of the Treaty of Lisbon was the proposal for a Directive on combating the sexual abuse and sexual exploitation of children and child pornography that was adopted in 2011.[59] It implements international standards, such as the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

The Directive proposes the criminalization of obtaining access to child pornography by means of information and communication technology.[60] This enables law-enforcement agencies to prosecute offenders in cases where they are able to prove that the offender opened websites with child pornography, but are unable to prove that the offender downloaded material. Such difficulties in collecting evidence arise, for example, if the offender is using encryption technology to protect downloaded files on his storage media. The Explanatory Report to the Convention on the Protection of Children points out that the provision should also be applicable in cases where the offender only views child pornography pictures online without downloading them. In general, opening a website does automatically initiate a download process – often without the knowledge of the user. As a consequence, the provision is mainly relevant in cases where consumption of child pornography can take place without download of material. This can, for example, be the case if the website enables streaming videos and, due to the technical configuration of the

[59] Directive 2011/92/EU of the European Parliament and of The Council of 13 December 2011 on Combating The Sexual Abuse And Sexual Exploitation Of Children And Child Pornography, And Replacing Council Framework Decision 2004/68/JHA

[60] See Art. 5, No. 3, of the Draft Directive.

streaming process, does not buffer the received information but discards it straight after transmission.

In addition to the criminalization of acts related to child pornography, the initial draft contained a provision that obliges Member States to implement the process of blocking websites containing child pornography.[61] Several European countries,[62] as well as non-European countries like China, Iran and Thailand, use such an approach. Concerns relate to the fact that none of the technical concepts has proven to be effective, and the approach entails a concomitant risk of over-blocking. As a consequence, the mandatory blocking was changed and it was left to Member States to decide if blocking obligations should be implemented on the national level.

e. The European Union Agency for Cybersecurity (ENISA)

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004.The Agency works closely together with Members States and other stakeholders to deliver advice and solutions as well as improving their cybersecurity capabilities. It also supports the development of a cooperative response to large-scale cross-border cybersecurity incidents or crises and since 2019; it has been drawing up cybersecurity certification schemes.[63]

l. Organisation for Economic Co-operation and Development[64]

The Organisation for Economic Co-operation and Development **(**OECD)is a unique forum where governments work together to address the economic, social and environmental

[61]Gercke (2009), the Role of Internet Service Providers in the Fight against Child Pornography. *Computer Law Review Internationa*l, p. 69.
[62]Clayton/Murdoch/Watson, Ignoring the Great Firewall of China, retrieved 13/7/2018 2:00pm fromwww.cl.cam.ac.uk/~rnc1/ignoring.pdf;
[63]ENISA (2012) *National Cyber Security Strategies Practical Guide on Development and Execution*, retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-strategy-for-germany/view accessed on 06/08/2019 at 4:38pm
[64] The Organisation for Economic Co-operation and Development was founded 1961. It has 34 member countries and is based in Paris. For more information, see: www.oecd.org

challenges of globalization. The OECD is at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organization provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Union takes part in the work of the OECD.

The OECD focuses on security in cyberspace as a driver for economic prosperity and social development. The 2002 Recommendation of the OECD Council concerning Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security (the 2002 Security Guidelines) established the first international set of fundamental principles focused on the development of security policies in an open environment. They can be used by governments to develop national policies as well as by public and private organisations to design their own security policies

In 2003 and 2004, the OECD carried out a survey to examine how governments undertook the implementation of the 2002 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security ("Security Guidelines"). The results of this survey highlighted that almost all governments had finalised their national strategy for fostering a culture of security (OECD, 2005). Between 2009 and 2011, several countries

adopted or initiated the development of a new generation of strategies, sometimes called "cybersecurity strategies".

One of the major tools utilized by the OECD is the comparison of National cybersecurity strategies of member nations. Its comparison of national cybersecurity strategies provides a useful source of information and inspiration in the context of the review of the Guidelines initiated in 2012.[65] The comparative analysis of a new generation of national cybersecurity strategies in ten OECD countries reveals that cybersecurity policy making is at a turning point. In many countries today, it has become a national policy priority supported by stronger leadership.[66]

As at 2019 in pursuit of its policies the OECD is making efforts to encourage tax administrations around the globe to step up their efforts to support the fight against money laundering and terrorist financing. It has launched a handbook intended to raise the awareness of tax examiners, auditors, and investigators of the important role they can play in combating these crimes.[67]

3.3.2 Response of the Asian Countries to cybersecurity Threats

a. Asia-Pacific Economic Cooperation[68]

The Asia-Pacific Economic Cooperation (APEC) has identified cybercrime as an important field of activity, and APEC leaders have called for closer cooperation among officials involved in the fight against cybercrime.The Declaration of the 2008 meeting of the APEC

[65]OECD (2002) *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. Retrieved at http://oe.cd/security. 15/08/2019 at 4:30pm

[66] OECD (2012) *Cybersecurity Policy Making at a Turning Point: Analysing a new generation of national cybersecurity strategies for the Internet economy*, available at https://www.oecd. org/sti/ieconomy /cybersecurity %20policy%20making.pdf accessed 15/08/2019 at 4:30pm

[67]APEC/OECD (2019), *Combatting Tax Crimes More Effectively in APEC Economies, Organisation for Economic Co-operation and Development and Asia-Pacific Economic Cooperation*. Retrieved from www.oecd.org/tax/crime/combatting-tax-crimes-more-effectively-in-apec-economies.htm. 28/07/2018 10:55am

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

Telecommunication and Information Ministers in Bangkok, Thailand, highlighted the importance of continuing collaboration to combat cybercrime. Until now, APEC has not provided a legal framework on cybercrime, but has referred to international standards such as the Budapest Convention on Cybercrime. In addition, APEC has closely studied the national cybercrime legislation in various countries under a cybercrime legislation survey, and has developed a database of approaches to assist economies in developing and reviewing legislation. The questionnaire used for the survey was based on the legal framework provided by the Budapest Convention on Cybercrime.

b. Statement on fighting terrorism (2002)

In 2002, APEC leaders released a Statement on Fighting Terrorism and Promoting Growth to enact comprehensive laws relating to cybercrime and develop national cybercrime investigating capabilities.[69] They committed to endeavouring to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with the provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 and the Council of Europe Convention on Cybercrime, by October 2003. In addition, they committed to identifying national cybercrime units and international high technology assistance points of contact and creating such capabilities, to the extent they do not already exist, by October 2003, and establishing institutions that exchange threat and vulnerability assessment (such as computer emergency response teams).

c. Telecommunications and Information Working Group

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

[69] Russell S., Kopparthi S., Gregor U. (2004) Cyber Criminals on Trial: *Criminal Justice Matters*. Retrieved from www.aic.gov.au/conferences/other/urbas_gregor/2001-04-cybercrime.pdf. accessed 28/09/2018 10:55am

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

d. Conference on cybercrime legislation (2005)

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

3.3.3 The Response of the Common wealth to Cybersecurity Threats

Cybercrime is among the issues addressed by the Commonwealth. Their activities concentrate in particular on harmonization of legislation. This approach to harmonize legislation within the Commonwealth and enable international cooperation was influenced, among other things, by the fact that, without such an approach, it would require several bilateral treaties within the Commonwealth to deal with international cooperation in this matter taking into account the rising importance of cybercrime.

At the 2000 meeting, the Law Ministers and Attorney-Generals of small Commonwealth jurisdictions decided to set up an expert group to develop model legislation on digital evidence. The Law Ministers of the Commonwealth also mandated an expert group to develop a legal framework for combating cybercrime on the basis of the Council of Europe

Convention on Cybercrime. The Expert Group presented its report and recommendations as well as the draft Model Law on Computer and Computer Related Crime in 2002[70],

In addition to providing legislation, the Commonwealth has organized several training activities. The Commonwealth Network of IT and Development (COMNET-IT) co-organized training on cybercrime in April 2007. In 2009, the Commonwealth Third Country Training Programme on legal framework for ICT was held in Malta, with the support of the Commonwealth Fund for Technical Co-operation (CFTC). Another training was organized in 2011. In 2011 the Commonwealth presented "The Commonwealth Cybercrime Initiative". The main objective of the initiative is to assist Commonwealth countries in building their institutional, human and technical capacities with respect to policy, legislation, regulation, investigation and law enforcement. It aims to enable all Commonwealth countries to effectively cooperate in the global combat of cybercrime.

3.3.4 Africa's Response to Cybersecurity Threats

a. African Union

African Union has played very important in Africa's efforts to contain cyber threats. During the extra-ordinary conference of the African Union Ministers in charge of Communication and Information Technologies, which was held in Johannesburg in 2009, the ministers addressed various topics related to the increasing use of ICT in the African country. It was decided that African Union Commission should – jointly with the UN Economic Commission for Africa – develop a legal framework for African countries that addresses issues like electronic transactions, cyber security and data protection.[71]

[70] Model Law on Computer and Computer Related Crime, LMM (02)17; available www.thecommonwealth.org /sharedaspfiles/uploadedfiles/%7BDA109CD2-5204-4FABAA7786970A639B05%7D_Computer%20Crime.pdf. Accessed 30/07/2017 12:30pm

[71] Marco G. (2014*) Understanding cybercrime: Phenomena, Challenges and Legal Response* retrieved from www.uneca.org/aisi/docs/AU/The%20Oliver%20Tambo%20Declaration.pdf accessed 28/04/2016 3:45pm

In 2011 the African Union presented the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity in Africa. The intention of the drafters is to strengthen existing legislation in member states regarding information and communication technologies. With regard to the mandate, that was not limited to cybercrime, but also included other information society issues such as data protection and electronic transactions- The Convention is more comprehensive than most other regional approaches. It contains four parts. Part one is related to electronic commerce. It addresses various aspects such as contractual responsibility of an electronic provider of goods and services, treaty obligations in electronic form and security of electronic transactions. The second part deals with data protection issues. The third part is related to combating cybercrime. Section 1 contains five chapters. This includes a set of six definitions (electronic communication, computerized data, racism and xenophobia in ICTs, minor, child pornography and computer system).[72]

Additionally, the third part addresses the need of a national cybersecurity policy and a related strategy. The second chapter deals with general aspects related to legal measures. This includes standards related to statutory authorities, democratic principles, protection of essential information infrastructure, harmonization, double criminality and international cooperation.[73] The third chapter addresses issues related to a national cybersecurity system. This includes a culture of security, the role of the government, public-private partnership, education and training and public awareness-raising.[74] Chapter 4 is dedicated to national cybersecurity monitoring structures. The fifth chapter addresses international cooperation.

> Article III – 1 – 21: International cooperation
> Each Member State shall adopt such measures as it deems necessary to foster exchange of information and the sharing of quick, expeditious and

[72] Art. III-1.
[73] Art. III-1-1 to Art. III-1-7
[74] Art. III-1-8 to Art. III-1-12.

> reciprocal data by Member States' organizations and similar organizations of other Member States with responsibility to cause the law to be applied in the territory on bilateral or multilateral basis.
> Article III – 1 – 25: Model of international cooperation
> Each Member State shall adopt such measures and strategies as it deems necessary to participate in regional and international cooperation in cybersecurity. The Resolutions geared to promoting Member States' participation within this framework of relations have been adopted by a large number of international governmental bodies including the United Nations, the African Union, the European Union, the G8, etc. Organizations like the International Telecommunication Union, the Council of Europe, the Commonwealth of Nations and others, have established model frameworks for international cooperation which Member States may adopt as a guide.

The convention also deals with substantive penal law which includes criminalization of illegal access to a computer system, illegal retaining oneself in a computer system, illegal system interference, illegal data input, illegal data interception and illegal data interference.[75] The provisions show a lot of similarities with best practices from other regions – including standards introduced within Africa.

It also criminalises aspects of computer-related forgery, illegal use of data, illegal system interference with the intent to obtain an advantage, data protection violations, illegal devices and participation in a criminal organization.[76]

The criminalisation of illegal use of computer data is going beyond the standards defined by most other regional instruments. The Draft African Convention introduces a criminalisation of producing and disseminating child pornography, procuring and importing child pornography, possessing child pornography, facilitating the access of minors to pornography, dissemination of racist or xenophobic material, racist attacks perpetrated through computer systems, racist abuse through computer systems and denying

[75] Art. III-7 1)
[76] See 1272 Art. III-8. Art. III-9, Art. III-10., Art. III-11, Art. III-12. Art. III-13.

or approving genocide or crimes against humanity.[77] The convention contains provisions that deal in a broader manner with legislation related to Cybercrime and the admissibility of electronic evidence ("written electronic matter").

b. African Union Convention on Cybersecurity and Personal Data Protection

This Convention on the establishment of a Legal Framework for Cyber-security and Personal Data Protection embodies the existing commitments of African Union Member States at sub-regional, regional and international levels to build the Information Society; it aims at defining the objectives and broad orientations of the Information Society in Africa and strengthening existing legislations on Information and Communication Technologies (ICTs) of Member States and the Regional Economic Communities (RECs).

The goal of this Convention is to address the need for harmonized legislation in the area of cyber security in member states of the African Union, and to establish in each State party a mechanism capable of combating violations of privacy that may be generated by personal data collection, processing, transmission, storage and use. By proposing a type of institutional basis, the Convention guarantees that whatever form of processing is used shall respect the basic freedoms and rights of individuals while also taking into account the prerogatives of States, the rights of local communities and the interests of businesses; and take on board internationally recognized best practices.

The Convention seeks, in terms of substantive criminal law, to modernize instruments for the repression of cybercrime by formulating a policy for the adoption of new offences specific to ICTs, and aligning certain offences, sanctions and criminal liability systems in force in Member States with the ICT environment.

[77] See Art. III-14, Art. III-15, Art. III-16, Art. III-17, Art. III-19, Art. III-20, Art. III-21, Art. III-22.

3.3.5 Responses of the Arab World to Cyber Security Threats

a. Arab League and Gulf Cooperation Council[78]

A number of countries in the Arab region have already undertaken national measures and adopted approaches to combat cybercrime, or are in the process of drafting legislation. Examples of such countries include Pakistan,[79] Egypt and the United Arab Emirates (UAE).[80] In order to harmonize legislation in the region, UAE submitted model legislation to the Arab League (Guiding Law to Fight IT Crime).[81] In 2003, the Arab Interior Ministers Council and the Arab Justice Ministers Council adopted the law. The Gulf Cooperation Council (GCC)[82] recommended at a conference in 2007 that the GCC countries seek a joint approach that takes into consideration international standards.

b. Arab League Convention on Cybercrime

The Arab Convention on Combating Information Technology Offences, signed by the Sultanate on 15/02/2012, had been issued on the basis of the public interest. This convention aims to strengthen and support the bonds of cooperation among the Arab states in the field of combating IT offences, in order to ward off the dangers of crimes, maintaining the security of Arab states and the interests and safety of their communities and members.

The Convention states that each member state, in accordance with its basic systems or constitutional principles, is committed to fulfilling its obligations arising from the application of this Convention in a manner consistent with the principles of equality in the

[78] Solange G. (2016) Cyber Power: Crime, Conflict and Security in Cyberspace, CRC Press, retrieved from www.itu.int /osg/csd/cybersecurity/gca/global_strategic_report/index.html. accessed 20/6/2016 2:30pm

[79] Draft Law on Regulating the Protection of Electronic Data and Information and Combating Crimes of Information, 2006.

[80] Law No. 2 of 2006, enacted in February 2006.

[81] 2007 Regional Conference Booklet on Cybercrime, Morocco, p.6, from www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.retrieved 12/06/2019 8:40pm

[82] Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and UAE.

territorial sovereignty of states and non-interference in the interior affairs of other states, and that the Convention does not entitle any member state to undertake, in the territory of another state, the judicial jurisdiction nor the functions that are reserved exclusively for the authorities of that other state in accordance with its domestic law.

The Convention also provides for the imposition of sanctions on the entry, amendment or withholding some information, mail fraud, interference with the private lives or posting obscene materials.

3.3.6 The Americas Response to Cybersecurity Threats

a. Organization of American States[83]

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

The Meetings of REMJA recommended the establishment of an intergovernmental expert group on cybercrime. The expert group was mandated to complete a diagnosis of criminal activity which targets computers and information, or which uses computers as the means of committing an offence; complete a diagnosis of national legislation, policies and practices regarding such activity; identify national and international entities with relevant expertise; and finally identify mechanisms of cooperation within the inter-American system to combat cybercrime.

[83] Marco G. (2012) *Understanding Cybercrime: Phenomena, Challenges and Legal Response,* ITU retrieved at www.oas.org/juridico/english/cyber.htm, and at: www.oas.org/juridico/english/ ministry_of_justice_v.htm. accessed 12/8/2018 12:40pm

REMJA addressed the topic of cybercrime and agreed on a number of recommendations.[84]These recommendations included agreement to support consideration of the recommendations made by the Group of Governmental Experts at REMJA'sinitial meeting as its contribution to the development of the Inter-American Strategy to Combat Threats to Cybersecurity, referred to in OAS General Assembly Resolution AG/RES. 1939 /XXXIII-O/03), and to ask the group, through its chair, to continue to support the preparation of the strategy.

The meeting further recommended that Member States should review mechanisms to facilitate broad and efficient cooperation among themselves to combat cybercrime and study, where possible, the development of technical and legal capacity to join the 24/7 Network established by the G8 to assist in cybercrime investigations. Member States were asked to evaluate the advisability of implementing the principles of the Council of Europe Convention on Cybercrime and consider the possibility of acceding to that Convention.

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

The organisation also considered the preparation of pertinent inter-American legal instruments and model legislation for the purpose of strengthening hemispheric cooperation in combating cybercrime and considering standards relating to privacy, the protection of information, procedural aspects, and crime prevention. Member States were asked to establish specialized units to investigate cybercrime, identify the authorities who will serve

[84]Stein S. (2008) *The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva* retrieved from www.oas.org/juridico/english/cyber_meet.htm. accessed 12/8/2016 11:20am

as the points of contact in this matter and expedite the exchange of information and obtaining of evidence, and in addition, to foster cooperation in efforts to combat cybercrime among government authorities and Internet service providers and other private-sector enterprises providing data transmission services.

Similarly, the organisation recommended that technical cooperation activities continue to be held under the auspices of the OAS General Secretariat, through the Secretariat for Legal Affairs, and the Council of Europe, and that efforts be continued to strengthen exchange of information and cooperation with other international organizations and agencies in the area of cybercrime, so that the OAS Member States may take advantage of progress in those forums. Finally, the secretariats of the Inter-American Committee against Terrorism (CICTE) and the Inter-American Telecommunication Commission (CITEL) and the Working Group on Cybercrime were requested to continue developing permanent coordination and cooperation actions to ensure the implementation of the Comprehensive Inter-American Cybersecurity Strategy adopted through OAS General Assembly Resolution AG/RES. 2004 (XXXIV-O/04).

3.3.7 The Caribbean's Response to Cybersecurity Threats

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

and legal frameworks. Under this project, nine work areas have been identified[85] in which model policies and model legislative texts were developed to facilitate the development and harmonization of legislation in the region. Cybercrime was one of the nine work areas. The development of the model legislative text took place in three phases.

In the first phase, existing legislation in the beneficiary countries was collected and reviewed. Parallel, regional and international best practices were identified. Priority was given to standards that are directly applicable in at least some of the beneficiary countries. The review also included best practices from other regions, such as the EU and Africa. The assessment report contained an overview of the existing legislation, as well as a comparative law analysis that compared the existing legislation with regional and international best practices. In order to prepare a gap analysis, the assessment report in addition identified special needs in the region (such as legislation on spam) that are not necessarily addressed by international best practices. The assessment report was discussed with stakeholders from the beneficiary countries. On the basis of the assessment report and gap analysis, the stakeholders drafted model policy guidelines.

In the second phase, a model legislative text was developed taking into account the policy guidelines. At a second workshop, policy experts, law drafters and other stakeholders from the beneficiary countries discussed and amended the draft model legislative text that was prepared for the meeting, and adopted it. The model legislative text has three key aims: it provides specific sample language that is in line with international best practices, it reflects the special demands of the region and it is developed with law drafting practices in the region in mind, so as to ensure smooth implementation. The model legislative text contains a complex set of definitions, and substantive criminal law provisions, including provisions

[85] Electronic transactions, Electronic evidence in e-commerce, Privacy and data protection, Interception of communications, Cybercrime, Access to public information (freedom of information), Universal access and service, Interconnection and access and finally Licensing.

dealing with issues like SPAM that have a high priority for the region but are not necessarily contained in regional frameworks such as the Council of Europe Convention on Cybercrime.

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

3.3.8 The Pacific's Response to cybersecurity Threats

In parallel to the ITU and EU co-funded project in the Caribbean the same organizations launched a project in the Pacific (ICB4PAC).[86] The project aims – based on a request by the Pacific Island countries – to provide capacity building related to ICT policies and regulations. In this regard it focuses on building human and institutional capacity in the field of ICT through training, education and knowledge sharing measures. Beneficiary countries are 15 Pacific Island countries.

The project included a comprehensive comparative legal analysis that provided an overview about existing legislation in the region as well as a comparison with best practices from other regions. Best practices from other regions were presented and structures for a harmonized policy and legislation were developed. They addressed substantive criminal law, procedural law, international cooperation, liability of Internet Service Provider (ISP), electronic evidence and crime prevention measures.

The Secretariat of the Pacific Community organized a conference related to the Fight against

[86]Gerke M. (2009), *Strategy, Policy, Legislation, Prevention and enforcement*. Retrieved from www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html 9/3/2020

Cybercrime in the Pacific. The event was co-organized by the Council of Europe. During the conference aspects related to substantive criminal law, procedural law and international cooperation were discussed.

3.4 Scientific and Independent Approaches to Cybersecurity Issues

a. Stanford Draft International Convention

A well-known example of a scientific approach to developing a legal framework for addressing cybercrime at the global level is the Stanford Draft International Convention (the "Stanford Draft").[87] The Stanford Draft was developed as a follow-up to a conference hosted by Stanford University in the United States in 1999.[88] Comparison with the Council of Europe Convention on Cybercrime[89] that was drafted around the same time shows a number of similarities. Both cover aspects of substantive criminal law, procedural law and international cooperation. The most important difference is the fact that the offences and procedural instruments developed by the Stanford Draft are only applicable with regard to attacks on information infrastructure and terrorist attacks, while the instruments related to procedural law and international cooperation mentioned in the Council of Europe Convention on Cybercrime can also be applied with regard to traditional offences such as terrorism. These instruments are still applicable till date.

b. Global Protocol on Cybersecurity and Cybercrime

Article 1-5 of the Global Protocol on Cybersecurity and Cybercrime relate to cybercrime and recommend the implementation of substantive criminal law provisions, procedural law

[87]Abraham D. S, (2000) *Toward an International Convention on Cyber Security, Hoover Press* available at http://media.hoover.org/documents/0817999825_221.pdf. accessed on 13/08/2018 10:45am

[88]Goodman B. (2002), The Emerging Consensus on Criminal Conduct in Cyberspace, *UCLA Journal of Law and Technology*, 6(1) p. 70, also available at http://media.hoover.org/documents/0817999825249.pdfwww.Lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; accessed on 23/08/2019 10:50pm

[89] Council of Europe Convention on Cybercrime (CETS No. 185), see http://conventions.coe.int. accessed on 15/08/2019 12:30pm

provisions, measures against terrorist misuse of the Internet, measures for global cooperation and exchange of information and measures on privacy and human rights.[90] The model legislation provided in appendix to the protocol is to a large degree (Articles 1-25) exactly based on the wording of the provisions provided by the Council of Europe Convention on Cybercrime.

3.5 Sub-Regional/Multilateral Responses to Cybersecurity Threats

3.5.1 East African Community

East African Community (EAC) member states have committed to developing a strong and effective cyber-security framework to protect the bloc against cyber threats. Member states have agreed to develop and promote a strong culture of cyber-security that recognises and effectively responds to the global threats and challenges associated with the internet, interconnected mobile networks and related technologies. This includes exchanging cyber security best practices and maintaining an open dialogue on the full range of challenges and threats for their effective utilisation and collaboration. The three-day workshop also attended by security personnel from the region, pledged to build on the work of the EAC Cyber Laws Reform Program, and in particular, the EAC Framework for Cyber laws.

The Cyber laws were adopted in May 2010, in which Partner States committed to enact comprehensive cyber-security legislation, including cybercrime legislation consistent with the Council of Europe Convention on Cybercrime (2001). Other measures to combat cyber threats include strengthening capacity to investigate and prosecute cybercrimes, joining and participating in the 24/7 Cybercrime Network and creating national Computer Emergency Readiness Teams (CERTs). The move is in line with Articles 98 and 99 of the Treaty for

[90]Schjolberg G. (2009), *A Global Protocol on Cybersecurity and Cybercrime*, available at www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf. retrieved 12/07/2019 10:30pm

the Establishment of the East African Community (EAC) where Partner States undertake to cooperate in the establishment and operation of communications infrastructure and the development and deployment of ICT applications and services, and building on the work of the EAC Task Force on Cyber laws. Cyber threats include internet and mobile frauds, cyber-based terrorism, computer intrusions, and online sexual exploitation.

The various East African countries have scaled up efforts to combat cybercrimes through a multi-stakeholder approach involving the government, industry and civil society organizations. A cybersecurity management task force chaired by Kenya has been coordinating activities aimed at rooting out cybercrimes in the five East African Community member countries. This taskforce deals with cybersecurity at legal, policy and regulatory levels. As countries concerned seek to involve the International Telecommunications Union's (ITU) help. The East African Communications Organisations (EACO) Congress, an umbrella body of all five regulators, will pursue ITU support for the establishment of the national CERTs.[9192]The five regulators will also establish a collaborative framework for the national CERTs at regional and international levels. EACO will work to establish and harmonize internet security policies and internet laws in the East African region. EACO has also adopted a proposal for telecommunications operators to form and run sectoral CERTS and nominate representatives to sit on national CERTs.

The five member states are each at different stages of developing their Internet laws, but the laws will be uniform across the board, with just a few in-country peculiarities sticking out.

[91]Henry O. Q, Alexander M. (2012),Fighting Cybercrime in Africa, *Scientific & Academic Publishing* p-ISSN: 2163-1484, e-ISSN: 2163-149, 22(6): 98-100 available at www. hallafrica.com. 2012. Accessed on 22/08/2016 10:20am

[92] James G. (2012.), East Africa region moves to curb cybercrime, *Buddecomm Africa research*. Pdf retrieved 23/08/2016 10:45am from See www. hallafrica.com.

3.5.2 Economic Community of West African States (ECOWAS)

One of the efforts of the ECOWAS is the first West African Cyber Crime Summit convened on 30th November, 2011 to 2nd December, 2011 in the Nigeria capital, Abuja. The Summit was organized by the Economic and Financial Crime Commission (EFCC) in collaboration with United Nation on Drugs and Crime (UNODC), the Economic Community of West African States (ECOWAS) and Microsoft. The summit focused on "The Fight against Cybercrime: Towards Innovative and Sustainable Economic Development". Participants from all over the world considered local and international cybercrime strategies and policies with a view to strengthening international cooperation and developing a regional road map that tackles cybercrime and fosters economic growth.[93]Over 450 people were in attendance from across the world including Togo, Guinea, Guinea Bissau, Gambia, Ghana, Senegal, Ivory Coast, Niger, Austria, UK, France, USA, Turkey, South Africa, UAE, Tunisia and Nigeria. Various international and regional organizations were present, including United Nation on Drugs and Crime (UNODC), Council of Europe (CoE), INTERPOL, US Federal Bureau of Investigation, US Federal Trade Commission, US Department of Homeland Security, Economic Community of West African States (ECOWAS), European Union and FRANCOPOL. The summit focused on how to: position the fight against cybercrime as a national priority to help the economic development in the region; provide a platform to develop capacity building with scalable and sustainable resources; strengthen trust by developing partnerships among various stakeholders at the national and international level; government, civil society, academics, industry and international organizations; showcase best practices and case studies of

[93]EccuniU (2011), *West Africa to Fight Cybercrime - Online Computer Training Can Create IT Security Awareness*, retrieved from www.EzineArticles.com.2011. Pdf on 23/08/2016 2:00pm

partner organization in combating cybercrime.[94] One form of cybercrime that has become especially associated with the region is the Advance Fee Fraud, collectively known as "Nigeria" or "419" scams. Through schemes such as fake lotteries, bogus inheritances, romantic relationships, investment opportunities or - infamously - requests for assistance from officials, scammers promise an elusive fortune in exchange for advanced payments.

One of the major achievements of ECOWAS in the regional fight against cybercrime is the production of the Cybercrime directive: [95]The objective of this Directive is to adapt the substantive penal law and the criminal procedure of ECOWAS Member States to the cybercrime phenomenon. The directive is applicable to all cybercrime-related offences within the ECOWAS sub-region. The directive makes provision for, fraudulent access to computer systems, fraudulently remaining in a computer system, interfering with the operation of a computer system, fraudulent input of data in a computer system, fraudulent interception of computer data, Fraudulent interception of computer data, Fraudulent modification of computer data, fraudulent production of computer data, fraudulent production of computer data, fraudulently obtaining any benefit whatsoever, fraudulent manipulation of personal data, obtaining equipment to commit an offence, production of child pornography, import or export of child pornography, possession of child pornography, facilitation of access of minors to child pornography, Possession of racist or xenophobic written documents, threat through a computer system[96]

[94] *ibid*
[95] Article 1, Definitions, Objectives and scope of the ECOWAS, cybercrime Directive
[96] Articles, 2,3,4,5,6,7,8,9,10,11,12,13,14,15, 16,17, 18,19, ECOWAS, Cybercrime Directive

3.6 Response of Selected Nations to Cyber Security Challenges

3.6.1 The United State

In the US, the Computer Fraud and Abuse Act is the key legislation. It prohibits unauthorized access or damage of "protected computers" as defined in 18 U.S.C.§ (e)(2). Although various other measures have been proposed, such as the Cybersecurity Act of 2010, the International Cybercrime Reporting and Cooperation Act[97]and Protecting Cyberspace as a National Asset Act of 2010.[98] There is the Executive Order13636 "Improving Critical Infrastructure Cybersecurity" which was signed in February 12, 2013.

The Department of Homeland Security has a dedicated division responsible for the response system, risk management program and requirements for cybersecurity in the United States called the National Cyber Security Division.[99] The division is home to US-CERT operations and the National Cyber Alert System. The National Cybersecurity and Communications Integration Center brings together government organizations responsible for protecting computer networks and networked infrastructure.[100]

One of the priorities of the Federal Bureau of Investigation (FBI) is to: "Protect the United States against cyber-based attacks and high-technology crimes",[101] and they, along with the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA) are part of the multi-agency task force, The Internet Crime Complaint Center, also known

[97] Text of H.R.4962 as Introduced in House: International Cybercrime Reporting and Cooperation Act – U.S. Congress. OpenCongress. Retrieved from www.waccs.net.2011 2013-09-25.
[98] Archived January 20, 2012, at the Wayback Machine. Retrieved from www.waccs.net.2011on 21/08/2016
[99] National Cyber Security Division. U.S. Department of Homeland Security. Retrieved from www.waccs.net.2011June 14, 2017; ^ Jump up to: a b "FAQ: Cyber Security R&D Center". U.S. Department of Homeland Security S&T Directorate. Retrieved August 24, 2017. 2:20pm
[100] Federal Bureau of Investigation – Priorities. Federal Bureau of Investigation. Retrieved from www.waccs.net.2011 on 23/08/201
[101] Internet Crime Complaint Center available at www.waccs.net.201122/08/2016 3:40pm

as IC3.[102]In addition to its own specific duties, the FBI participates alongside non-profit organizations such as InfraGard.[103]

The criminal division of the United States Department of Justice operates a section called the Computer Crime and Intellectual Property Section(CCIPS). The CCIPS is in charge of investigating computer crime and intellectual property crime and is specialized in the search and seizure of digital evidence in computers and networks.[104]

The United States Cyber Command, also known as USCYBERCOM, is tasked with the defense of specified Department of Defense information networks and "ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."[105] It has no role in the protection of civilian networks. The U.S. Federal Communications Commission's role in cybersecurity is to strengthen the protection of critical communications infrastructure, to assist in maintaining the reliability of networks during disasters, to aid in swift recovery after, and to ensure that first responders have access to effective communications services.

The Food and Drug Administration has issued guidance for medical devices[106]and the National Highway Traffic Safety Administration[107]is concerned with automotive cybersecurity. After being criticized by the Government Accountability Office,[108] and following successful attacks on airports and claimed attacks on airplanes, the Federal Aviation Administration has devoted funding to securing systems on board the planes of

[102]Infragard, Official Site. Infragard. Retrieved from www.waccs.net.201129 August 2016. 2:15pm
[103] Robert S. M (2011), III – Infra Gard Interview at the 2005 InfraGard Conference". Infragard (Official Site) --Media Room. Retrieved www.waccs.net.2011from August 29, 2016. 9:40am
[104] United States Ministry of Justice Official Site seewww.waccs.net.2011Accessed 12/5/2016 8:40am
[105] U.S. Department of Defense, Cyber Command Fact Sheet. stratcom.mil. May 21, 2010. From www.waccs.net.2011 Accessed 20/6/2016 12:12pmwww.waccs.net.2011
[106]Cybertelecom Federal Internet Law & Policy An Educational Project: *FCC Cybersecurity*. FCC. From www.waccs.net.2011 Accessed 20/07/2016 10:12am
[107]Cybersecurity for Medical Devices and Hospital Networks: *FDA Safety Communication*. Retrieved from www.waccs.net.201123/8/2016, 10:00am
[108]Automotive Cybersecurity-National Highway Traffic Safety Administration (NHTSA)". Retrieved from www.waccs.net.2 01123/7/2016. 10:40am

private manufacturers, and the Aircraft Communications Addressing and Reporting System. Concerns have also been raised about the future Next Generation Air Transportation System.[109]

The Computer emergency readiness team is another entity that fights computer crimes in US. The Computer emergency response team, is a name given to expert groups that handle computer security incidents. In the US, two distinct organizations exist, although they do work closely together; US-CERT; part of the National Cyber Security Division of the United States Department of Homeland Security, and CERT/CC; created by the Defense Advanced Research Projects Agency (DARPA) and run by the Software Engineering Institute (SEI).

3.6.2 Russia

Russia is one of the countries most bedeviled by cyber insecurity. This has made the country to adopt strict cyber security measures to secure its cyber space. It ranks second only to the US in global cybersecurity measures. Russia runs a program "Digital Economy of the Russian Federation", which was approved on July 28, 2017. According to Russia, the main challenges that impede the development of the digital economy are the growth of cybercrime domestically and internationally, the increased capabilities of external actors, and the lack of qualified ITC security experts. The program therefore suggests that both system and government operators should take certain basic, compulsory measures: 1) Increase the security of critical information infrastructure and the stability of its functioning; 2) Develop mechanisms for detecting and preventing cyber threats and eliminating their consequences; 3) Increase the protection of citizens and territories against an emergency caused by information technology hacks on critical infrastructure; and 4)

[109] ibid

Improve crime prevention pertaining to ITC and counteract any such violations (via Russia's Doctrine of Information Security, 2016).[110]

The Central Bank of Russia organized a Financial Sector Computer Emergency Response Team (FinCERT) with the main tasks of analyzing data on cyberattacks, provide recommendations about securing money transfers, and coordinate information exchange between law enforcement and financial institutions. In 2018, FinCERT created an automated incident processing system (ASOI) to simplify the process of information exchange as well as to increase the efficiency and level of network security. In 2019 FinCERT), it is expected

put into operation its "Antifraud System," which is intended to track unauthorized money transfers. Today, FinCERT unites 718 different organizations, including 517 banks.

Cybercrime falls under Chapter 28 of the Russian Criminal Code (Articles 272-274.1). Federal Law No. 111 (April 2018) established criminal liability for fraud using electronic payment methods (credit/debit cards) as well as other "computer frauds" (Articles 159.3 and 159.6 of the Criminal Code, respectively).

In September 2018, the National Coordination Center (NCC) was established under the control of the Federal Security Service (FSS) to deal with computer incidents and protect national information resources. FSS is the primary body responsible for detecting and preventing cyber attacks. Under the FSS/NCC, the GosSOPKA[111] program is meant to connect companies to detection systems that are geared to prevent and eliminate computer attacks. In 2018, GosSOPKA identified over 4.3 billion cyberattacks on Russian critical information infrastructure (CII), of which more than 17,000 were labeled as serious dangers.

[110]Alexander S. (2019)*Russian ITC Security Policy and Cybercrime pdf* retrieved from http://www.ponarseurasia.org/memo/russian-itc-security-policy-and-cybercrime on *06/08/2019 6:26pm*

[111]The acronym GosSOPKA (*ГосСОПКА*) stands for "Preventing and Eliminating the Consequences of Computer Attacks on Russia's Information Resources."

The laws that aim to establish the organizational and legal framework for securing CII include Federal Law No. 187 (July 2017). This law, which entered into force on January 1, 2018, defines a computer attack as a targeted threat or the actual impact of software or hardware on a telecommunication network with the purpose of violating or ending its functionality. Federal Law No. 194 (also July 2017) introduced criminal liability on those that cause harm to CII (Article 274.1 of the Criminal Code).

Under the law, industries and entities themselves are obliged to inform the authorities promptly about computer incidents, render assistance to FSS or FinCERT officials, and install applications that can detect, prevent, and eliminate cyberattacks. The specific CII security applications should be able to prevent unauthorized access to information, recover a facility's critical information (ensure that there are backups), and have continuous interaction with the NCC. For its part, the NCC is supposed to perform information security monitoring, forecast cyber threats, ensure cooperation between telecom operators and information resource owners, and pinpoint the cause of cyber incidents.[112]In 2018, NCC specialists stopped more than 20,000 cyberattacks at the source and analyzed over 100 samples of malware.

In May 2019, President Vladimir Putin signed the "Internet isolation bill," which is meant to provide for the stable operations of the *RuNet* in case it is disconnected from the World Wide Web. The new measure, which is supposed to go into effect on November 1, 2019, requires Internet providers to install equipment to route Russian web traffic through domestic servers. Although it may serve to protect digital assets from criminal elements, it might also curtail Russians' access to the international information space and allow average citizens to be tracked and identified online.

[112]Rauno K., Erkki K.(2013) Proceedings of the 12th European Conference on Information Warfare and Security: ECIW 2013 available at securitylab.ru news accessed *06/08/2019 6:40pm*

CII entities are the information systems and telecommunication networks of the government and government-linked agencies. They are a top focus to safeguard for high level policymakers. CIIs constitute the automated technical process management systems (ATPMS) that are active in the defense, healthcare, science, communications, transport, credit/financial, energy, nuclear, space/rocket, metallurgical, chemical, fuel, and mining industries. About 10,000 fields or subfields are listed as linked to Russian CII. According to the law, unauthorized access to protected data stored at a CII is punishable by imprisonment for two to six years with a fine of 500,000 to 1 million rubles (Article 274.1 of the Criminal Code).

Russia also involved international dimension to its cybersecurity policies. In 2017, the Russian Foreign Ministry prepared and offered new conventions to the UN General Assembly on countering digital crime. In December 2018, the Assembly adopted two Russian-proposed resolutions (both supported by India, a major ITC provider) under the titles: "Developments in the field of information and telecommunications in the context of international security" and "Countering the use of information and communications technologies for criminal purposes." The resolutions aim to safeguard a state's so-called privileged data while promoting global consensus and working out concrete and practical approaches to countering cybercrime. The Russian proposals helped open a new chapter in the global discussion and supervision of ITC security.

3.6.3 Canada

On October 3, 2010, Public Safety Canada unveiled Canada's Cyber Security Strategy.[113][114]The aim of the strategy is to strengthen Canada's "cyber systems and critical

[113]FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks. retrieved from https://www.nelsonmullins.com/documentdepot/fda_cybersecurity_docs.pdf on 25/7/ 2018. 10:40am

infrastructure sectors, support economic growth and protect Canadians as they connect to each other and to the world."[115]Three main pillars define the strategy: securing government systems, partnering to secure vital cyber systems outside the federal government, and helping Canadians to be secure online.[116]

The strategy involves multiple departments and agencies across the Government of Canada.[117] The Cyber Incident Management Framework for Canada outlines these responsibilities, and provides a plan for coordinated response between government and other partners in the event of a cyber-incident.[118]The Action Plan 2010–2015 for Canada's Cyber

Security Strategy outlines the ongoing implementation of the strategy.[119] Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) is responsible for mitigating and responding to threats to Canada's critical infrastructure and cyber systems. The CCIRC provides support to mitigate cyber threats, technical support to respond and recover from targeted cyber-attacks, and provides online tools for members of Canada's critical infrastructure sectors.[120]The CCIRC posts regular cyber security bulletins on the Public Safety Canada website.[121] The CCIRC also operates an online reporting tool where individuals and organizations can report a cyber-incident.[122] Canada's Cyber Security Strategy is part of a larger, integrated approach to critical infrastructure protection, and

[114]Automotive Cybersecurity - National Highway Traffic Safety Administration (NHTSA)". Retrieved from www.waccs.net.201123/5/2018. 10:12am
[115] "U.S. GAO - Air Traffic Control: FAA Needs a More Comprehensive Approach to Address Cybersecurity as Agency Transitions to NextGen". Retrieved from www.waccs.net.201123/6/2016. 12:00pm
[116]*Ibid*
[117] Aliya S. (2016). FAA Working on New Guidelines for Hack-Proof Planes. Nextgov. Retrieved from www.waccs.net.2011 25/7/2018. 10:50am
[118]Cyber Incident Management Framework for Canada. Public Safety Canada. Government of Canada. Retrieved from www.waccs.net.201110/8/2018.
[119]Action Plan 2010–2015 for Canada's Cyber Security Strategy. Public Safety Canada. Government of Canada. Retrieved from www.waccs.net.2011 20/8/2017. 12:10pm
[120]Canadian Cyber Incident Response Centre. Public Safety Canada:Fundamentals of Cyber Security for Canada's CI Community (2016) (1st Edition) Retrieved from www.waccs.net.2011 1/6/ 2016. 12:10pm
[121]*Ibid*
[122]*Ibid*

functions as a counterpart document to the National Strategy and Action Plan for Critical Infrastructure.[123]

Public Safety Canada also partnered with STOP.THINK.CONNECT, a coalition of non-profit, private sector, and government organizations dedicated to informing the general public on how to protect themselves online.[124] Subsequently, the Government of Canada launched the Cyber Security Cooperation Program.[125] The program is a $1.5 million five-year initiative aimed at improving Canada's cyber systems through grants and contributions to projects in support of this objective.[126][127]Public Safety Canada administers and routinely updates the Get CyberSafe portal for Canadian citizens, and carries out Cyber Security Awareness Month during October.[128]

3.6.3 China

China's network security and information technology leadership team was established on February 27, 2014. The leadership team is tasked with national security and long-term development and co-ordination of major issues related to network security and information technology. Economic, political, cultural, social and military fields as related to network security and information technology strategy, planning and major macroeconomic policy are being researched. The promotion of National network security and information technology law is constantly under study for enhanced national security capabilities.

[123]abc "Action Plan 2010–2015 for Canada's Cyber Security Strategy". Public Safety Canada. Government of Canada. Retrieved from www.waccs.net.201 13/7/2016. 12:40pm
[124]Government of Canada Launches Cyber Security Awareness Month with New Public Awareness Partnership". Market Wired. Government of Canada. 27 September 2012. Retrieved from www.waccs.net.2011 23/8/2016. 8:30pm
[125]Cyber Security Cooperation Program. Public Safety Canada. Retrieved from www.waccs.net.20111/08/ 2018. 8:42pm
[126]ibid
[127]Cory P. (2016) Canadian Cyber Security: Incidents and Action, Society of Internet Professionals Retrieved from http://www.sipgroup.org/canadian-cyber-security-incidents-and-action/ 23/8/2016. 2:00pm
[128] Tier3 — Cyber Security Services Pakistan from https://tier3.pk/ accessed 10/10/2016 7:40pm

3.6.4 United Kingdom

The United Kingdom (UK) is fifth inglobal leading cyber security rankings. Several measures have been put in place by the Government of the UK to protect the cyberspace. The Office of Cybersecurity was formed in 2009 and became the Office of Cybersecurity and Information Assurance (OCSIA) in 2010. OCSIA is located in the Cabinet Office and coordinates cybersecurity programmes, including location of the National Cybersecurity Programme funding. The Cybersecurity Operations Centre (CSOC) was formed in 2009. CSOC is housed with Government Communications Headquarters (GCHQ), and is responsible for providing analysis and overarching situational awareness of cyber threats.

The Centre for the Protection of National Infrastructure (CPNI) provides guidance to national infrastructure organisations and businesses on protective security measures, including cyber. Communications-Electronic Security Group (CESG)is the National Technical Authority for Information Assurance and is situated within GCHQ. CESG provides information security advice and a variety of information assurance services to government, defence and key infrastructure clients. Computer emergency response teams (CERTs) exist in a number of public and private sector organisations. GovCERTUK is responsible for all government networks, while CSIRTUK, CPNI's CERT, responds to reported incidents concerning private sector networks in the critical national infrastructure. [129]

3.6.5 India

In India some provisions for cybersecurity have been incorporated into rules framed under the Information Technology Act 2000. The National Cybersecurity Policy 2013 is a policy

[129] Cyber Security in the UK, Postnote No 389, September 2011. Retrieved from www.waccs.net.2011 Accessed 11/8/2019 10:00am

framework by Department of Electronics and Information Technology (DeitY) which aims to protect the public and private infrastructure from cyber-attacks, and safeguard information, such as personal information (of web users), financial and banking information and sovereign data. The Indian Companies Act 2013 has also introduced cyber law and cybersecurity obligations on the part of Indian directors.

3.6.8 France

The strategic stances taken in recent years at the highest political level have enshrined cyber security's place as a priority of the government's action. France conducted a profound overhaul of its defence and national security policy in the 2008 and 2013. White papers and new priorities have been defined and validated by the President of the French Republic. These include cyber-attack prevention and response, which have been identified as a major priority in the organization of national security.

The French Network and Information Security Agency (ANSSI, Agencenationale de sécurité des systèmesd' information) was created in July 2009 to address the increasing challenge of cyber-attacks, in line with the recommendations of the White Paper on Defence and National Security. It is an inter-ministerial agency attached to the Prime Minister's office. ANSSI's importance was raised in early 2011 when the Agency became the national authority for information systems defence. Following the creation of the Agency, France published a national Strategy for the defence and security of information systems in 2011. The 2013 White Paper confirmed the cyber threat and specifically identified the threat of sabotage against critical infrastructure.

One of the major focuses of the national cybersecurity strategy adopted in 2011 is the development of international cooperation: in addition to the establishment of bilateral relationships in the area of cybersecurity. As part of the Ministry of Defence's efforts to

strengthen its cyber defence capacities, a position of General Officer responsible for cyber defence was created in 2011 to coordinate the Ministry's action in this area and provide a primary interface in the event of a cyber-crisis. In February 2014, a Cyber Defence Pact was produced to lay down the Ministry of Defence's ambitions through to 2019.

For its part, the Ministry of the Interior (Police and Gendarmerie) is responsible for fighting cybercrime. A position of Prefect responsible for the fight against cyber threats was created in 2014. The Ministry of Foreign Affairs and International Development ensures the coherence of France's positions internationally as regards cybersecurity. France contributes actively to the design of cybersecurity policies within international organizations. In this respect, we are particularly attentive to the work underway within North Atlantic Treaty Organisation (NATO) and the European Union on cybersecurity, as well as at the UN and the Organization for Security and Co-operation in Europe (OSCE).

Like other countries, including the United States, the United Kingdom, Germany, Russia and Japan, which have created cyber issues coordinator positions within their Foreign Ministries, the French Ministry of Foreign Affairs and International Development entrusted these matters to the Deputy Secretary-General in 2011, later creating a specific cybersecurity coordinator position in October 2014.

In 2013, a new White Paper was published in response to the assessment that cyber-attacks against the network and information systems of numerous French businesses and public sector enterprises were increasing in number and sophistication. This marked a turning point: no longer would the State merely provide for its own cybersecurity requirements; rather, from now on, it would also provide for those of operators of vital importance (a notion defined by law as "An operator whose unavailability could strongly threaten the economic or military potential, the security or the resilience of the Nation").

This stepping up of cybersecurity was translated in the law, which stated as a result that the most critical networks and information systems of these operators of vital importance would have to: comply with the security standards defined by ANSSI in liaison with the operators; have strong detection mechanisms in place, operated by ANSSI or buy trusted service providers; and report major incidents to ANSSI. Finally, the law empowered ANSSI to conduct or request audits on these systems to verify security levels and, in the event of a major crisis, to request implementation of the necessary measures as defined by the government.

The Military Programming Law (Law No. 2013-1168) adopted on 19 December 2013 followed the guidelines set by the 2013 White Paper on Defence and National Security. This legislative mechanism enabled national public and private sector operators of vital importance to better protect themselves and ANSSI – and other State bodies – to better support them in the event of a cyber-attack. Article 22 of the Law provided for the adoption of measures to step-up the security of operators of vital importance and granted new prerogatives to the Prime Minister.[130]

The last decade has seen significant developments in the promulgation of international and regional instruments aimed at countering cybercrime. These include binding and nonbinding instruments. The genesis, legal status, geographic scope, substantive focus, and mechanisms of such instruments are the focus of the entire chapter of this work.

This section of the research highlighted various efforts by international bodies, organisations and nations in response to the threat to the cyberspace and the information regime. International/global responses to cyber threats by various international organisations; resolutions conventions and protocols by the UN, ITU, regional cyber threats

[130]The French National Digital Security Strategy 2015 retrieved from http://www.ssi.gouv.fr/en/cybersecurity-in-france/ accessed 20/06/2016 12:40pm

responses like that of the council of Europe, European Union, OEDC, the commonwealth, the African Union, the Pacific, Arab League and Gulf cooperation Council, Organization of American States, the Caribbean, and sub-regional agreements have been discussed. Africa's collective and individual efforts towards cybersecurity like that of the East African Community, ECOWAS, and selected National responses have also been discussed. These efforts have all been analysed for the purposes giving insight into the various legal, institutional, policy measures put in place by various international, regional, sub regional bodies and individual nations aimed at ensuring cybersecurity.

This chapter of the research indicates that substantial efforts have been made globally to protect to ensure cybersecurity and protect the information technology regime.

CHAPTER FOUR:

ANALYSIS OF LEGAL AND POLICY RESPONSES TO INFORMATION TECHNOLOGY AND CYBERSECURITY CHALLENGES IN NIGERIA

4.1 Introduction

It is incontestable that the Cyberspace has ushered in new opportunities; however it has also increasingly become toxic, especially in Nigeria. Back in 2001, Nigeria was reported by the American National Fraud Information Centre as having the fastest growing online scam. Subsequently, Nigeria was ranked the 3rd most active country for cybercrime activity globally. With the phenomenal growth in telecommunications, cybercrime is becoming even more sophisticated in the country. Mobile technology is making the menace very difficult to control. These new ways of communicating and transacting business have largely rendered our criminal laws obsolete. Even anti-virus software, encryptions, firewalls, login passwords, and others are not 100% protective.[1]

Cyberspace is today one of the great legal frontiers. From 2000 to 2008, the Internet has expanded at an average rate of 305 % on a global level, and currently an estimated 146 billion people are "on the Net."[2]. Live statistic on October 3, 2015, had it that Nigeria has over 80million Internet users out of world average of over 3 billon users.[3]

It is as a result of this that the Nigerian government, has been in the forefront of ensuring all-inclusive legislative discourse in ensuring cybersecurity. In continuation of measures towards safeguarding the nation's presence in cyberspace the ONSA in partnership with the Ministry of Communications Technology, Federal Ministry of Justice, Central Bank of

[1]SRM: Cyber Incident Response: Perspectives From The Risk Ecosystem http://nigerianlawtoday.com/2015/08/cleaning-up-nigerias-cyberspace-new-cybercrime-act-to-the-rescue.html, accessed on 10/09/2016 10:30am

[2] See World Internet Usage and Population Statistics, http://www.internetworldstats.com/stats.htm (June, 2008

[3]U. M. Mbanaso, G. A. Chukwudebe& E. E. Atimati (2015) A Critical Assessment of Nigeria's Presence on the Cyberspace, Proceedings of the International Conference on Cyberspace Governance: the imperative for National & Economic Security, held on 4th -7th November, 2015 at Shehu Musa Ya'adua Centre, Abuja. P. 3

Nigeria, Economic and Financial Crimes Commission, Nigerian Communications Commission, National Information Technology Development Agency, Nigerian Communication Satellite and Galaxy Backbone has come up with several initiatives to curb the menace of cyber-insecurity.[4]

It is therefore necessary to assess how Nigeria has fared in the current world of cyber insecurity; what has Nigeria done, and is still doing to ensure cybersecurity and secure the cyberspace? This chapter examines the cybersecurity readiness of Nigeria compared to the global efforts in this regards. This chapter considers the various efforts made by Nigeria in securing the cyberspace in whatever guise or ramification; ranging from legal, policy and institutional measures.

4.2 Legislative Frame Work on Cyberspace in Nigeria

4.2.1 The Nigeria Criminal Code Act 2004[5]

The Criminal Code Act criminalizes any type of stealing of funds in whatever form. Although cybercrime is not mentioned in the Act, it is a type of stealing punishable under the criminal code. The most renowned provision of the Act is Chapter 38, which deals with "obtaining Property by false pretences-Cheating." The specific provisions relating to cybercrime is section 419.

Section 419 provides:

> "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."[6]

[4] I. Frank & E. Odunayo (2013) Approach to Cybersecurity Issues in Nigeria: Challenges and Solution, International Journal of Cognitive in Science, Engineering and Education, Vol.1 No.1 Pp. 1-11 at p.2

[5] Cap C39 Laws of the Federal Republic of Nigeria 2004

[6] (Part 6, chapters 38, Laws of the Federation of Nigeria Act, 2004)

The criminal code also provides for online child pornography, though the Code does not specifically mention child pornography it however criminalises obscene publication. Section 233D (1) of the Act provides:

> "subject to the provisions of this chapter, any person who, whether for gain or not, distributes or projects any article deemed to be obscene for the purposes of this chapter, commits an offence punishable on conviction by a fine not exceeding four hundred naira or by imprisonment for a term not exceeding three years or by both."

Besides criminalizing false pretences and obscene publications, which currently can be linked to criminal activities in the cyberspace; the criminal code is not primarily a cyber-related legislation. It was enacted long before the rise of cybercrimes. In relation to cyber security, this piece of legislation can be considered obsolete and scanty and cannot be relied on to fight the menace of cyber insecurity. Its inclusion in this research work is to showcase how indirectly we have laid a foundation for cybercrimes legislations even without realizing it.

4.2.2 Wireless Telegraphy Act2004.

The Wireless Telegraphy Act (WTA) was initially enacted in 1961. Having preceded all other extant laws in the sector, the WTA nevertheless continues to provide clarity in relation to the nature of the regulatory management of communications in Nigeria. Essentially, the Act seeks to regulate the licensing, location and operation of wireless telegraphy services in Nigeria. Under the Act, it is an offence for a person to establish or use any station for wireless telegraphy, or install or use apparatus for wireless telegraphy except in accordance with a licence issued by the Commission.[7] In this regard, the "Commission" is defined to mean the Nigerian Communications Commission (with regard

[7]Ss 4-6 of *Nigerian Communications Act* of 2003 (NCA)

to telecommunications matters) and the National Broadcasting Commission (with regard to broadcasting matters).[8]

Though the Act makes provisions to cover regulations as to wireless telegraphy; misleading messages and interception and disclosure of messages among others; it has not comprehensively provided and delineated cyber offences and clearly specified penalties for such offences, rather the Act is a regulatory instrument for wireless telegraphy.

4.2.3 The National Broadcasting Commission Act 2004[9]

The Act was first promulgated as a Decree on 24 August 1992. However, the Decree and its amendments have been adopted as an Act of the National Assembly. The National Broadcasting Commission Act regulates radio broadcasting activities in Nigeria, as well as the licensing of Cable, Direct-To-Home (DTH) and all terrestrial radio and television services. It aims to implement the National Mass Communication Policy of the Federal Republic of Nigeria and also sets standards with regards to the contents and quality of materials being broadcast over the country's radio waves. Though a critical component in convergence, neither the law nor the institution appear interested in regulatory convergence[10] in the manner that technology has made it possible for broadcasting, internet and phone calls to occur through the use of one piece of equipment, such as a computer or a mobile phone.

Strictly speaking, the Act is not primarily a cyber-security legislation, but simply regulatory instrument of the broadcasting industry. The connection between the Act and cyber or computer offences is by operation rather than substance. In substance the Act

[8]S 3 of the NCA.
[9]See the *National Broadcasting Commission Act* 38 of 1992 (amended by Act 55 of 1999) now CAP N11 Laws of the Federation 2004.
[10]Merging the National Broadcasting Commission (NBC), Nigerian Communications Commission (NCC) and National Information Technology Development Agency (NITDA) as one regulatory entity for the Information and Communications Technology (ICT) sector.

provides for regulation of the broadcasting industry as an aspect of the information technology component of Nigeria, as a result, becoming cyber related legislation for the purposes of its functions and operation, but not specific a comprehensive legislation on cyber related offences.

4.2.4 The National Film and Video Censors Board Act 2004[11]

The National Film Video Censors Board Act was enacted in 1993. The Act established the National Film Video Censors Board as a regulatory body to regulate the films and video industry in Nigeria. The Board is empowered by law to censor, approve and classify all films and videos whether imported or produced locally.[12] It is also the duty of the Board to register all films and video outlets across the country and to keep a register of such registered outlets.[13] Over the years, the NFVCB has operated without interfacing with either the National Broadcasting Commission or the Nigeria Communications Commission.

4.2.5 The Nigerian Communications Act 2003

The Act was enacted in 2003 to create a regulatory framework for the Nigerian communications industry.[14] The Act established the Nigerian Communications Commission (NCC) as an independent National Regulatory Authority (NRA) for the telecommunications industry in Nigeria.[15] The Act further created provisions for the licensing and operations of telecommunications service providers and other related matters.[16] Ten years after the enactment of the Act, it remains doubtful that the regulator

[11]Cap. N40 Laws of Federation Nigeria, 2004
[12]Evangelist Mrs Helen Ukpabio v National Films and Video Censors Board **(2008) LPELR-CA/A/103/06**.
[13]See generally the *National Film Video Censors Board Act* Cap N40 LFN 2004
[14]S. 1 of the NCA.
[15]S 3 of the NCA.
[16]2 of the NCA

has discovered and effectively utilised the sector-specific regulatory powers conferred on it under the legislation.

4.2.6 The Economic and Financial Crime Commission Act 2004

The Economic and Financial Crime Commission Act (as amended) provides the legal framework for the establishment of the Economic and Financial Crime Commission. Some of the major responsibilities of the Commission under the Act include: the investigation of all financial crimes, including advance fee fraud, money laundering, counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, contract scam; the coordination and enforcement of all laws against economic and financial crimes laws and enforcement functions conferred on any other person or authority; the examination and investigation of reported cases of economic and financial crimes with a view to identifying individuals, corporate bodies, or groups involved; undertaking research and similar works with a view to determining the manifestation, extent, magnitude, and effects of economic and financial crimes and advising government on appropriate intervention measures for combating same; taking charge of, supervising, controlling, coordinating all the responsibilities, functions, and activities relating to the current investigation and prosecution of all offences connected with or relating to economic and financial crimes, in consultation with the Attorney-General of the Federation; the coordination of all investigating units for existing economic and financial crimes, in Nigeria;[17]

A close perusal of the EFCC Act leaves much to be desired, as the act has not holistically provided for cybercrimes typology and mete out appropriate sanctions. The major cyber related offence mentioned by the Act is computer credit card fraud provided in section 6(b)

[17] part 2 of the of the Economic and Financial Crimes Commission Act Laws of the Federation of Nigeria, 2004,

of the EFCC Act. This is not sufficient to contemplate the Act as having made adequate provision for the fight against cyber and information technology related crimes such spamming, phishing and ATM related fraud.

4.2.7 Advance Fee Fraud and Other Related Offences Act 2006

Under the Act[18], the EFCC is charged with the responsibility for the enforcement of its provisions. The part that concerns the cyberspace is the provisions of part 2 of the Act.

Part 2 of the Act, provides for electronic telecommunications offences as follows: - (a) by placing duty on all electronic communications service remote computing service providers, to obtain subscriber's name and address, failure to comply by both the subscriber to furnish and the provider to obtain attracts liability regime and penal consequences on conviction under section 12. Section 13 of the Act makes it the duties of telecommunications and internet service providers and internet cafes operators to register with the EFCC, maintain a register of all fixed line customers or non-fixed line or Global System of Mobile Communications (GSM) and submit on demand to the commission such data and information as are necessary or expedient for giving full effect to the performance and functions of the commission. Failure to do so with intent to disguise or conceal the nature of his activities or the use of services and facilities, constitutes an offence and the liability regime on conviction is 3 years imprisonment and operational licence may be revoked or cancelled under the section.

Generally in regards to cyber or computer related threats issues, the Act only cover the regulation of internet service providers and cybercafés; it does not deal with the broad

[18] Advance Fee Fraud and Related Offences Act 2006

spectrum of computer misuse and cybercrimes[19]. The Act has also been criticised for not properly handling the problems associated with the use of electronic evidence in cybercrime prosecution[20]

4.2.8 Nigeria Deposit Insurance Corporation (NDIC) Act 2006

Sections 27-32 of the Act mandate the NDIC to carry out onsite and offsite surveillance of insured financial institutions. The prime reason for the provision is the prevention of fraud in the banking system. Owing to the potent threat of electronic/cyber fraud, the NDIC and CBN have developed the Electronic Financial Audit Sub-System (E-FASS) towards the actualisation of its mandate under sections 27-32

4.2.9 The National Information Technology Development Agency Act 2007

The Act among other things empowers the National Information Technology Development Agency to develop guidelines for electronic governance and monitor the use of electronic data inter change and other forms of electronic communication transaction as an alternative to paper-based method in government. The main object of the Act is "...to provide for the establishment of National Information Technology Development Agency (NITDA) and related matters" this is further summarized in section 6 of the Act.

Section of 6 of NITDA ACT provides six major objects of the Act; 1) Create a framework for the planning, research, development, standardization application, coordination, monitoring, evaluation and regulation of information technology practice, activities and systems in Nigeria and all matters related hereto and for that purpose, and which without detracting from the generality of the foregoing shall include providing universal access for

[19]Finextra (2005) Deutsche Bank signs global license for TT dealing system available at www.finextra.com/news/fullstory.aspx?newsitemid=14314 accessed 23/8/201910:30am

[20] Kathleen O.,Wiseman U.,Nyako A.,Tosin O.,(2016) Prosecution of Cyber Crimes in Nigeria: Matters Arising, Paper Presented at the 49th Annual Nigerian Association of Law Teachers(NALT) Conference Nasarawa State University, Keffi, 27th May.

information technology and systems penetration including rural, urban and underserved areas; 2) Provide guidelines to facilitate the establishment and maintenance of appropriate for information technology and systems application and development in Nigeria for public and private sectors urban-rural development, the economy and the government; 3) develop guidelines for electronic governance and monitor the use of electronic data inter change and other forms of electronic communication transaction as an alternative to paper-based method in government; 4) develop guidelines for the standardization and certification of information technology escrow source code and object code domiciliation application and delivery system in Nigeria; 5) render advisory services in all information technology matters to the public and private sectors create incentives to promote the use of information technology in all sphere of life in Nigeria; 6) introduce appropriate regulatory policies and incentives to encourage private sector investment in the information technology industry. Determine critical areas in information technology requiring research intervention and also advice government on ways of promoting the development of information technology in Nigeria; and 7) accelerate internet and intranet penetration in Nigeria and promote sound internet governance.[21]

This act covers a wide range of issues regarding the Nigerian cyberspace. However, the real intent of the Act is not to curb cyber related threats but to establish the National Information Technology Development Agency (NITDA), whose major function is to provide regulatory oversight on matters concerning information technology. It is therefore, strictly speaking, not a major cybersecurity regulation, but relates to the cyberspace by operation.

[21] The Long Title to the National Information Technology Development Agency Act 2007

4.2.10 Terrorism (Prevention) Act, 2011

Terrorism (Prevention) Act, 2011 empowers the Attorney General of the Federation, the

National Security Adviser or the Inspector General of Police to, for the purposes of prevention or detection of offences or the prosecution of offenders under this Act give such directions as appear to him to be necessary to any communication service provider to retain communications data[22].

The Act provides that the Attorney General of the Federation, the National Security Adviser or the Inspector General of Police may with the approval of the President, on request made by the appropriate authority of a foreign state, disclose to that authority any information in his possession or in the possession of any other government department or agency relating to, among other things; the use of communication technologies by terrorist groups if such disclosure is not prohibited by law and not prejudicial to national security.[23] Section 29 (3) of the Act, provides that a video recording made under the section shall be admissible in evidence and video recording is defined to include the recording of visual images or sound by electronic or other technological means[24].

The 2013amendment of the Act provides extra-territorial application of the Act, and strengthens terrorist financing offences[25] the Act contains 10 amendments to the principal Act. The Act amends section 1 of the principal Act by inserting a new section "1A" after the new section 1(4) of the principal Act, which empowers law enforcement agencies, to among other things, establish, maintain and secure communications, both domestic and

[22]Section 26 (1), (2) (3),
[23]Section 23 (1) (d), Terrorism prevention Act, 2011
[24] Section 29(4) Terrorism Prevention Act, 2011
[25]Explanatory Memorandum to the, Terrorism (Prevention) (Amendment) Act, 2013

international, to facilitate the rapid exchange of information concerning acts that constitute terrorism.

The Act also provides that any person arrested under reasonable suspicion of commission of an offence shall be detained by law enforcement or security officer without having access to his phone or communication gadget[26] section 29 (1) (2) (3)(4) of the Act, provides that for the purposes of prevention of terrorism, the relevant law enforcement agency, with the approval of the attorney General of the federation may, with the approval of the national security adviser, apply ex-parte to a judge for an interception of communication order, and such a judge may make an order to require a communication service provider to intercept and retain a specified communication or communications of a specified description received or transmitted or about to be received or transmitted by that communications service provider. Such law enforcement agency may be authorised by the court to enter any premises and to install in such premises, any device for the interception and retention of a communication or communications of a specified description and to remove and retain such a device for the purpose of intelligence gathering. Such order shall specify the maximum period for which a communications service provider may be required to retain communications data.

Any information contained in a communication intercepted or retained whether in Nigeria or in a foreign country shall be admissible in a proceeding for an offence under the Act, as evidence of truth.

Section 29 (3) of the Act, provides that a video recording made under the section shall be admissible in evidence. This therefore provides some departure from the provision of section 84 of the Evidence Act, 2011 concerning electronically generated evidence, which

[26]Section 28 (1) (b) and subsection (4) (b) Terrorism (Prevention) (Amendment) Act, 2013

stipulates compliance with the conditions of admissibility under the section. The section implies that one could tender and admit video recordings which are relevant to terrorism related offences to be admissible without the formality of section 84 of the evidence Act, which in some cases renders relevant evidence inadmissible on the technical grounds of non-compliance with section 84 of the Evidence Act, 2011.

The Act could be criticised on the grounds that it scantily provides for cybercrimes, only in relation to terrorism, therefore it could not be taken to be a comprehensive legislation on cybercrimes, or regulation on criminal activities in the cyberspace in Nigeria.

4.2.11 Money Laundering (prohibition) Act 2011(as amended)

This Act makes comprehensive provisions to prohibit the financing of terrorism, the laundering of the proceeds of crime, or an illegal act.It makes it compulsory for a transfer to or from a foreign country of funds or securities by a person or body corporate including a Money Service Business of a sum exceeding US$10,000 or its equivalent shall be reported to the Central Bank of Nigeria, Securities and Exchange Commission or the Commission in writing within 7 days from the date of the transaction. Such reports shall indicate the nature of the transfer, the amount, names and addresses of the sender and receiver of the funds or securities.

The Act limits the amount of money to be paid or accepted as cash payment. For an individual it is now N5 million while a body Corporate it is N10 million. Anything in the excess of that must be made through a Financial Institution,[27]

S. 3 (6) & (7) provides where there is a reasonable room to suspect that the amount involved in a transaction is a proceeds of a crime or illegal act, then the Bank shall require

[27] Section 1 (a) &(b) ibid

identification of customer regardless that the amount in the transaction is less than USD10,000 or equivalent; where it appears that the customer may not be acting on his own account, the bank shall seek from the customer, by all reasonable means as to the true identity of the principal. Where the customer is a body corporate, the bank shall take reasonable means to understand the ownership, control structure, the natural persons who truly own and control the customer. By Section 6 (1) & (2)where there is a special suspicion on any account because of the frequency which is unjustifiable, unreasonable or unusual the bank shall within 7 days after the transaction: draw up a written report containing all relevant information, with the identity of the principal and the beneficiaries where applicable; take appropriate steps to prevent the laundering of proceeds of a crime or an illegal act; send a copy of the report to the Commission whether the transaction was completed or not.

Section 6(5) (b) confers powers on the EFCC and CBN or their authorized representatives to place a stop order on any account or transaction for a time not exceeding 72 hours if it is discovered in the course of their duties that such accounts are involved in any crime. And, where it is not possible for the EFCC or the CBN to conclude their investigation within 72 hours, they must obtain an Order from the Federal High Court directing the Bank to block the funds, accounts or securities; It is an offence for the Bank to fail to report to the Commission any reasonable suspicion within 7 days as stated in section 6 (1) and (2) and is liable upon conviction to a fine of N1million for each day during which the offence continues; where funds are blocked under an Order obtained from the Federal High Court by the EFCC or other relevant Agency under section 6(7), and there is evidence of conspiracy between the Bank and the owners of the funds, the bank involved shall not be

relieved of liability under this Act and criminal proceedings for all offences arising therefore may be brought.

Under Section 10 the bank is under an obligation to report within 7days to the commission of any single transaction, lodgement or transfer of funds in excess of N5million or its equivalent for individual, or N10million or its equivalent for body corporate. A contravention of this disclosure is an offence and upon conviction attracts a fine.

Under Section 13, in order to identify and locate proceeds, properties, objects or other things related to the commission of an offence under this Act, the EFCC, CBN or other regulatory agencies may by the Order of the Federal High Court, place any bank account or any other account comparable to a bank account under surveillance; obtain access to any suspected computer system; obtain communication of any authentic instrument or private contract, together with all bank, financial and commercial records when the account, telephone line or computer system is used by any person suspected of taking part in a transaction involving the proceeds, of a financial or other crime.

The Act amends section 11 by inserting new subsections 2, 3 and 4 which prohibits the establishment and operation of, correspondence with, and patronage of a shell bank. Section 25 defines a shell Bank as "a bank that is not physically located in the country in which it is incorporated and licenced, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision[28];

The money Laundering Act is a statute enacted to check the rising incidence of crimes relating to laundering of money via banks and other financial institutions by individuals and body corporate. It is not a comprehensive regulatory framework on cyber related

[28]The only plausible means of transaction for such banks is through electronic means

offences. The provisions do not adequately cater for cyber threats in Nigeria. At best the Act is supplementary to legislations on cybercrimes and related threats.

4.2.12 The Lagos State Criminal Law 2011

Recognizing the need for protection from cyber related offences, the Lagos State enacted the Lagos state criminal law which penalizes some aspects of computer related crime. The Criminal Law prohibits unauthorized access to a program or data. It states that "[a]any person who intentionally causes a computer program to perform any function with intent to secure unauthorized access to any program or data held in any computer is guilty of a misdemeanor and is liable to imprisonment for 2 years"[29]. The law also prohibits the unauthorized modification of the contents of any computer.[30]

The good thing about this law is that the modification does not have to be harmful to be a crime under the provision. Any modification without the consent of the owner or operator of the computer, device or system would suffice for purposes of inculpation under the Act. The law also imposes severe punishment for cases where the modification impairs or otherwise damages the computer or device.[31]

Though this legislation provides for cyber related offences it is not comprehensive in its provision for cyber related offences legislation. The Act is not designed as a primary legislation for cyber offences, rather, it criminalises both conventional and cybercrimes. Its provisions are however helpful in fighting computer related offences.

[29] Section 385 the Lagos State Criminal Law 2011
[30] Section 387 ibid
[31] Section 388 ibid

4.2.13 Evidence Act 2011

The emergence of the cyberspace and the ICT regime has established its impact on the Evidence Act. This has resulted in improved provisions of the new Evidence Act, 2011.[32] The Act recognises electronic communication and admissibility of electronically generated evidence.

Certain provisions under the Act have been modified to reflect the prevailing attitude of the Act to issues such as document and admissibility of electronically generated evidence. The most significant is the new definition of "document" provided in section 258-(1) to include- (a) books, maps, graphs, drawings, photographs; and also includes any matter expressed or described upon any substance by means of letters, figures or marks or by more than one of these means, intended to be used or which may be used for the purpose of recording that matter; (b) any disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some equipment) of being reproduced from it; and (c) any film, negative, tape or other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced from it; and (d) any device by means of which information is recorded, stored or retrievable including computer output. The definition is so broad that it can conveniently accommodate all known forms of storage and record of information.

However, the criticism of the new Act is also majorly founded on the unbridled broadness of what constitute document as this may constitute serious problem for practitioners in the application of the Act. This is because the definition of document accommodate information in all forms of devices, and also accommodates the device itself as a form of

[32]Ladan M.T (2015) op cit. p.8

document for instance, information stored in a flash drive can rightly be described as a document under paragraph (a) of the definition of a 'document' under paragraph 'd' of the same definition, the flash drive itself constitutes a document.

The foregoing poses a problem for practitioners in terms of application, the implication being that 'document' such as flash drives, tapes or sound track can also be classified as private and public documents under sections 102 and 103 of the evidence Act, 2011. Where such document falls within the purview of public documents, the law requires that only a Certified True Copy of same can be admissible in evidence. Section 104 provides for what a certified true copy of a document is. The question then, is "how does a public officer in custody of a flash drive or a sound track certify a copy of such a device as a certified true copy in compliance with section 104'?[33] Providing an answer to this remains a challenge.

Another outstanding contribution of the Evidence Act, to the cyber world is the provision of section 84 of the Act which provides for admissibility of statements in documents produced by computers. This provision was previously missing in the former Act. The section lays the conditions for the admissibility of an electronically generate evidence. These conditions are:

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

2. There must have been a regular supply of similar information in the ordinary course of business.

[33] Ibid.

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

4. Information contained in the document is derived or reproduced from information supplied to the computer in the ordinary course of those activities.

The foregoing conditions laid down by the Evidence Act generates inherent problems; by paragraph (a) it requires some sort of consistent use of the computer for a specific purpose as preconditions for admissibility of documents produced by such computer. This means a computer that is regularly used to store or process statement of account cannot produce a deed of assignment that will be admissible in evidence. Under paragraph (b) the information derived from a computer must not be of an isolated nature. There has to be a regular supply of similar or related information to the computer in the ordinary course of business over the period under review. This may unduly restrict the nature of evidence that may be admissible under the provision.

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

Under paragraph (d) the essential condition is that the information must be supplied to the computer in the ordinary course of the activities. This raises the question as what happens if such document is simply produced using a computer that is usually not ordinarily used in the course of its activities to produce such document, would that render such a document

inadmissible? For instance if a computer is used in its ordinary course of business to produce document in Microsoft words only within the period, but the computer was however used by somebody to produce a document in Portable Document Format (pdf), would such document be inadmissible?[34]

Though the Evidence Act is a serious improvement which enables the courts and legal practitioners to cope with activities in the cyberspace, it is not without its own shortcomings as highlighted above. To deal with the foregoing challenges, it is pertinent to harmonise and reconcile the expanded definition of document with other aspects of the Evidence Act in order to eliminate such amusing confusion. A possible solution would be to reconsider the definition of a document. The legislature in the course of trying to solve one problem may have unwittingly created another. It is important the Act is amended to create a distinction between 'devices' and 'document' as forms of evidence. Different considerations should apply to both forms in the application of the Act. For instance, while 'public documents' may require certification as a prerequisite for admissibility, some other forms of authentication should be created for 'public devices'[35] this in in view of the fact that section 104 of the Act is clearly designed for 'documents' and does not in any way envisage 'devices'

4.2.14 The Cybercrime (Prohibition, Prevention, Etc.) Act 2015

The Cybercrime Act, 2015outlines the legal and institutional frameworks needed to drive/facilitate the nation's preparedness to secure the cyberspace. It has made substantive criminal law, procedural law, as well as international cooperation provisions that meet the

[34]Ladan M.T (2015) op cit.p.8
[35]ibid

standards of the Budapest Convention and other international instruments in the fight against cybercrime and ensure cybersecurity.

The Act seeks to provide an effective, unified and comprehensive legal framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria; ensure the protection of critical national information infrastructure; enhance cyber security and the protection of computer systems and networks, electronic communications; data and computer programs, Intellectual property and privacy rights;[36]

Section 3 of the Act provides for the designation of certain computer system or networks as critical national information infrastructure as well as prescribe minimum standards, guidelines rules or procedure for the protection, general management, audit and inspection of critical information infrastructure. Section 4 provides for audit of critical information infrastructure by the office of national security adviser.

Sections 5-36 of the Act[37] cover the various offences identified as cybercrimes under the Act and their penalties, these include: offences against critical national information infrastructure, unlawful access to computer, use of cyber cafes to commit fraud, system interference, intercepting electronic messages, emails, electronic money transfers, tampering with critical infrastructure, wilful misdirection of electronic messages, unlawful interceptions, computer related forgery, computer related fraud, theft of electronic devices, unauthorized modification of computer systems; network data and system interference, forgery of electronic signature, cyber terrorism, fraudulent issuance of E-instructions, identity theft and impersonation, child pornography and related offences, cyber stalking, cybersquatting, racist and xenophobic offences, attempts, conspiracy, aiding and abetting,

[36]Section 1 of the Cyber Crimes (prohibition, prevention etc) Act, 2015
[37]Part 4 ibid

importation and fabrication of computer of E-tools, breach of confidence by service providers, manipulation of ATM/POS terminals, phishing, spamming and spreading of computer virus, electronic related fraud, dealing in card of another, purchase or sale of card of another, use of fraudulent device or attached e-mails and websites.

Section 7(1) particularly provides for the registration of cybercafés as a business concern both with the Computer Professionals Registration Council in addition to a business name registration with the Corporate Affairs Commission, and they are to maintain a register of users. This is ostensibly for the purpose of monitoring online activities in the cybercafés

Sections 37 addresses the duties of financial institution (i.e verify the identity of its customers carrying out electronic financial transactions, and apply the principle of know your customers in documentation). Section 38 provides the duties of service providers (which include records retention, protection of data, and interception of electronic communications). Under Section 38 (2) a service provider shall, at the request of the relevant authority referred to in subsection (1) of this section or any law enforcement agency – (a) preserve, hold or retain any traffic data, subscriber information, non-content information, and content data; or records retention and protection of data. (b) release any information required to be kept under subsection (1) of this section. (3) A law enforcement agency may, through its authorized officer, request for the release of any information in respect of subsection (2) (b) of this section and it shall be the duty of the service provider to comply.

Section 39 provides that where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceedings, a Judge may on the basis of information on oath; (a) order a service provider, through the application of technical means to intercept, collect, record,

permit or assist competent authorities with the collection or recording of content data and/or traffic data associated with specified communications transmitted by means of a computer system; or (b) authorize a law enforcement officer to collect or record such data through application of technical means. Section 39 provides for interception of suspicious electronic communication by service providers pursuant to court order. Section 40 mandates service providers to comply with the provisions of the Act and disclose information upon request by law enforcement agencies, and failure attracts a penalty regime of N10,000,000 and a fine of officers of such service providers.

Sections 41 to 44[38] give the office of the National Security Adviser the power of coordination and enforcement, as well as making provision for establishment of a National Computer Emergency Response Team (CERT), and National Computer forensic Laboratory. It also established the cybercrime Advisory council. S. 42 particularly provides for the establishment of Cybercrime Advisory Council. Under section 45 (1), a law enforcement officer may apply ex-parte to a Judge in chambers for the issuance of a warrant for the purpose of obtaining electronic evidence in related crime investigation. (2) The Judge may issue a warrant authorizing a law enforcement officer to- (a) enter and search any premises or place if within those premises, place or conveyance –(i) an offence under this Act is being committed; or (ii) there is evidence of the commission of an offence under this Act; or (iii) there is an urgent need to prevent the commission of an offence under this Act.

Sections 46 to 49 give the power of arrest, search, seizure and prosecution to law enforcement officers. Sections 50 to 56 give jurisdiction to the Federal High Court to try offences under the Act, and also provides for international cooperation. The issues covered

[38] Part V of the Cyber Crimes (prohibition, prevention etc) Act, 2015

include: Extradition; Mutual Assistance Requests; Expedited preservation of data, Evidence Pursuant to a Request; and Form of Requests.

Under section 55 (1) - Nigeria may be requested to expedite the preservation of electronic device or data stored in a computer system, or network, referring to crimes described under this Act or any other enactment, pursuant to the submission of a request for assistance for search, seizure and disclosure of those data. Section 55(2) (a) to (f) – spelt out the prerequisites that a request under subsection (1) of this section shall meet. 57 to 59 deal with regulations and interpretation.

The Cybercrimes Act makes extensive provisions which, if effectively implemented, would create cybersecurity and provide the much needed regulation of electronic transactions. The Act however has some loopholes among which is the fact that coverage is not given to issues relating to the adoption of cloud services including data sovereignty and ownership of data/content or liability of content authors e.g. for citizens participating in areas like journalism. Also the prosecution of denial-of-service (DoS) and computer-worm attacks which naturally pose serious challenges to most criminal law systems, as they may not involve any physical impact on computer, have also not been covered by the Act.

Another issue concerns the enforcement of the provisions of the Act. Section 7(1) particularly provides for the registration of cybercafés as a business concern both with the computer professionals registration council in addition to a business name registration with the corporate Affairs commission, and also requires cybercafés to maintain a register of users through sign-in register, and that the register shall be available to law enforcement agents whenever needed. Interestingly, the said section does not provide for sanction if the section is contravened. This brings the section in conflict with the provision of section

36(12) of the Constitution of the Federal Republic of Nigeria, 1999(as amended). The section provides:

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

It is basic that any provision of law that prescribes no punishment for violation of its provision is not a law, because it has served no useful purpose. In **Akingbola v FRN**,[39] the Appellants were tried before the Failed Banks Tribunal in Lagos pursuant to the Failed Banks (Recovery of Debts) and Financial Malpractices in Banks Decree, 1994. They were found guilty and convicted on three counts of falsely boosting the balance of A.C.B. Plc's clearing account with the Central Bank of Nigeria contrary to s. 435(2) of the Criminal Code and punishable under section 23(4) of the failed Banks Decree. The Appellants appealed the judgment on the ground that it was unconstitutional to have convicted them for conspiracy to boost and boosting an account, when such offence is unknown to Nigerian Law. Relying on the cases of **Aoko v. Fagbemi** [40] and **F.R.N v. Ifegwu**[41] the Supreme Court held that the conviction and sentences were null and void, and set aside same.

Section 37 of the Act criminalises unauthorised debit on a customer's account by financial institutions and failure to reverse such unauthorised debit within 72 hours upon written notification by the customer. In practice banks breach this provision almost all the time, how many have been prosecuted? Section 19(3) shifts the burden of proof to the bank customer "to prove that the financial institution in question could have done more to safeguard its information integrity"

[39](2014) LPELR-24258
[40][1961] ANLR 400
[41](2003) 15 NWLR (Pt.842)113

Another defect in the Act is that, it provides that one of its overriding objectives is the protection of critical information infrastructure, but no definition of what constitute critical National Information Infrastructure is given anywhere in the Act. In addition, section 4 provides for audit and inspection of critical National Information Infrastructure by the office of the National Security Adviser upon a presidential Order made under section 3. It has not however defined what "Audit" should include or exclude. Perhaps the advantage could be that, by giving powers to designate certain computer systems or network as critical National Information Infrastructure, it is an open cheque, as the list could be expanded or diminished.

The researcher is of the view that with the passage of the Electronic Transaction bill into law, and in addition to the Payment System Management Bill when finally passed into law by the National Assembly, some of the inherent challenges of the Cyber Crimes Act 2015 could be addressed.

4.3 Proposed Legislations

Beside existing legislations dealing with cyber related offences, particularly the Cyber Crimes Act, 2015, several legislations have been proposed and presented to the National Assembly for the purposes of tackling the menace of Cyber threats. These proposed legislations are outlined below:

4.3.1 Computer Security & Critical Information Infrastructure Protection Bill, 2005

This Bill was first made public in 2005. The bill is wide, extensive and covers a lot of issues related to security of computer, systems and networks, Protection of critical ICT infrastructures, investigation, and prosecution of online crimes or crimes committed in the cyberspace.

The bill covers such Offences as unlawful access to a computer, unauthorised disclosure of access code, fraudulent electronic mail messages, computer fraud, computer forgery, system interference, misuse of devices, denial of service, identity theft and impersonation, records retention and data protection, authorised interception, failure of service provider to perform certain duties, cybersquatting, cyber-terrorism, violation of intellectual property rights with the use of a computer, etc., using any computer for unlawful sexual purposes etc., Attempt, conspiracy and abetment.[42]

The bill provides for the security and protection, audit and inspection of Critical Information Infrastructure and provides punishment for offences against Critical Information Infrastructure.[43]

Interestingly, section 23 of the bill provides for a civil remedy. It provides that nothing shall preclude the institution of a civil against a person liable under this Act by any interested party. This therefore is departure from conventional penal laws that most times provide for punishment without any, or with minimal remedy for the victim, except part 9 of the Criminal Procedure Code which provides for compensation to a victim of a crime, either in part or in whole, compensation to an innocent purchaser for value of any property he has to give up as a result of the crime and compensation to an accused person tried on a vexatious charge. The Administration of Criminal Justice Act,[44] the Criminal Code Act,[45] the Criminal Procedure Act[46] and the Administration of Criminal Justice Law of Lagos, 2011[47] are other legislations with some form of compensation for the victim. This bill however, not only provide compensation, but also provides avenue for the victim to

[42]Part II, Computer Security & Critical Information Infrastructure Protection Bill, 2005
[43]Part III, Computer Security & Critical Information Infrastructure Protection Bill, 2005
[44]Section 314 Administration of Criminal Justice Act, 2015
[45] Part 9(Sections 365 – 367) 371) of the Criminal Procedure Code Cap. 30 LFN 2004
[46] Part 2(Sections 255 – 260), Criminal Procedure Act Cap 80 LFN 2004
[47] Part 20 (Sections 285 – 289), Administration of Criminal Justice Law of Lagos, 2011

institute civil suit for the purposes of seeking compensation for the wrong done. Section 24(1) of the bill vests jurisdiction for offences under the Act on the High Court of a State and the Federal High Court.

On a general plane, this Bill seeks to create legal liability and responsibility for modern global crimes carried on over a computer or computer systems forming a network, i.e. the internet. However, the causes for concern that one has for the Bill are that: first, there is no independent authority to monitor compliance with the provisions of the bill apart from the regular law enforcement agencies. It is not enough to stipulate penalties for non-compliance, there must be an appropriate machinery in place to ensure that private information is not abused in the course of data gathering for whatever purposes.

Secondly, there is no provision for award of compensation where the data rights of individuals are violated. The imposition of higher monetary penalties may do well to enrich the coffers of the government but they do not in any way compensate for losses suffered when personal data is abused or misused. Though the Bill attempts to provide for the security of data, it is not clear-cut data protection legislation. The Bill also exhibits some clear defects or lacunae among others like: no appointment of a regulatory body to ensure compliance or redress breaches; no provisions for circumstances where data can be used without the consent of the data subject regardless of whatever effect it would have had on the protection of personal information.

4.3.2 Cybersecurity and Data Protection Agency (Establishment, etc.) Bill 2008.

The Bill provides for the establishment of the Cybersecurity and Information Protection Agency[48]charged with the responsibility of securing computer systems and networks and

[48] See Section 1(1), Cyber Security and Data Protection Agency (Establishment, etc.) Bill 2008

liaison with the relevant law enforcement agency for the enforcement of cybercrimes laws, and for related matters[49]

Sections 7-23 provide for the following: offences relating to unlawful access to a computer; unauthorized disclosure of access, pass word code etc.; fraudulent electronic mail, message and spamming; computer fraud and data forgery; system interference; misuse of devices; unlawful access; impersonating and fraudulent access; standard equipment and services; failure of service provider to provide certain duties; cybersquatting; cyber terrorism; violation of intellectual property rights with the use of computer; using any computer for child sexual exploitation; attempt, conspiracy and abetment.

Section 24 provides that, the president may on the recommendation of the Agency, by order published in the Federal Gazette, designate certain computer systems, networks and information infrastructure vital to the national security of Nigeria of the economic and social wellbeing of its citizens, as constituting critical information infrastructure. Offences against critical information infrastructure are punishable under section 26 of the Bill.

The Bill appears to have made some germane additions to the content of the Cybercrimes Act, 2015. In substance the Bill duplicates so many provisions of the Cybercrimes Act and the Electronic Transactions bill. It is an unnecessary duplication of laws.

4.3.3 Electronic Fraud (Prohibition Bill), 2008

The bill seeks to prohibit all electronic frauds in the Federal Republic of Nigeria. It criminalizes unauthorized access to computer be it public or private. Section 1 of the bill prohibits electronic frauds such as, unauthorized access to a computer and/or other electronic devices or in case of authorization, exceeds authorized access to computers and

[49]Long title, Cyber Security and Data Protection Agency (Establishment, etc.) Bill 2008

or communication devices; use of counterfeit access devices; use of unauthorized access devices; possession of any device designed to manipulate credit or ATM card; causing damage to a government computer with the intent to defraud; accessing a computer and or electronic device to commit espionage; traffic in pass words for public, private and or financial institutions computer or relevant electronic devices.

Other aspects covered by the bill include; registration of cyber café to ensure monitoring of such cafes, interception of electronic messages, willful misdirection of E-messages for fraudulent purposes, fraudulent purposes, fraudulent issuance of E-money orders, sending obscene messages, manipulation of computer data, purchase of forged E-cards, falsification of E-data, validity of electronic signatures and its exceptions., diversion of E-mail for personal gains in financial institutions, E-identity theft, E-card fraud, usage of fake E-access devices, manipulation of ARM/POS terminals, computer damage and for other related matters.

This bill may not be required since we already have the Cyber Crimes Act 2015.The provisions of the bill and the Cyber Crimes Act are essentially same in substance, and would amount to unnecessary multiplication of laws to have another law with similar provisions.

4.3.4 Payments System Management Bill, 2009

The bill provides for the management, administration, operation, regulation, oversight and supervision of payments, clearing and settlement systems in Nigeria and for matters connected therewith[50].

[50] Long title, Payments System Management Bill, 2009

Section 2 of the bill provides that- (1) No person, other than the Bank, shall commence or operate a payments system except in accordance with an authorisation issued by the Bank under the provisions of this Act:

Section 6 provides for revocation of authorization-(1) If a system provider: (i) contravenes any provisions of this Act; (ii) does not comply with the regulations; (iii) fails to comply with the orders or directions issued by the Bank; or (iv) operates the payments system contrary to the conditions subject to which the authorisation was issued,

Under Section 11 the Bank shall have the right to access any information relating to the operation of any payments system and the system provider shall provide access to such information. Section 12 provides that any officer of the Bank duly authorised in writing may, for the purpose of ensuring compliance with the provisions of this Act or any regulations, enter any premises where a payments system is being operated and may inspect any equipment, including any computer system or other documents in the premises and may call upon any employee of such system provider or participant or any other person working in such premises to furnish such information or documents as may be required by such officer. Section 27 provides that the Bank, system participants and service providers must retain all records obtained by them during the course of the operation and administration of the payments, clearing and settlement systems for a minimum period of five years from the date of the conclusion of the transaction.

Section 28 provides for dishonour of electronic funds transfer for insufficiency of funds in the account it provides that where an electronic funds transfer initiated by a person from an account maintained by the person cannot be executed on the ground that the amount of money standing to the credit of that account is insufficient to carry out the transfer instruction, such person shall be deemed to have committed an offence and shall, without

prejudice to any other provisions of this Act, be punished with imprisonment for a term which may extend to two years, or with a fine which may extend to twice the amount of the electronic funds transfer, or with both Section 29[51] provides requirement for digital signature it states all electronic transactions under the payments system shall be digitally signed in a manner that may be determined by the Bank. It further provides that for the purpose of subsection (1) of this section, all system participants shall register with a public key infrastructure recognised by the Bank.

The bill makes important contributions to the current legislation on cybercrimes as it provides for issues like regulation of payment systems, dishonour of electronic funds transfers for insufficiency and requirement for digital signature. The bill however has not comprehensively provided for cyber offences in general, as it is clear that fighting cyber threats is not the primary intendment of the Bill.

4.3.5 Computer Security and Protection Bill, 2009

This bill provides for the security of computer and computer networks as well as critical information infrastructure in Nigeria. It also provides for offences and penalties relating to unlawful acts committed with the uses of computers. A prominent feature of the bill is the establishment of the Nigerian computer security and protection agency to provide legal basis and technical infrastructure for combating cybercrimes in Nigeria.

Part 5 of the bill criminalizes unlawful access to computer; unauthorized disclosure of access code; illegal communication using computer; system interference and misuse of devices; denial of service; identity theft and impersonation; records retention by service providers; failure of service providers to perform certain duties; cybersquatting; cyber

[51] Section 29 (1)(2), Payments System Management Bill, 2009

terrorism; violation of intellectual property rights with the use of computers; using any computer for unlawful sexual purposes; Attempt, conspiracy and abetment. The bill also provides for the security and protection critical information infrastructure; critical information infrastructure as well as audit and inspection of critical information infrastructure.[52]

This Bill makes reproduces certain provisions of the current Cyber Crimes Act, 2015; it would therefore be a duplication of laws when eventually passed by the National Assembly. Even though the bill only makes slight additions to the provisions already made by the cybercrimes Act.

An important, and perhaps one of the major contributions of the bill is the establishment of agency that shall establish and maintain a system for monitoring and tracking the suspected misuse of any computer for the commission of any crime in Nigeria; gather and compute data on any offence committed or perpetrated through the use of any computer for the purposes of investigation, prosecution and enforcement under this Act and other relevant laws in Nigeria; formulate measures and strategies to prevent the utilization of any computer for the commission of any crime in Nigeria; and carry out public enlightenment campaigns or public awareness programmes to educate Nigerians on crimes committed in the cyberspace and fraud-related activities on the internet; [53]

In essence, the bill provides for preventive measures through consistent monitoring and tracking of computer misuse. The provision on public enlightenment campaigns or public awareness programmes is a welcome innovation which has not been properly catered for in other Bills and Acts.

[52] Part 6, Computer Security and Protection Bill, 2009
[53] Under section 6, Computer Security and Protection Bill, 2009

4.3.6 Telecommunications Facilities (Lawful Interception of Information) Bill, 2010

This Bill requires telecommunications service providers to put in place and maintain certain capabilities that facilitate the lawful interception of information transmitted by telecommunications and to provide basic information about their subscribers to the Nigeria Police Force and the State Security Service. It is divided into 13 parts, 54 Sections and 2 schedules.

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

4.3.7 Cyber Security Bill 2011

The Bill seeks to provide measures for national cybersecurity and for the prevention, detection, responds and prosecution of cybercrimes and other related matters. It is divided into 6 parts and 38 Sections. The objects and scope of this bill is to provide an effective legal framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria; and enhance cybersecurity and the protection of computer systems and networks, electronic communications; data and computer programs in Nigeria;[54]

Part 2 of the bill provides for offences and penalties which include unlawful access to a computer; unlawful interception of communications; unauthorized modification of computer program or data; system interference; misuse of devices; computer pornography

[54] Section 1:-(1), Cyber Security Bill, 2011

and related offences; identity theft and impersonation; cybersquatting; cyber terrorism; racist and xenophobic offences; records retention and protection of data by service providers; interception of electronic communications; failure of service provider to perform certain duties; Attempt, conspiracy, aiding and abetting; Corporate liability.

Part 3 of the bill provides for designation of certain computer systems or networks as national critical information infrastructure, audit and inspection of such critical information infrastructure, and provides for offences against this critical information Infrastructure.

This Bill makes substantial reproduction of the current Cyber Crimes Act, 2015, it would therefore be a duplication of laws, even though the bill makes slight additions to the substance of the Act.

4.3.8 The Frivolous Petitions (Prohibition, etc.) (the Anti-Social Media) Bill 2015

The Bill is meant to protect the rights and freedom of a person against abuse as a result of any petition or statement submitted against such person without a duly sworn affidavit supporting the petition or statement. Though the word person is used in the Bill, the Bill is clearly meant to protect public officers from frivolous petitions; the bill seeks to criminalize the act of individuals sponsoring frivolous petitions to tarnish or blackmail public servants or the Senate President, political office holders for selfish purposes.

The Bill prohibits any person from maliciously making allegations or publishing petitions in both print and electronic media with intent to discredit or set the petitioned person

against any person, group ofpersons, or government institution. The punishment for doing so is a 2-year imprisonment or N4, 000,000 fine.[55]

The Bill has been criticized from several angles; prominent among such is that the Bill violates the freedom of expression of Nigerians, which resulted to its being thrown out by the senate. Section 39(1) of the 1999 Constitution of the Federal Republic of Nigeria guarantees that every person shall be entitled to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference. Subsection (2) provides that every person shall be entitled to own, establish, and operate any medium [including social media] for the dissemination of information, ideas, and opinions.

Though Section 39(3) of the constitution stipulates that the National Assembly can justifiably make any law that will reasonably restrict the freedom of expression guaranteed under section 39, however, the National Assembly's power to do so is not unlimited. Section 39 limits the exercise of such powers by providing they can only make such laws for the purpose of preventing the disclosure of information received in confidence, maintaining the authority and independence of courts, or regulating telephony, wireless broadcasting, television or the exhibition of cinematograph films; or imposing restrictions upon persons holding office under the Government of the Federation or of a State, members of the armed forces of the Federation or members of the Nigeria Police Force or other Government security services or agencies established by law. Therefore, section 39 of the Constitution does not give the National Assembly the power to restrict the freedom of expression of any person.

[55]Section 3(3), Frivolous Petitions (Prohibition, etc.) Bill, 2015

Another similar, but more stern provision of the constitution on freedom of expression is section 45(1). The section appears to have greatly restricted freedom of expression and some other freedoms guaranteed under sections 37, 38, 39, 40, and 41 of the Constitution. It provides that these provisions shall not invalidate any law that is reasonably justifiable in a democratic society if the law is in the interest of defence, public safety, public order, public morality or public health; or for the purpose of protecting the rights and freedom of other persons.

Notwithstanding the provision of section 45 of the constitution, the National Assembly cannot justify the invalidation of section 39 of the Constitution with such undemocratic provisions as the Frivolous Petition Bill. The initial stand by the Senate was that the bill was in accordance with section 45(2) of the Constitution. This is not enough justification because by seeking to protect the interest of public servants or public office holders, the bill is itself encroaching on the rights and freedom of other persons. If fundamental rights and freedom guaranteed by the Constitution are invalidated obnoxiously because other persons' rights need to be protected, there will be no rights left for anyone to live for. The Bill will hurt public accountability, transparency, the rule of Law and good governance in a democratic society like Nigeria.

By requiring that a petitioner must swear to an affidavit supporting his or her petition, the bill greatly discourages an innocent petitioner, who has written a petition in good faith, with the threat of perjury. In a growing democracy like ours where citizens are yet to imbibe the culture of petitioning their leaders because their safety under our weak laws is often put in great danger, the Frivolous Petitions (Prohibition, etc.) Bill is counter-productive.

From the political angle the bill appears to be made not in the interest of Nigerians. Here the rule of law is tilted in favour of public office holders only. The bill appears to be self-serving. It is a public bill seeking to protect political interests.

The bill potentially threatens the freedom of expression through the social media. Though the Senate had tried to explain that the bill is not meant to throw behind bars, people who criticised the government on social media, but protect a person's right against frivolous petitions. Many commentators are of the view that the 8th Assembly of the Senate was either being dishonest or out rightly ignorant about the Bill before it. For instance, Section 3(4) of the Bill clearly restricts social-media user's freedom of expression when it provided that:

> "Where any person through text message, tweets, WhatsApp or through any social media [,] post any abusive statement knowing same to be false with intent to set the public against any person and/or group of persons, an institution of government or such other bodies established by law shall be guilty of an offence and upon conviction shall be liable to an imprisonment for two years or a fine of N2,000,000.00 or both such [sic] fine and imprisonment."

Section 3(4) of the Bill is an attempt to smuggle an anti-social media restriction which has nothing to do with frivolous petitions into the bill. The section restricts free speech on social media and other electronic media by prohibiting what the drafter terms 'any abusive statement knowing same to be false with intent to set the public against any person…". 'Abusive statement' is a dangerously wide term. What amounts to an abusive statement? Does it include criticisms? Who determines what is abusive? Petitions and affidavits are not the same with messages and posts on social media platforms. Tweets, Text messages, Facebook updates, Instagram photos, or LinkedIn posts, and WhatsApp messages and status have nothing to do with frivolous petitions. The Bill potentially threatens Nigerian's access to and use of information under the Freedom of Information Act.

The Frivolous Petitions (Prohibition, etc.) Bill is clearly a barefaced violation of the citizen's constitutional rights and freedom. Neither section 39 nor section 45 of the Constitution permits the encroaching provisions of this anti-democratic Bill. The Bill is a big threat to individual freedom and democracy. The existing laws, the Cybercrimes Act as well as the Criminal and Penal Codes, already provided adequate protection to those who genuinely feel that their rights have been abused or encroached upon by means of false, frivolous, malicious, mischievous, and vexatious petitions.

Section 51 of the Criminal Code punishes sedition while section 375 punishes publication of defamatory statements. This Bill has been particularly resisted by Social-media activists, Online Publishers Association (OPA), Nigerian Guild of Editors (NGE),the Socio-Economic Rights Accountability Project (SERAP), and other similar organizations. The SERAP in particular has gone ahead to appeal to the United Nations Special Rapporteur on the promotion and protection of the right to freedom and opinion expression over Senate's Frivolous Petitions (Prohibition, etc.) Bill. These cumulated pressures resulted to the throwing away of the Bill.

4.3.9 Electronic Transactions Bills 2015

The Bill seeks to facilitate the use of information in electronic form for conducting transactions in Nigeria. Furthermore, the Bill seeks to provide a legal and regulatory framework for: (a) conducting transactions using electronic or related media; (b) the protection of the rights of consumers and other parties in electronic transactions and services; (c) the protection of personal data; and (d) facilitating electronic commerce in Nigeria.

Though the bill was passed into law by the Senate at its plenary session of Thursday, 18th May, 2017, it is yet to be signed into law by Nigeria's President Buhari due to what has been described as drafting issues.

The main objects of the Bill are: to eliminate legal barriers to the effective use of electronic communications in transaction; to promote the harmonization of legal rules on electronic transactions across national boundaries; to facilitate the appropriate use of electronic transactions; to promote business and community confidence in electronic transactions; and to enable business and the community to use electronic communications in their transactions with government. [56]

Sections 15 and 16 of the Bill provide for e-contracts. The Bill provides that unless the parties agree otherwise, an offer, the acceptance of an offer or any other matter that is material to the formation or operation of a contract may be expressed by means of information in electronic form; or by an act that is intended to result in electronic communication, such as touching or clicking on an appropriate icon or other place on a computer screen, or by speaking.[57] It also provides that a contract is not invalid or unenforceable by reason only that it was made in electronic form.[58] Section 16 states that, a contract may be formed by the interaction of computer programmes or other electronic means used to initiate an act or to respond to electronic information, in whole or in part, without review by an individual at the time of the response or act.

The passage of the Bill by the National Assembly is a laudable development. The Bill is an attempt to deepen the benefits derivable from electronic transactions and address, as much as possible, certain legitimate concerns about electronic transactions in Nigeria such as

[56] Section 1, Electronic Transactions Bills, 2015
[57] Section 15(1), Electronic Transactions Bills, 2015
[58] Section 15(1), Electronic Transactions Bills, 2015

non-disclosure of full information on products and services, deceptive advertisement, improper description of products, delivery of defective products, poor informal dispute settlement procedures, double payments and poor customer service.

However, the Bill itself is not without some shortcomings. Some of the identified shortcomings are not necessarily peculiar to the Bill but relate generally to the nature of electronic transactions. The shortcomings, which are not exhaustive they include:

The Bill's most significant provision is in respect of anonymity. It requires the seller of goods and services to disclose information about itself, the goods and details of the transaction. However, the Bill does not address issues regarding non delivery of goods which have been paid for. It also does not require the buyer to disclose information about itself, as in the case of the seller. This may seem moot, since in most cases in Nigeria, the identity of the buyer is not as important especially where delivery of the goods or performance of the service is only triggered upon payment of the quoted price by the buyer. But the issue that may arise is, what happens where the seller devotes resources to deliver the goods under such arrangement of pay on delivery, and the seller is unable to locate the buyer's address? The issue remains unresolved.

Further, the Bill does not address the urgent need for data protection laws which would regulate the extent to which information provided by users of electronic platform in accessing the platform would be used. Given that a significant amount of personal information is stored on computers and are capable of instant transmission to anywhere in the world at a click, it appears that the right to keep certain information to oneself, and to tell other people that certain things are none of their business is currently under technological threat. Many countries have laws which restrict the release of personal information without the consent of the owner of the information; restrict use of such

information for the purpose for which it is provided, and provide sanctions in the case of breach. The Bill does not currently address this concern.

The Bill provides for the formation of contract in electronic form. It provides that subject to the agreement of parties "…an offer, acceptance or any other matter that is material to the formation of a contract may be expressed in electronic form, by a click, or by speaking". Section 15 of the Bill also provides for when an electronic communication is presumed to have been sent or received. The Bill is not however clear on when a contract can be said to have come into existence, and whether display of online goods amounts to an offer or an invitation to treat. It also does not clearly state whether an offer is made once the email containing the offer has been sent, or when it has been received by the other party. Issues bordering on legal principles of offer and acceptance have been subject of several judicial pronouncements stipulating when offer and acceptance are said to have been made, and clarity is desired in relation to how they apply in online transactions.

The Bill makes provisions for payments to be made by electronic means, it does not however provide a guarantee as to the safety or security of making payment by such means. The reprieve is that the Cybercrimes Act deals with matters relating to cybersecurity and should be read together with the Bill, when assented to the President.

Another conflict area under the Bill is in the enforcement and conflict of laws. Electronic transactions give rise to the issue of jurisdiction and choice of law given the fact that the parties to the transaction may reside in different locations with different set of laws. The Bill provides that an electronic communication is deemed to be sent from the sender's place of business and received at the addressee's place of business.[59] However, the Bill is silent on what happens where the only address provided is an email address, in which case,

[59] Section 19(4) Electronic Transaction Bill, 2015

a determination of whether the applicable location should be that of the registrar for the "*url*" for the email account or that of the internet service provider from where the email is generated will be required.

The Bill is silent on the adjudication process of disputes relating to electronic transactions and the need for a specialized court which will address issues relating to e-commerce. In order to properly adjudicate on issues relating to electronic transactions whether as a practitioner or as an adjudicator, one must be knowledgeable in the intricacies and technical details of information and communications technology.[60]

4.4 Policy Framework on the Cyberspace in Nigeria

The Federal Government of Nigeria, in a bid to regulate activities in the cyberspace, for the purpose of curbing cyber threats and offences, has formulated several policies at different times, these include the following:

4.4.1 The Nigerian National Policy for Information Technology

This policy was approved by the Federal Executive Council in March 2001 with the establishment of the National Information Technology Development Agency (NITDA), charged with the implementation responsibility. The policy recognized the private sector as the driving engine of the IT sector. Under the policy NITDA is to enter into strategic alliance, collaboration and joint venture with the private sector for the actualization of the IT vision, which is to make Nigeria an IT capable country as well as using IT as an engine for sustainable development and global competitiveness. It is also to be used for education, job creation, wealth creation, and poverty eradication. Emphasis is to be laid on

[60]Aniaka O. (2017)Analysing The Adequacy Of Electronic Transactions Bill 2015 in Facilitating E-Commerce In Nigeria available at: http://ssrn.com/abstract=2651120 accessed 06/06/2019 2;15pm

development of national information infrastructure backbone (NIIB) as well as the human resources development.[61]

It is however regrettable to note that Nigeria has not made substantial progress in terms of implementing the objectives stated above in its National policy on IT. Till date, Nigeria is still dependent on foreign countries for importation of computer hardware, software packages, and depending on foreign experts for the technical know-how[62]. It has been stated[63] that in terms of information technology development, South Africa stands in sharp contrast to other Africa countries including Nigeria. It is estimated that there are about 270,000 Internet Service Providers (ISPs) in that country. The IT policy in Nigeria has a mission statement that says: "To make Nigeria an IT capable country in Africa and a key player in the Information Society by the year 2005, using IT as the engine for sustainable development and global competitiveness." As stated in the IT policy, by 2005 Nigeria was to become "an IT capable country in Africa." However till date Nigeria is still lagging behind.[64]

4.4.2 Telecommunication Policy in Nigeria

In 1998, the Ministry of Communications published the maiden edition of the National Policy on Telecommunications. The policy was approved and published three years after its production in 1995. Consequently, at the time of publication, certain prescriptions contained in the policy were outdated, overtaken by events or required further modification, in order to be consistent with new developments and emerging industry

[61]Adomi, E., (2006). *Application of Information and Communication Technologies (ICTs) in Nigerian High Schools*. *Warri*, Publication of the Nigerian Library Association, Delta State Chapter. p.1
[62]*ibid*
[63]Omoigui, N (2005). The Information Age Has a Key to Nigeria's Renaissance: Opportunities Risks, And Geopolitical Implications. Retrieved 10/12 2016 10 am from http://www.waadoorg/Nigeria_scholars/archive/opinion/NosaTech.html
[64]Adomi, E. (2006). Op cit. 129

trends both locally and internationally. The need for Telecommunications Policy in Nigeria becomes compelling. The former President (Chief Olusegun Obasanjo) approved the National Policy on telecommunications presented by the committee on telecommunications policy for Nigeria and the policy was launched in October 1999[65].

The overriding objective of the National Telecommunications Policy is to achieve the modernization and rapid expansion of the telecommunications network and services and social development, and integrate Nigeria internally as well as into global telecommunications environment. Telecommunications services should accordingly be efficient, affordable, reliable and available to all. Some of the short-term objectives of the National Policy on Telecommunications, 2001 are to promote widespread access to advance communications technologies and services, particularly the internet and related capabilities; develop and enhance indigenous capacity in telecommunications technology; participate effectively in international telecommunications activities in other to promote telecommunications development in Nigeria, to meet the country's international obligations and derive maximum benefit from international cooperation in these areas; ensure that the government invests its interest in the state owned telecommunications facilities; review and update telecommunications laws in other to bring all telecommunications operators under the regulatory control of Nigerian Communications Commission (NCC).

The Policy also articulated medium- term objectives which are to; provide a new regulatory environment that is sufficiently flexible to take into account new technological development and the international trend towards convergence; ensure that public telecommunications facilities are accessible to all communities in the country; encourage domestic production of telecommunications equipment in Nigeria and development related

[65]National Policy on Telecommunications (Federal Republic of Nigeria, 2001)

software and services; encourage the development of information super-highway that will enable Nigerians enjoy the benefits of globalization and convergence; create the enabling environment, including the provision of incentives, that will attract investors and resources to achieve the objectives earlier stated.

4.4.3 National Cybersecurity Policy

The policy outlines the actions government and other players alike will take to lessen the risks and secure the gains of our continuous dependence on cyberspace. The national cybersecurity policy sets out the strategic intent of the government of Nigeria in mitigating the country's cyber risk exposure; curtailing cyber threats that are inimical to national security and the Nigerian economic well being[66]

In terms of the rationale, the national cybersecurity policy seeks to enable Nigeria confront the growing challenge of cyber threats that are constantly challenging confidentiality, integrity and availability of cyberspace which can affect the critical functioning of the state. In this wise, the strategy identifies five key cyber threats that pose significant challenges to Nigeria and are inimical to national growth and security. These threats are cybercrime, cyber-espionage, cyber conflict, cyber terrorism, and child online abuse and exploitation.[67]

The goal of the national cybersecurity policy is to manage security threats in cyberspace in line with the overall national security objective. The aim of the policy is to chart a course towards an assured and trusted presence in the cyberspace[68] The objectives of the national cyber security policy includes among others, to:[69]facilitate an effective legal and governance mechanism for Nigeria's presence in cyberspace and cyber security ecosystem;

[66]See part 1-4 of the National Cybersecurity Policy, part one provides for the background, global context and national cybersecurity threat environment
[67]Part. 1-2 ibid
[68]Part three, p.7. ibid
[69]Part 4 at p. 9 ibid

develop an information security and control mechanism for the protection and safety of Nigeria's national critical information infrastructure and its associated economic infrastructure operating in the cyberspace; provide measures for the identification, monitoring, analysis and evaluation of the national critical information infrastructure for maintaining Nigeria's active presence in the cyberspace; develop a national cybersecurity assurance framework, compliance and enforcement mechanism; develop a centralised national emergency readiness and incident management coordination capability; promote emergence of an appropriate legislative environment, intellectual property, data protection and privacy rights; develop a framework for inter-agency collaboration on combating cybercrime and cyber security; establish multi-stakeholder partnerships, cooperation and leadership advisory mechanisms for information sharing, intelligence gathering and coordinated response; develop national criteria for the development of cybersecurity manpower, identify baseline requirements, qualifications for cybersecurity professional and implement measures for certification and regulations of cybersecurity skills, products, and services; facilitate institution of a unified National strategy on cybersecurity to provide guidance, initiatives and measurable action plan in the development, implementation and sustainability of a national cybersecurity roadmap; develop a national mechanism for the establishment of Nigeria's national cybersecurity coordination (NCCC) to serve as the focal point for cybersecurity incident monitoring and response i.e. Nigeria National Computer Emergency Response Team (ng CERT) to coordinate and regulate sectoral computer emergency response team (s- CERT) and the establishment of a National Digital forensic Laboratory (NDFL) in the country[70]

This policy provides a comprehensive document to properly tackle the threat of cybercrimes and related problems in the Nigerian cyberspace.

[70]Part 4 at p. 9 ibid

4.4.4 The National Cybersecurity Strategy (NCSS) - 2014/15

The National Cybersecurity Strategy presents Nigeria's readiness to provide cohesive measures and strategic actions towards assuring security and protection of the country's presence in cyberspace, safeguarding critical information infrastructure, building and nurturing trusted cyber-community. The strategy identifies specific cyber threats worldwide and inimical to national interest as: cybercrime, cyber-terrorism, cyber conflict, cyber espionage and child online abuse and exploitation. These threats have significant capability to damage the integrity of the nation, disruption of critical information infrastructure operations, as well as undermine government operations and national security.

In terms of rationale, the NCSS is developed to articulate, coordinate and guide the country in the implementation of National Cybersecurity Policy and in developing cohesive counter-threat measures for the protection, security and defence of National cyberspace.

The aim of the NCSS is to provide a cohesive roadmap, initiatives and implementation mechanism for achieving the national vision on cybersecurity. The National Cybersecurity Strategy is directed at achieving the following objectives, among others: a comprehensive cybercrime legislation and cyber threat counter measures that are nationally adoptable, regionally and globally relevant in the context of securing the nation's cyberspace; provision of measures that protect critical information infrastructure, as well as reducing national vulnerabilities through cyber securities assurance frame work; and to articulate an effective computer emergency response capability. The strategy comprehensively covers several aspects of the fight against cyber offences, however we are yet to see effective implementation of this strategy.

4.4.5 Bank Verification Number (BVN) Policy

Owing to the increasing incidents of compromise on conventional security systems (password and PIN), there is a high demand for greater security on access to sensitive or personal information in the Banking system, the Central Bank of Nigeria through the Banker's Committee and in collaboration with all banks in Nigeria on February 14, 2014 launched a centralized biometric identification system for the banking industry tagged Bank Verification Number (BVN). The BVN gives each Bank customer a unique identity across the Nigerian Banking industry that can be used for easy identification and verification at Point of Banking operations.

The role of the BVN is aimed at curtailing hazards associated with social security and credit risks[71] BVN uses biometric technology to register customers in the financial system. Biometrics refers to identification of an individual based on physiological attributes - fingerprint, voice, facial and other features. It records these physical features which are unique to individuals. The records would be used to identify the person afterwards[72]. Once a person`s biometrics have been recorded, the BVN issued, the account would be accessed through BVN. The Major objectives of the initiatives are to protect bank customers, reduce fraud and strengthen the Nigerian Banking system

Customers Bank accounts are protected from unauthorized access with the use of BVN. Through an enhanced biometric real-time security system, danger of unauthorized access to customers' bank account is brought under check. The BVN is encompassing in detecting fraud of whatever type, whether through unauthorized access or through illegally

[71] Leland & David, (1977), The BVN Anatomy, *the Journal of Finance*, Vol.32 (2)., Pdf retrieved on 14/10/2016 12:00pm

[72] Douglas D. (1991), What is BVN, *Journal of Political Economy*, vol. 99,(4), pp. 689-721

authorized forms, and any other form of fraud that is against the rule of law and social justice[73]

The policy operates such that if one has accounts in several banks, one does not need to do the enrollment process in each bank. It is only done in one bank. Once a customer receives the special BVN number via SMS, the customer simply visits his other banks and submit the number to them. The benefits of BVN include: BVN gives a unique identity that can be verified across the Nigerian Banking Industry (not peculiar to one Bank), Customers Bank Accounts are protected from unauthorized access, issues of identity the ftare addressed, thus reduce exposure to fraud. The BVN will, enhance the Banking Industry chances of being able to fish out blacklisted customers; reduce fraudulent activities on bank account; reduce queue in banking halls; standardize efficiency of banking operations; unify customers unique BVN as the accepted means of identification across all Nigerian Banks[74]

This policy, good as it appears, has its shortcomings. It protects the individual's data from unlawful access on one hand, and on the other hand it exposes the individual's privacy as ones' bank details can be retrieved through his phone number. The BVN requirement involves the storage of sensitive biometric data, which in itself is the target of cybercriminals.

4.5 Institutional Frame Work

Through the combined efforts of both the government and the private sector several institutions have been set up to help in the drive towards cybersecurity and the protection of critical information infrastructure. Some of these institutions are provided below:

[73]Meza D., David and Webb, D. C. (2000) Does Credit Rationing Imply Insufficient lending? *Journal of Public Economics,* 78 (3). pp. 215-234. ISSN 0047-2727
[74]VFS Global (2001) 3 Simple Steps to Apply For Bank Verification Number http://www.bvn.com.ng/ accessed 12/10/2016 10:40am

4.5.1 Nigerian Communications Commission (NCC)

The Nigerian Communications Commission (NCC) was established by the Nigerian Communications Act as an independent national regulatory authority for the telecommunications industry in Nigeria.[75] The NCC is responsible for creating an enabling environment for competition among operators in the industry as well as ensuring the provision of qualitative and efficient telecommunications services throughout the country. The main functions of the NCC, apart from implementing the WTA, include*:* the facilitation of investments in and entry into the Nigerian market for the provision and supply of communications services equipment and facilities; the protection and promotion of the interest of consumers against unfair practices including but not limited to matters relating to tariffs and charges for and the availability and quality of communications services, equipment and facilities; ensuring that licensees implement and operate at all times the most efficient and accurate billing system; and the promotion of fair competition in the communications industry and the protection of communications services and facilities providers from the misuse of market power or anti-competitive and unfair practices by other services or facilities providers or equipment suppliers.[76]

The Nigeria Communications Commission (NCC), has also established a Media and Information Security Department to explore ways to protect corporate and individual citizens from the cyber challenges, providing awareness and information to help those vulnerable to these cybercrimes to curb the menace of cybercrimes in the country. [77]

[75]See s 3 of the NCA
[76]S 3 of the NCA.
[77] Nigerian Communications Commission official site http://www.ncc.gov.ng/16-about-ncc accessed 27/7/2017 8:24am

4.5.2 The National Information Technology Development Agency (NITDA)

Following the approval of the National Information Technology Policy (National IT Policy) by the Federal Government of Nigeria in March 2001, the National Information Technology Development Agency (the NITDA) was established in 2001 under the Federal Ministry of Science and Technology. It was initially given the task of implementing the policy through coordinating and promoting the development and use of information technology in Nigeria. NITDA was formally established in 2007under an Act of the Nigerian National Assembly.[78]

The primary functions of the NITDA under the law comprise these: creating a framework for the planning, research, development, standardisation, application, coordination, monitoring, evaluation and regulation of information technology practices, activities and systems in Nigeria and all matters related thereto and for that purpose;[79] providing guidelines to facilitate the establishment and maintenance of appropriate infrastructure for information technology and systems application and development in Nigeria for the public and private sectors, urban/rural development, the economy and the government;[80] developing guidelines for electronic governance;[81] developing guidelines for the networking of public and private sector establishments;[82] developing guidelines for the standardisation and certification of information technology Escrow Source Code and Object Code Domiciliation, Application and Delivery systems in Nigeria;[83] rendering advisory services in all information technology matters to the public and private

[78]The NITDA Act, 2007
[79]S. 6(a) of the NITDA Act.
[80]S. 6(b) of the NITDA Act.
[81]S. 6(c) of the NITDA Act.
[82]S. 6(d) of the NITDA Act.
[83]S. 6(e) of the NITDA Act.

sectors;[84] introducing appropriate regulatory policies and incentives to encourage private sector investment in the information technology industry;[85] determining critical areas in Information technology requiring research intervention and facilitating research and development in those areas; and, accelerating internet penetration in Nigeria and promoting sound internet governance.[86]

An additional function of NITDA is to advise the Federal Government generally on issues related to the management and administration of Nigeria's country code top level domain (.ng) and also to supervise any organisation incorporated under the laws of Nigeria to manage and administer Nigeria's country code top level domain (.ng)[87]

The National Information Technology Development Agency (NITDA) has also adopted the COBIT 5 framework, which is expected by implementation to help "provide a holistic approach by including all the minimum requirements for a policy framework and thus lead to a better cybersecurity atmosphere in Nigeria".[88]

4.5.3 Office of the National Security Adviser.

The Office of the National Security Adviser has produced the National Cybersecurity Policy, the National Cybersecurity Strategy and the National Cybersecurity Roadmap.[89]Worried by the increasing cybercrime and the potential dangers inherent, the Office of the National Security Adviser (ONSA) has partnered with Microsoft Nigeria and other industry stakeholders, to tackle the ugly cyber related threats. The partnership is centred on cybersecurity capacity building with the aim of supporting ONSA, Federal

[84]S 6(f) of the NITDA Act.
[85]S. 6(g) of the NITDA Act.
[86]S. 6 of the NITDA Act.
[87]Second schedule, s 6(m) of the NITDA Act - Supplementary Provisions Relating to the Supervision of the Management of the Country Code Top-level Domain (.ng) on the Internet.
[88]Abikoye O. and Yusuf S. (2014) Cybersecurity in Nigeria: *Need for A Paradigm* Shift Retrieved from www.pinigeria.org on 10/07/2019 10:10am
[89]ibid

Government Ministries, Departments and Agencies (MDAs), to grow capacity with respect to global approaches to national cybersecurity strategy, addressing cybersecurity risks, computer emergency response Team (CERT) management, security and privacy of data in the cloud, cybersecurity forensics and audit skills, global policy and legal developments, cloud computing and its benefits, growing local data hosting capabilities, in line with the new Nigerian cybercrime law, the Cybercrime Act 2015.[90]

4.5.4 Office of the Attorney General of the Federation

The Attorney General's office has a unit called the Cybercrime Prosecution Unit provides the overall policy, legislation and prosecution thrust. Currently, the Federal Ministry of Justice has commenced training of legal practitioners on forensic evidence in order to strengthen the capacity of legal officers of the ministry in the area of forensic evidence examination and presentation. The training seeks to expose them to the nature and scope of digital and cybercrime in the society. The ministry in collaboration with First Digital & Techno-Law Forensics Company, held a four-day Forensics Evidence Boot Camp for legal officers of the ministry in Abuja recently. The essence of the training is to have a group of Lawyers who will be better informed in the prevention and detection of digital and computer crime and who will support law enforcement agencies and the judiciary in the skilful handling of digital evidence.[91]

[90] Emeka A. (2015) NSA, Microsoft Team up to Tackle Cybercrime in Nigeria available at: https://www.vanguardngr.com/2015/11/nsa-microsoft-team-up-to-tackle-cybercrime-in-nigeria/ Read more at: https://www.vanguardngr.com/2015/11/nsa-microsoft-team-up-to-tackle-cybercrime-in-nigeria/ https://www.vanguardngr.com/2015/11/nsa-microsoft-team-up-to-tackle-cybercrime-in-niger accessed 10/10/20172:42am

[91] Dernièremise à jour (2018) Cybercrime policies/strategies retrieved from http://www.Nigerianelitesforum.com/ng/computers-and-ict/21334-nigeria-fg-begins-training-on-forensicsevidence.html #ixzz4LSVca4Ck accessed 12/10/2016 10:40am

4.5.5 Ministry of Communications Technology

The Ministry of Communications Technology is now the regulating body of the Nigerian Communications Commission (NCC), National Information Technology Development Agency (NITDA), and the Nigerian Postal Services (NIPOST). Two Limited Liability Companies that are wholly owned by the Government-Nigeria Communications Satellite Limited and Galaxy Backbone Plc- have also been brought under the Ministry[92]

4.5.6 The National Broadcasting Commission

The National Broadcasting Commission (NBC) is established by the National Broadcasting Commission Act.[93] The NBC is responsible for advising the Federal Government on the implementation of the National Mass Communication Policy, with particular reference to broadcasting as well as licensing Cable, DTH, and all terrestrial radio and television services. The NBC is also responsible for undertaking research and development in the broadcast industry, upholding the principles of equity and fairness in broadcasting, and establishing and disseminating a national broadcasting code, while also setting standards with regards to the contents and quality of the materials broadcast.

4.5.7 The National Environmental Standards and Regulation Enforcement Agency

The National Environmental Standards and Regulation Enforcement Agency (NESREA) was established in 2007 by the National Environmental Standards and Regulation Enforcement Agency (Establishment) Act. The Agency is responsible for ensuring the effective enforcement of environmental laws and regulations in the country, except in the oil and gas industry. The Act establishing the Agency creates provisions for the setting of

[92]Ladan M.T (2015) op cit. pg.136
[93]See the NBC Act LFN 2004

air quality standards and atmospheric protection.[94] The Act also prohibits the discharge of hazardous substances into the air or upon the land and waters of Nigeria or at the adjoining shorelines except where such discharge is permitted or authorised under any law in force in Nigeria.[95] Importantly, these provisions constitute a framework for controlling hazardous emissions from telecommunications and ICT equipment to prevent environmental and health hazards. An oversight in the law is illustrated by incessant confusion between the NESREA and the NCC's competing claims over the regulation of masts.

4.5.8 The Standards Organisation of Nigeria

The Standards Organisation of Nigeria (SON) was established under the Standards Organisation of Nigeria Act[96] as a regulatory framework for enforcing standardising methods of production in Nigeria. The SON is required under the law to be actively involved in the inspection of imported goods and quality assessment at the ports and manufacturing establishments. The importance of this exercise is enormous, considering the economic, health and safety implications of the influx of substandard goods into the country. This regulatory function of the SON extends to the ICT industry in the regulation and enforcement of standards of ICT products and equipment manufactured in the country or imported from elsewhere.

4.5.9 Economic and Financial Crimes Commission (EFCC)

Economic and Financial Crimes Commission was established under section 6 of the Economic and Financial Crimes Commission Act. The Commission is given enormous regulatory powers over the activities highlighted in section 46 of the Act[97] including the

[94]S. 20(1) of the NESREA Act. S 27(1) of the NESREA Act.
[95] S 27(1) of the NESREA Act.
[96]Standards Organisation of Nigeria Act of 2004.
[97] Section 46, EFCC Act, 2004

investigation of all financial crimes such as advance fee fraud, money laundering, counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, contract scam etc.[98] The Commission is also mandated to adopt "measures to eradicate the commission of economic and financial crimes."[99] More importantly, the Commission is also to act as the co-ordinating agency for the enforcement of the provisions of the Money Laundering Act, the Advance Fee Fraud and other Related Offences Act, 1995, the Failed Banks (Recovery of Debt and Financial Malpractices in Banks) Act, 1994 the Banks and other Financial Institutions Act, Miscellaneous Offences Act, and any other law or regulation relating to economic and financial crimes, including the Criminal Code and Penal Code.[100] EFCC has taken giant strides in the direction of minimizing the prevalence of economic and financial crimes by the prosecution of a number of notable Nigerians for their alleged involvement in these crimes.[101]

4.5.10 The Nigerian Cybercrime Working Group (NCWG)

The Nigerian Cybercrime Working Group (NCWG) is an Inter-Agency body made up of all key law enforcement, security, intelligence and ICT Agencies of government, plus major private organizations in the ICT sector; including Economic and Financial Crimes Commission (EFCC), Nigeria Police Force (NPF); the National Security Adviser (NSA), the Nigerian Communications Commission (NCC); Department of State Services (DSS); National Intelligence Agency (NIA); Nigeria Computer Society (NCS); Nigeria Internet Group (NIG); Internet Services Providers' Association of Nigeria (ISPAN); National Information Technology Development Agency (NITDA), and Individual citizen

[98] Section 6(b), EFCC Act, 2004
[99] Section 6(e), EFCC Act, 2004
[100] Section 7(2), EFCC Act, 2004
[101] The Federal High Court's conviction of Mrs Anajemba over money-laundering offences is a typical example of such convictions. The *Guardian,* Tuesday, June 12, 2005, p 1.

representing public interest. The major mandate of the group include public enlightenment – Cybersecurity Forum for the Financial Services Sector, building institutional consensus amongst existing Agencies, providing technical assistance to the National Assembly on Cybercrime and the draft act; laying the groundwork for establishment of institutional capacity in Nigeria, etc.[102]

4.5.11 The Nigeria Internet Governance Forum Multi-stakeholders Advisory Group (NIGF-MAG)

The Nigeria Internet Governance Forum Multi-stakeholders Advisory Group (NIGF-MAG), comprises the Federal Ministry of Communications (MoC), National Information Technology Development Agency (NITDA), Nigerian Communications Commission (NCC), Nigeria Internet Registration Association (NIRA), Internet Society Nigeria Chapter (ISOC NG), Digita lSENSE Africa Media, Creative Technology Development International (CTDL), and Global Network for Cyber Solution (GNC). This group coordinates the Nigeria Internet Governance Forum **(**NIGF). This forum provides a platform for national dialogue, interactions, contributions and exchange of ideas on challenging and emerging policy issues relating to public policy issues on the Internet and Internet Governance Ecosystem. It offers opportunities for stakeholders from the Governments, Civil Society, Businesses, Technical Community, Academia, youth and women including development partners and multinational corporations operating in the Nigerian Internet ecosystem to come together, harnesses ideas, builds consensus and offers collective solutions to the thematic sessions.[103]

[102]ibid
[103]See the NIGF-MAG official site www.nigf.org.ng. accessed

4.5.12 The Nigerian Internet Registration Association (NIRA)[104]

The Nigerian Internet Registration Association (NIRA) was founded on March 23, 2005 as a stakeholder-led organisation responsible for the management of Nigeria's Country Top Level Domain Name (ccTLD) ".ng."The organisation is coordinated by NITDA, with stakeholders drawn from within Nigeria's Internet Community. The NIRA seeks to maintain and promote the operational stability and utility of the ccTLD".ng" and, by ensuring cost effective administration, to promote the development and establishment of a policy framework for the development and administration of the "ng", "cc" and "TLD".

4.5.13 Computer Emergency and Readiness Team[105]

In April 2014, the Nigerian government launched a Computer Emergency Readiness and Response Team (CERRT.ng) Ecosystem.This is an anti-cybercrime forensic laboratory that seeks to assist public institutions, private bodies and individuals in responding to computer, network and related cybersecurity challenges or threats. The Forensic laboratory, the first of its kind in the West African region, is expected to analyse and resolve cybersecurity incidents as needed, “in Nigeria, by Nigerians and for Nigerians”.

The body is aimed at responding to computer, network and related cybersecurity incidents. The system is aimed at addressing the national strategic interest that requires Nigeria to develop, nurture and patronise home-grown cybersecurity solutions with the objectives of generating employment, enhancing human safety and national well-being and promoting knowledge generation among others. It would identify existing and potential computer-related threats, notify as appropriate, build capacities, coordinate responses and liaise, as needed, with similar incident response teams locally and worldwide and also develop the

[104] NIRA (2011) see http://www.nira.org.ng/index.php/about-nira.
[105] *ibid*

requisite readiness process. The CERRT.ng Ecosystem was funded by NITDA with the goal of being a trusted intermediary organisation dedicated to providing "support" in responding to computer, network and related cybersecurity incidents by building national readiness through fostering the development of sectorial Computer Emergency Response Teams (CERTs).[106]

The CERRT.ng Ecosystem is envisaged as a collaborative multi-stakeholder Information Technology (IT) driven entity that promotes the development of requisite capacities and building of synergies within and between appropriate entities in all relevant spheres of the nation and beyond. CERRT.ng is actualised through the following core components: a Fusion Centre consisting of a cyber-monitoring centre that monitors the cyberspace, especially those parts of it that are carried on Nigerian based Information Communication Technology (ICT) infrastructure. It has a help desk where the public and organisations can report cyber-incidents. It will also engage in building collaborative platforms and cyber-threat analysis and generation of threat and incident statistics. The Awareness/Training/Liaison/Communications section will focus on building the capacity of Nigeria's human resource base by leveraging on the train-the-trainers approach. It will embark on capacity building partnerships with interested organisations especially academia, service providers, public and private sector organisations. It will facilitate the development of standards in-line with NITDA's mandate.[107]

The Cyber Forensics Laboratory will analyse and resolve cybersecurity incidents in Nigeria. The project is also designed to assist law enforcement and security elements in their investigations and evidence gathering processes by analysing ICT devices seized from

[106]A former acting Director General of Nigeria's National Information Technology Development Agency (NITDA), Dr. Ashiru Daura, said at the launch of CERRT in Abuja.
[107]Rukayat A. A., Charles O. U, Florence A. O.(2016) *Computer Forensic Guidelines: A Requirement for fighting Cyber Crime in Nigeria*, P.4 University of Lagos Press

those suspected of criminal activities. Besides, the project is aimed at ensuring collaboration with these elements in building and reinforcing their own capacities.[108]

4.5.14 The Nigeria National Computer Emergency Response Team (ng CERT)

The Nigeria National Computer Emergency Response Team (ng CERT) Operations Centre was officially commissioned in May, 2015 by the National Security Adviser. A Computer Emergency Response Team (CERT) is an expert group which handles computer security incidents. They are human counterparts to anti-virus software in the sense that when new viruses or computer security threats are discovered, these teams document these problems and work to fix them. Being that these teams are made up of people who can react to new situations, they are much more capable of dealing with new virus threats than anti-virus programs would be by themselves.[109]

The primary goals of a CERT include: establishing a capacity to quickly and effectively coordinate communication among experts during security emergencies in order to prevent future incidents; building awareness of security issues across the internet community; developing the cyber incident response plan; identifying and classifying cyber-attack scenarios; determining the tools and technology used to detect and prevent attacks; promoting cyber-security awareness;[110]

4.5.14 Directorate for Cybersecurity (DfC)

The Directorate for Cybersecurity (DfC) was created as a permanent autonomous body within the Office of the National Security Adviser (ONSA) to take over all assets and liabilities of the NCWG, including all uncompleted projects. Its main mandate is to develop

[108] *ibid*
[109] ITU (2008) Understanding The Concept Of Cyber Security: Policy Competition & Economic Analysis Department Understanding The Concept of Cyber Security Pdf, retrieved from www.understanding-%the-Concept-of7&Cyber-Security.com 3/10/2018
[110] *ibid*

and implement a National Cybersecurity Policy for Nigeria; implement the National Cybersecurity Initiative (NCI); Draft and/or propose all relevant laws required to be enacted by the National Assembly for the security of computer systems and networks in Nigeria, pursuant to our national strategies on cybersecurity; establish a National Computer Emergency Readiness and Response Mechanism with Early Warning System (EWS) and Alerts for all cyber related emergencies in the country; establish a National Computer Forensics Laboratory, and coordinating the training and utilization of the facility by all law enforcement, security and intelligence agencies; create the requisite technical capacity across law enforcement, security and intelligence agencies on cybercrime and cybersecurity; develop effective framework and interfaces for inter-agency collaboration on cybercrime and cybersecurity; establishing appropriate platforms for public private partnership (PPP) on cybersecurity; coordinating Nigeria's involvement in international cybersecurity cooperation to ensure the integration of our country into the global frameworks on cybersecurity; executing such other functions and responsibilities as it shall consider necessary for the general purpose of promoting cyber security in Nigeria and fostering a framework for critical information infrastructure protection in the country.[111]

4.5.15 Cybercrime Advisory Council

The Cybercrime Advisory Council was established by section S. 42 Cyber Crimes Act, 2015. It was inaugurated on 18th April, 2016. The Cybercrime Advisory Council is statutorily charged with functions and powers aimed at addressing the issues and challenges relating to standards, coordination and valuable technical cooperation, particularly in the areas of policy, legislation and capacity building, such as training of

[111]Udotai (2016) Cybersecurity- Framework- *Praia*-Nov -07.pdf- retrieved 2/7/ 2019 12:20pm

cyber-security personnel, investigators, digital forensics personnel, prosecutors, judges and lawmakers[112].

4.5.16 Stakeholders Consultative Forum on Child Online Protection (COP)

Stakeholders Consultative Forum on Child Online Protection (COP) recommended; an all-inclusive multi-stakeholder and multi-sectoral collaboration through partnership and alliances with clearly defined national policy and guidelines. The aftermath of the forum led to the development of Nigerian Child Online Protection Policy Framework and Guidelines covering the following key actors; Parents, guardians, teachers, children, policy maker, law enforcement and industry in 2012.[113]

4.5.17 The Central Bank of Nigeria (CBN)

The CBN is the only public agency certified under internationally recognised standards in cybersecurity. Section 6(5) (b) of the Money Laundering Act, 2011, confers powers on the EFCC and CBN or their authorized representatives to place a stop order on any account or transaction for a time not exceeding 72 hours, if it is discovered in the course of their duties that such accounts are involved in any crime. Where it is not possible for the EFCC or the CBN to conclude their investigation within 72 hours, they must obtain an Order from the Federal High Court directing the Bank to block the funds, accounts or securities. It is an offence for the Central Bank to fail to report to the Commission any reasonable suspicion within 7 days as stated in section 6 (1) and (2) Money Laundering Act, 2011, and is liable upon conviction to a fine of N1million for each day during which the offence continues. CBN by the provision of the Money Laundering Act is empowered to impose a penalty of

[112] Section 43 of the Cybercrime (Prohibition, Prevention, etc.) Act, 2015

[113]Segun H. O. (2016) Cybersecurity, Women and Child Online Protection. A lead Paper Presentation delivered at Women Leaders Forum organized by High-Tech Centre for Nigerian Women and Youth, December 1-2, Sheraton Hotel, Abuja.

not less than N1million or the suspension of any license issued to the bank for failure to comply with the provisions of arousing adequate awareness among the staff.

Pursuant to its powers under the CBN Act, the CBN has issued a number of regulations on e-banking and e-payments. Notable in this regards are: the Guidelines on E-banking in Nigeria, 2003; the Regulatory Framework for Mobile Payment services in Nigeria, 2009; Standards and Guidelines on Point of Sale (POS) Card Acceptance Services; Guidelines on Card Issuance and Usage in Nigeria, 2014; Guidelines on Stored Value and Prepaid Card[114]

4.6 Emerging Trends and Challenges in Regulating the Cyberspace in Nigeria

The Cyberspace is generally dynamic and ever evolving given its peculiar nature. There are constantly emerging issues which in some cases pose serious challenges in the regulation of the cyber space. This is because; as soon as a regulation is made it becomes outdated almost immediately because, within the time taken in passing such legislation several things would have changed. These trends and challenges include:

4.6.1 Difficulty in Internet Governance

Internet governance refers to regulatory mechanisms put in place to ensure the equitable allocation of internet resources such as domain names and internet protocol (IP) addresses. Some notable regulatory mechanisms in this regard have evolved. These include the Internet Corporation for Assigned Names and Numbers (ICANN) and the Nigeria Internet Registration Association (NIRA).

[114]Ladan M.T (2015) op cit. p. 8

The Internet Corporation for Assigned Names and Numbers (ICANN)[115] was founded over ten years ago as a non-profit, multi-stakeholder organisation dedicated to coordinating the Internet's address system. The organisation, based in California, seeks to promote competition in the domain name marketplace while ensuring Internet security and stability. The organisation has established a set of principles known as the Uniform Dispute Resolution Policy (UDRP) for Domain Names[116] to guide the resolution of domain name disputes. The policy establishes a procedure for the online resolution of disputes relating to internet domain names. It also proposes a non-national authority for the resolution of internet domain name disputes, which avoids the competition and conflict that arise from the existence of a variety of national courts and rules.[117]

4.6.2 Jurisdictional Questions

A disturbing legal issue has been that of finding the appropriate jurisdiction where valid judicial enforcement could take place in situations where two parties in different jurisdictions enter into a contract or an enforceable agreement over the internet. Private international law, attempted to provide traditional solution through the "forum state" and "target state" system.[118]

The forum state system

Under this system, legal obligations in cyberspace are restricted to a particular territorial

jurisdiction defined in an online contract. Such jurisdiction will be the forum state, and legal action cannot be brought to enforce any obligations between the parties except in that jurisdiction. The forum state system is generally supported by the business community,

[115] Robin G. (2011) Civil society involvement in ICANN Strengthening future civil society influence in ICANN policymaking: Civil Society & ICANN P.4 20 APC
[116] *ibid*
[117] *ibid*
[118] Benyehlef and Fabien (2005) Lex Electronica 55-58.

which places much emphasis on the risk of having to protect itself against proceedings in a wide range of jurisdictions. This position is strengthened by the realization that it may be difficult on the one hand to restrict the field of such claims to a given jurisdiction because an internet site is published worldwide, and on the other hand, there is a real and "virtual" challenge in identifying the user's location with certainty.[119]

The target state system

Under the target state system, legal obligations in cyberspace are not restricted to a particular territorial jurisdiction, but extend to the jurisdiction where a consumer is located. This system is preferred by consumer advocates because it tends to provide consumers with more extensive protection by allowing them to institute legal proceedings in their own countries and consequently take to advantage of their own national laws on consumer protection.[120]

4.6.3 Net Neutrality

Net neutrality refers to the concept that a broadband network should operate without any restrictions on the kinds of equipment attached to it, or on the mode of communication allowed.[121] "Net neutrality" is a principle that advocates no restrictions by internet service providers and governments on content, sites, platform, kinds of attachment, and the modes of communication. The principle states that if a given user pays for a certain level of internet access, and another user pays for the same level of access, then the two users should be able to connect to each other at the subscribed level of access. Neutrality proponents claim that telecommunications services providers seek to impose a "tired" service model upon users in order to control the paths and pipeline of internet services

[119] *ibid*
[120] *ibid*
[121] Peter C. O (2014) ICT Laws in Nigeria: Planning and Regulating a Societal Journey into the future, PER/PELJ(17)

provided by them. They further argue that such would remove competition, create artificial scarcity, and oblige subscribers to buy uncompetitive services. Many believe that net neutrality is primarily important as a preservation of current freedoms.[122]

4.6.4 Convergence

Convergence refers to the integration or merging of previously separate services in telecommunications/telephony, media/broadcasting and internet technologies into a single technological unit. The practical consequence is interoperability and the ability to access and operate services through a single device e.g. accessing the internet or a broadcast through a mobile phone. According to the ICT Regulation Toolkit "Convergence" is facilitated by the transition from analogue to digital, voice to data, narrowband to broadband, circuit switched to packet switched, one way to interactive, scarcity to abundance, and the accompanying digitalization of all content. Generally, convergence allows both previously separate sectors and entirely new sectors to compete in the same newly expanded market space.'[123] For example, there are already numerous examples of markets offering IPTV and mobile television. In this new, converged market space, customers can expect the seamless provision from multiple sources on a single device of all electronic communications for one supplier competing with many other suppliers.[124]However, convergence is not complete in most developing countries, such as Nigeria. The implication is that the benefits of a converged ICT environment have been limited by the absence of a converged regulatory environment as well as a binding legal

[122]Adavize (2019) Net Neutrality: Reviewing the Nigerian Communications Commission Internet Industry Code of Practice available at http://bits.blogs.nytimes.com/2013/05/20/aid-for-f-c-c-in-defending-its-net-neutrality-rules/?ref=netneutrality. Accessed 15/03/2020
[123] Colin B. and Lara S. (2009) A Digital Future: Regulatory Challenges In A Brave New World: in (ed.) ITU Telecommunications Regulation Handbook Tenth Anniversary Edition P. 181
[124]*Ibid*

framework. Having the preceding pillars in place would support interoperable technologies that drive convergence and enable consumers to enjoy the benefits of convergence.

The contemporary challenge with convergence in Nigeria in contrast to other experienced market systems such as Europe is the reluctance to embrace regulatory convergence.

4.6.5 Computer-Generated Documentary Evidence

In 2011 a new *Evidence Act* was enacted to authorize the admissibility of "statements contained in a document produced by a computer as evidence".[125]The fact that computer-generated documents were previously inadmissible had made it difficult for the courts to make binding decisions on certain issues, especially those related to the ICT, and had created situations that dented the activities of government as well as private individuals in Nigeria. For instance, the Nigerian contract laws required that a contract should be oral or in writing, and did not contemplate the formation of electronic contracts.[126] Under the new regime, however, documents in electronic formats containing electronic signatures as verification, for instance, will freely be processed, thus closing the earlier legal vacuum.[127] The earlier judicial interpretations[128] on the admissibility of electronic documents created juridical confusion as there were conflicting decisions across various courts in the land, including the Supreme Court. Some confusion may still occur in the

[125] S 84(1) of the Nigeria Evidence Act of 2011.
[126]Udotai "Growth and Challenges of Information Technology" 234.
[127]The Nigerian Electronic Transactions Bill, 2015 has addressed the issue of e-contracts. The Bill proposes to facilitate the use of information represented in electronic media, regardless of the technologies employed, by giving electronic documents functional recognition.
[128] See the cases of **Nuba Commercial Farms Limited v NAL Merchant Bank Ltd 2002 24 WRN 157, 2003 FWLR (Pt 145) 661 CA**; and **EFCC v Fani-Kayode unreported** case of 2009, where the Court of Appeal and the High Court respectively held that hard copies of electronic documents could not be admitted as evidence under the Nigerian Evidence Act. Contrast this with the position of the Supreme Court in the cases of **Esso West Africa Inc v Oyegbola1969 1 NNLR 194 and Anyeabosi v RT Briscoe (Nig) Ltd 1987 3 NWLR (Pt 59) 84; 2 NSCC (Vol 18 Pt 2) 805**, where the Supreme Court held that hard copies of electronic documents were admissible as evidence. See also the case of **Ogolo v IMB (Nig) Ltd NWLR (Pt 419) 314 CA**, where the Court of Appeal held that copies of electronic evidence were admissible

interpretation of "computer" and "equipment" to include mobile phones for the purposes of admissibility.[129]

4.6.6 The Centrality of Telecommunications/ICT Services

From the legal purview a major challenge to the ICT system in Nigeria include the poor construction and unsatisfactory implementation of sector-specific (e.g. telecommunications) laws. This challenge results from interpreting the regulations through a narrow lens, a practice that is far removed from the fundamental principles that underlie the provision of telecommunications services.[130] For the purposes of leapfrogging development in transition economies such as Nigeria, the implementation of the principles of affordability, availability and accessibility has been considered crucial. Though service providers are primarily accountable for access to, the availability of and the affordability of telecommunications services, nonetheless the government is still under a statutory obligation to the guarantee integrity of the ICT legal environment and processes.

4.6.7 Privacy Concerns

The huge possibilities and benefits that accompany ICT deployment and indeed, convergence, have been obscured by an indifference to appropriate regulation on privacy. ICT in Nigeria is developing without a legal framework to protect the privacy of individuals in this rapidly evolving ICT environment. This was recently evident in the confusion that attended the telecommunications providers' (and later, the government's) attempts to capture subscribers' data during the SIM registration exercise. The confusion that attended the exercise would be largely traced to the lack of a framework -

[129]While mobile phones were not expressly mentioned under the Evidence Act, s.84 (5) (c) of the Act may have suggested their inclusion. The section provides that "a document shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment".
[130] Accessibility, availability and affordability.

authorisations, a database, locations, guidelines and procedures relating to the capturing, storage and retrieval of data. Given the many negative uses to which data can be applied, it is necessary to develop a credible regime for the management and regulation of access to the personal data obtained from telecommunications subscribers. In this regard it should be noted that Nigeria presently lacks a data protection law. Data protection refers to the protection of the privacy of personal data or information relating to any identifiable individual from all forms of threats and abuses;[131] such as unauthorised destruction, accidental loss and unauthorized access, alteration or dissemination of data.[132]

4.6.8 E-commerce and Internet Banking

E-commerce has to do with commercial transactions that take place electronically or by means of an electronic data interchange.[133] On the other hand, internet banking refers to the use of internet technologies in bank transactions. In this form of banking, customers access their accounts and general information on bank products and services through computers, mobile phones or other intelligent devices[134] after establishing a connection with the bank's computer system over the internet. Internet banking is a form of E-commerce. Presently in Nigeria e-commerce and internet banking have not been fully developed. Consequently, a limited range of e-commerce and banking services are offered through the internet in Nigeria.[135]

[131] See Article 2(a) of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981). See also the EU Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (1995).
[132] See A 7 of the Council of Europe Convention for the Protection of Individuals with regard to AU
[133]Salawu et al (2007) OECD Economic and Social Impact of Electronic Commerce 28. JILT490-496.
[134]Jayaram. J.,P. N. Prasad (2013), Review Of E-Banking System And Exploring The Research Gap In Indian Banking Context: *International Journal of Innovative of Research and Development* Vol 2 Issue 2 P.
[135]*ibid*

4.6.9 The Cyberspace and Copyright Infringements

There are questions about copyright application in the digital space. One of such question is, to what extent is the Nigerian Copyright Act applicable to the digital space? At what point, would copyright infringements be said to occur and who would be held liable for this? This poses challenges in the regulation of the cyberspace. This is clearer if the followings provisions of the Nigerian copyright Act are examined.

Use of Copy Right Work for the Blind, Hearing Impaired and otherwise Disabled

The Nigerian Copyright Act exempts from copyright protection, the reproduction of published work for the exclusive use of the blind or disabled persons.[136] In other words, through a process called reverse engineering, approved institutions can reproduce published work, sound recordings in a way that is accessible to the disabled without authorization from the copyright owner. In the context of the digital space, reverse engineering may require the circumvention of technology protection measures (TPM).

Technology protection measures are technologies used to control access to copyright content, or to prevent users from copying protected content. For example, a password is a technology protection measure and circumventing this may be akin to breaking into someone's house.

Parody, Pastiche and Caricature Online Parody, Pastiche and Caricature

The Nigerian Copyright Act exempts from copyright control, exaggerated and often humorous imitations of original work; where such imitations serve to mock, celebrate or are created solely for entertainment.[137]

[136] Second schedule to the Copyright Act LFN 2004
[137] *ibid*

Extensive content sharing on the internet has drastically amplified imitations of original work. Daily, video skits are produced that imitate an original work of art, either to celebrate such art or to mock it. There is no judicial interpretation from Nigerian courts of law that have tested the applicability of this provision to content shared on the internet. It would therefore be of great importance for this to be clearly distinguished from piracy which attracts civil and criminal liability.

It is advisable that for any proper judicial decision to be made, the purpose of the imitated work, the permissions granted by the copyright owner are useful considerations to take into account. Foreign legislation and judicial interpretation also serve as guidance for adjudicating on these matters.

Dealing with User-Generated Content

Online communities such as blogs, social networking platforms and sharing sites thrive on content generated by members of these communities. The members, who generate specific content, hold the copyright to the generated content. As "social" platforms, the terms of use on these platforms also give a non-exclusive license to the platform holders to share content posted on the platforms with others who use the platform. Through privacy settings and terms of use, the community members also agree to allow other uses of the platform access to the copyrighted material and permission to share with others; without further authorization required. In an instance where a user signs up to use a community platform and through available settings, agrees for his content to be shared by other users of the platform, a copyright infringement may be difficult to establish.

Therefore, activities in the cyberspace have made it difficult to ascertain when intellectual property right violation is said to have occurred, and to what extent the Nigerian Copyright Act can be considered to cover the circumvention of technology protection measures?

This chapter of the research work uncovered the fact that the devastating effects of threats to the national cyberspace have long been realized in Nigeria. This explains the several efforts that have been made from the early 1960s to grapple with this social malaise through the enactment of several legislations. Initially, these efforts were channelled through the existing Criminal and Penal Codes in order to handle offences relating to fraud perpetrated under whatever guise. However, the increased sophistication in the modalities of these crimes, and the perceived inadequacies in the existing laws, made it necessary to enact other statutory instruments to tackle the problem. Consequently, successive attempts have been made by way of enacting/proposing laws/bills as well as setting up different bodies and institutions cum policies to combat this devastating threat to the cyberspace. These various laws and institutions as well as current trends and challenges in the cyberspace, have been examined in this chapter.

4.6.10 Nigerian Data Protection Regulation 2019

This is one of the most recent attempts by the government to ensure personal data protection. The Regulation came into force on 25th January, 2019, and applies to all transactions intended for the processing of personal data, notwithstanding the means by which the data processing is being conducted or intended to be conducted in respect of natural persons in Nigeria. The regulation applies to natural persons residing in Nigeria or residing outside Nigeria who are citizens of Nigeria. It prescribes the minimum data protection requirements for the collection, storage, processing, management, operation, and technical controls for information and is currently the only set of regulations that contains

specific and detailed provisions on the protection, storage, transfer or treatment of personal data. The regulation applies to Federal, State and Local Government agencies and institutions as well as private sector organisations that own, use or deploy information systems of the Federal Republic of Nigeria, and also apply to organisations based outside Nigeria if such organisations process personal data of Nigerian residents. The NITDA Guidelines define "personal data" as:

> "means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others; ".[138]

Lawful Processing of Data

Under the regulation the processing of personal data shall be lawful if at least one of the following applies:1) Compliance with Legal Obligation; 2) Performance of a Contract with the Data Subject Consent of Data Subject 3) Protecting the vital Interest of the Data Subjectand 4) to Protect Public Interest (Preserving national security or preventing the outbreak of law and order)[139]

Consent of a Data Subject

The regulations provide that No data shall be obtained except the specific purpose of collection is made know to the Data Subject; Controller is under obligation to ensure that consent of a Data Subject has been obtained without fraud, coercion or undue

[138] Regulation 1.3, Nigerian Data Protection Regulation 2019(definitions)
[139] Regulation 2.2 , Nigerian Data Protection Regulation 2019

influence;[140]For such consent to be valid the conditions laid down by the regulation are that the consent must be freely given; it must be specific; distinguishable; informed; demonstrable; and there must be right of withdrawal[141]

Under Regulation 2.13, the rights of Data Subject include: Right of access to information about the propose of the processing, categories of data processed, period for which the data would be stored, the sources of the data(charged fees in some instances); Right of rectification of inaccurate personal data; Right to be forgotten: where the data collector continues the processing of those data without justification, the data subject can withdraw consent and demand erasure of their data; Right to restrict processing: where the data subject cannot demand erasure the data subject has the right to demand that the data can only be held by the controller, and may only be used for limited purposes; Right of data portability: the data subject has the right to receive in a structured, commonly used, machine-readable format that supports re-use, transfer or transmitted from controller to another, store it; Right to object processing: where the basis of processing is public interest or legitimate interest of the controller, data subject can object processing for direct marketing purposes; Right to communicate erasure; Right to be informed about all rights; Right to right of information relating to processing of data on request; and Right to be informed about reasons of delay or non-provision of information.

Data Security

Regulation 2.6 provides for data security. It provides anyone involved in data processing or the control of data shall develop security measures to protect data; such measures include but not limited to protecting systems from hackers, setting up firewalls, storing data

[140] Regulation 2.3 Nigerian Data Protection Regulation 2019
[141] *ibid*

securely with access to specific authorized individuals, employing data encryption technologies, developing organizational policy for handling personal data (and other sensitive or confidential data), protection of emailing systems and continuous capacity building for staff.

Data controllers (defined as persons which, alone or jointly with others, determine the purposes and means of the processing of personal data) are obliged to prevent any transfer of data to any country that does not ensure an adequate level of protection within the context of the NITDA Guidelines. The NITDA Guidelines also prescribe that in determining the adequacy of the level of protection afforded by another country in relation to the transfer of data, consideration must be given to the nature of the data, the purpose and duration of the proposed processing operation(s), the rules of law, both general and sectorial, in force in the receiving country in question and the professional rules and security measures which are complied with in that country, which should not be lower than the content of the Guidelines.[142]

The challenge with this regulation however is that the provisions of the regulation are, however, not mandatory for private companies and only serve as a point of reference for data collectors with respect to the minimum data protection requirements for the collection, storage, processing, management, operation, and technical controls of personal data. The implication is that the breach of the data regulation by a private company that is not within the legal threshold of the minimum data protection requirements is not an offence. This may limit the application and impact of the regulation.

[142] Regulation 2.11 Nigerian Data Protection Regulation 2019

CHAPTER FIVE:

SUMMARY

5.1 Summary

The increasing dependence upon information technology and network infrastructure has given rise to new and multifarious risks to national security, governance and business processes. The information technology regime has come under persistent threat of attack and sophisticated information warfare. Owing to the economic, political and social risks associated with a concerted cyber-attack on a nation, various governments globally have introduced regulations aimed at protecting and defending information of national importance. As a result of these extreme circumstances, securing the cyberspace has become a shared responsibility of governments, business, organizations, and individual users who develop, own, provide, manage, service and use these information systems and network.

This dissertation appraised the legal and policy framework regarding the cyberspace and information technology regime in Nigeria. This work has clarified the meanings of concepts such as cyberspace, cybersecurity, mobile security, internet security, Critical Infrastructure Security and information security. In order to properly assess Nigeria's readiness and vulnerability regarding the constant fight to secure the cyberspace, this work glances at the trends and international best practices by way of looking at global, regional, sub-regional and national treaties, practices, conventions, laws, policies, regulations and other instruments, which provide yardstick for evaluating the legal and policy readiness of Nigeria in managing the cyberspace and information technology.

In Nigeria, several internet assisted crimes known as cybercrimes are committed daily in various forms. There is the rise of politically motivated attacks; the rapid adoption of cloud services and the application programming interface (API) and its attendant cybersecurity threat; the prevalence of phishing attacks and the increasing malware attacks. According to the Nigerian Communications Commission in 2017, Nigeria ranked third globally in cybercrimes behind the United Kingdom and the United States. The realization of these challenges explains the several efforts made from the early 1960s to grapple with this social malaise through the enactment of appropriate legislations. This work has examined relevant legislations, which include the Nigeria Criminal Code Act, Wireless Telegraphy Act, the National Broadcasting Commission Act, the National Film and Video Censors Board Act, the Nigerian Communications Act, the Economic and Financial Crime Commission Act, Advance Fee Fraud and Related Offences Act, the National Information Technology Development Agency Act, Nigeria Deposit Insurance Corporation (NDIC) Act, Terrorism (Prevention) Act, Money laundering (prohibition) Act, The Lagos State Criminal Law, Evidence Act and the Cybercrimes Act.

This work has also appraised, the possibility of properly regulating the provision and usage of ICT and other services in Nigerian cyberspace; the adequacy of established Institutional Framework for cyber laws; the degree of international cooperation; enforcement mechanisms on criminal activities in the cyberspace; and the efficiency in handling the burden of multiple regulations of similar activities in the Nigerian cyberspace.

This research uncovered the fact that, though several efforts have been made by the government and private sector in Nigeria to tackle cyber threats. These efforts are not sufficient, given the dynamic and evolving nature of the cyber and ICT regime. It therefore becomes expedient that legislations in Nigeria need to keep pace with the speedy and rapid

changes occasioned by the cyberspace and information technology regime. Reforms are needed to meet the prevalent and sophisticated cyber challenges. Additionally, adequate awareness and security measures need to be in place and enforced, as part of the solutions to cyber threats.

5.2 Findings

This research work has made the following findings:

1. That it is difficult to properly and efficiently regulate the cyberspace owing to the dynamic nature of cyber related activities; electronic transactions give rise to the issue of jurisdiction and choice of law. This is ostensibly because the parties to the transaction may reside in different locations with different set of laws, and the fact that our laws have not developed enough to properly regulate cyber activities. In Nigeria, the Electronic Transaction Bill, the only bill on e-commerce, provides that an electronic communication is deemed to be sent from the sender's place of business and received at the addressee's place of business.[1] However, the Bill is silent on what happens where the only address provided is an email address, in which case, a determination of whether the applicable location should be that of the registrar for the "*url*" for the email account or that of the internet service provider from where the email is generated will be required.

2. Despite the fact that several laws and policies have been made, and institutions set to regulate the cyberspace in Nigeria, these efforts have not been adequate to properly tackle the constant threats to the cyberspace and the information regime. These shortcomings among others include the fact that Nigeria does not have any

[1] Section 19(4) Electronic Transaction Bill, 2015

officially recognized agency that offers institutional support on issues like child online protection.; Nigeria does not have any officially recognized agency that reports incidents related to child online protection; Nigeria does not have any officially recognised national or sector-specific research and development (R&D) Programs/Projects for cybersecurity standards, best practices and guidelines to be applied in either the private or public sector-however; Nigeria does not have adequate officially recognised national or sector-specific educational and professional training programs for training and raising awareness with the general public, promoting cybersecurity courses in higher education.

3. Laws like the Cybercrimes Act 2015 provide that Nigeria shall seek international cooperation in its fight against cybercrimes, notwithstanding, this research work has revealed that though several efforts have been made, and are being made, Nigeria has not adequately utilised international cooperation in its attempt to protect its cyberspace.
4. There are very few specialised enforcement mechanisms on criminal activities in the cyberspace. One of such few such bodies is the Nigerian Army Cyber Warfare Command. The command was created in August 2018, and it comprises 150 IT trained officers and men drawn from the corps and services in the Nigerian Army. The aim of the command is to monitor, defend and assault in cyberspace through distributed denial of service (DDoS) attacks on criminals, nation states and terrorists. Currently, there is no body, organization or entity set up by the government to investigate, monitor and to enforce cyber laws for the purpose of punishing cyber criminals or offenders. The impact of this entity is yet to be felt. Both the Cyber Crimes Act, 2015 and the Electronic transactions Bill are silent on the adjudication process of disputes relating to electronic transactions and the need

for a specialized court which will address issues relating to e-commerce. It is unarguable that in order to adjudicate on issues relating to electronic transactions whether as a practitioner or as an adjudicator, one must be knowledgeable in the intricacies and technical details of information and communications technology.[2]

5. Multiple-regulation (of the same aspects of telecommunications operations) by two or more Government Ministries, Departments and Agencies (**"MDAs"**), presents the hazard of regulatory intervention by these entities working at cross purposes to the detriment of the affected operator. It is common place for instance to have the premises of a telecommunications operator sealed by a different MDA, after being cleared by another, thereby disrupting the operations of such telecommunications operator. For instance, there was a fierce battle between NCC and NESREA as a result of the wide differences in setback to be provided for telecommunication masts and over who defines the setback, and which setback to comply with by telecoms firms wishing to site BTS. While the NCC 2009 guideline provide for 5 meter setback which NCC was implementing for telecoms operators before NESREA came into existence, NESREA on the other hand has insisted on 10 metre. This disparity has created regulatory conflict between these Federal Government agencies. A typical example was the sealing up of a telecom base station facility belonging to MTN at EFAB Estate, Mbora District, Abuja. NESREA had claimed that MTN failed to comply with proper Environmental Impact Act before installing the mast. NCC went to the site and unseal the facility, insisting that MTN had complied with its stipulated standard of five (5) meters away from a residential building. Soon after unsealing, NESREA went back to reseal the facility

[2]Aniaka O. (2017) *Analysing the Adequacy of Electronic Transactions Bill 2015 in Facilitating E-Commerce in Nigeria* available at: http://ssrn.com/abstract=2651120 accessed 06/06/2017 2;15pm

insisting that the NCC had opened the facility without lawful authority, insisting that the site violated its regulations of 10 meters setback from a residential area. This inter-agency conflict has given rise to court cases. One of such is the pending court of Appeal case in Appeal No: **CA/A/174/09- MTN Nigeria Communications Limited V. NESREA**. NESREA had sue MTN at the High Court of the FCT for none compliance with NESREA's regulation in suit **No: FHC/ABJ/CS/541/08- National Environmental Standards Regulations & Enforcement Agency (Nesrea) v MTNN**.NESREA's allegation was that MTN's mast was sited close to residential building. MTN raised a preliminary objection which the High Court overruled, hence, the interlocutory Appeal. These associated setbacks and bureaucratic bottlenecks present significant regulatory discords that affect activities in the cyberspace.[3]

5.3 Recommendations

As uncovered by this research, cyber-threats are definitely a threat to the economy of a nation, peace and security with particular reference to Nigeria. Therefore, there is need for a holistic approach to combat cyberspace and computer related crimes and ensure cybersecurity in all ramifications.

To this end, the researcher recommends the following as mechanisms to combat cyber and information related threats and ensure cybersecurity in Nigeria:

1. There should be significant and continuous efforts aimed at ensuring proper regulation of the cyberspace, provision and usage of ICT services and related

[3]Harlem (2019) Regulatory Framework and Environmental Standards for Telecommunications Masts and Towers in Nigeria, retrieved from https://www.harlemsolicitors.com/2019/10/12/regulatory-framework-and-environmental-standards-for-telecommunications-masts-and-towers-in-nigeria/ on 22/02/2020

activities in Nigerian. This can be achieved through review of existing criminal laws to reflect current realities, and amendment of the Nigerian Cyber Crime Act 2015 to address the dynamic nature of cybersecurity threats. All States should be encouraged to update their criminal laws as soon as possible, in order to address the particular nature of cybercrime. With respect to traditional forms of crime committed through the use of new technologies, this updating may be done by clarifying or abolishing provisions that are no longer completely adequate, such as where statutes are unable to address destruction or theft of intangibles, or by creating new provisions for new crimes, such as unauthorized access to computers or computer networks. Such updating should also include procedural laws (for tracing communications) and agreements or arrangements on mutual legal assistance (for rapid preservation of data). In the formulation of new legislations, States should be inspired by the provisions of the Council of Europe Convention on Cybercrime.

2. Nigeria should strengthen the few and weak legal and institutional framework established for the coordination and implementation of cyber laws; forensic laboratories should be established in all investigating units of law enforcement agencies; there should be progressive capacity building programmes for the law enforcement agencies on cybercrime and cybersecurity; there should be a symbiotic relationship between firms (most especially, Internet Service Providers), government and civil society to strengthen legal frameworks for cybersecurity.

3. International cooperation at all levels should be further enhanced. Given the universal character of cyber threats, Nigeria should cooperate with other Nations to ensure the functioning and protection of the cyberspace. Nigeria can learn from the

experiences of nations like the US, Russia, UK and Israel in framing policies and regulations the Cyberspaceas well the dealing with offenders.

4. The government should set up a robust enforcement regime for criminal activities in the cyberspace. Cyber police who are specially trained to handle cybercrimes should be established. The Nigerian police should have a Central Computer Crime Response Unit to act as an agency to advise the state and other law enforcement agencies, and to guide and coordinate computer crime investigation.

5. The Government must develop plans to tackle the challenges posed by multiple regulations of similar activities in the cyberspace by two or more government agencies in Nigeria. There must be a synergy between all government agencies whose roles concern the cyberspace and information technology. Governments, the private sector and non-governmental organizations should work together to bridge the digital divide, to raise public awareness about the risks of cybercrime and introduce appropriate countermeasures, and to enhance the capacity of criminal justice professionals, including law enforcement personnel, prosecutors and judges. For this purpose, national judicial administrations and institutions of legal learning should include comprehensive curricula on computer related crimes in their teaching schedules.

BIBLIOGRAPHY

TEXT BOOKS

Chukkol, K.S (2010) the law of crimes in Nigeria, (Revised ed)., ABU Press, Zaria.

Ladan M.T, (2015) Cyberlawand Policy on Information and Communications Technology in Nigeria Ahmadu Bello University Press Limited p 104.

Onoja E.O (2015) Fundamental Principles of Nigerian law, Green World Publishing Company, Akwanga, Nasarawa State, p.605

JOURNALS

Gercke (2010), Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, Computer Law Review International, p. 75

Goodman B. (2002), The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, 6(1) p. 70

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

Spagnoletti, P; Resca A. (2008). The duality of Information Security Management: fighting against predictable and unpredictable threats. Journal of Information System Security. 4 (3): 46–62.

Ehimen O.R & Bola A., (2010)"Cybercrimes in Nigeria*" Business Intelligence Journal*, January, Vol.3, No.1 p.95

Ehimen O. R, Bola A. (2010).Cybercrime in Nigeria. Bus. Intelligence. J. 3(1):26.

Ayofe A., Oluwaseyi funmitan O. (2009). Approach to Solving Cybercrime And Cybersecurity. Int. J. Computer. Sci. Inform. Security Vol. 3, No. 1.

Folashade B.O. et al, (2013) The Nature, Causes and Consequence of Cyber Crime in Tertiary institution in Zaria-Kaduna state, American International Journal of Contemporary Research, Vol. 3, No. 9, p.98

Ibikunle F., (2013) Approach to Cyber Security Issues in Nigeria: Challenges and Solution, Publication of Department of Electrical & Information Engineering, Covenant University Nigeria, Vol,1 No1 p1.

Akuta, E.A., etal (May 2011) Combating Cybercrime in sub-Sahara Africa: A discourse on law, policy and practice" Journal of Peace, Gender and Development Studies, Vol.1 No.4 pp 129-137 at p. 129.

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

Longe, O.B.& Chiemeke, S.C. (2008): Cybercrime and Criminality in Nigeria- *What roles are internet Access Points in Playing. European Journal of Social Sciences,* Volume 6 No 4.

Longe,O.B, Mbarika, V., Kourouma, M., Wada, F.&Isabalija, R., (2009) Seeing Beyond the Surface: Understanding and Tracking Fraudulent Cyber Activities. *International Journal of Computer Science and Information Security.* Vol. 6 (3) pp. 124-135.

Mu'azu A.S & Abubakar M.K., (2014) Cybercrime in Nigeria: An Overview of Cybercrime Act 2013*, Journal of Law, Policy and Globalization*, ISSN 2224-3240 (Paper) ISSN 2224 – 3259 (Online) Vol.32, p.23

Nfor, E. S. and Maimusa, H. (2007) "Nigerian National Security and the Challenges of Globalization 1999-2006", M*aiduguri Journal of Peace and Development Studies,* 1, (2), July-December, p. 80.

Okeshola F.B & Adeta A.K., (2013) The Nature, Cause and Consequences of Cybercrime in tertiary Institution in Zaria, Kaduna State, American International Journal of Contemporary Research, Vol. l3. No.9, p1.

Meza D., David and Webb, D. C. (2000) Does credit rationing imply insufficient lending? Journal of Public Economics, 78 (3). pp. 215-234. ISSN 0047-2727.

Okpaga, A. (2007) "Enhancing National Security in Nigeria through Non-Military Perspectives" in Dada, J. P. and Adejo, A. M. (Ed) *Opcit,* p. 84

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

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

Osborn H.Q., etal, (2012) Fighting Cybercrime in Africa; *Computer science and Engineering*, 2(6) 118-100 Doi 1-.5923/j computer20/20206.03. p.2 Published online at :http://Journalsapub.org/computer.scientific&Academic publishing 2012.

Oyewume, A.O. (2012) "The ICT Revolution and Commercial Sectors in Nigeria: Impact and legal interventions" *University of Ibadan Law Journal,* Vol.2, No.1, May, pp.201-223.

Selma Dilek, etal (2015) applications of artificial intelligence techniques to combating cybercrimes: a review, *International Journal of Artificial Intelligence & Applications* (IJAIA), Vol. 6, No. 1, January P.2.

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

Wada F. &Oduloja G.O., (2012) E-banking and Cybercrime in Nigeria: A Theoretical Policy Perspective on Causation, Afr J. of Comp & ICTs, Vol5, No1 P69.

Walker J. K. (2001) 'The demise of the nation-state, the dawn of new paradigm warfare, and a future for the profession of arms' Air Force Law Review (51:2001

UNPUBLISHED CONFERENCE/SEMINARS PAPER

Segun H. O. (2016) Cybersecurity, Women and Child Online Protection. A lead Paper Presentation delivered by at Women Leaders Forum organized by High-Tech Centre for Nigerian Women and Youth, December 1-2, Sheraton Hotel, Abuja.

Chiesa, R., (2011). 'Auditing the Hacker's Mind: The Hacker's Profiling Project. A Presentation by Chiesa Raoul at WINS International Best Practice Conference, Vienna, Austria.

Adomi, E. (2006). Application of Information and Communication Technologies (ICTs) in Nigerian High Schools. Warri: Nigerian Library Association, Delta State Chapter. AGM.

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

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

Anderson, J. M. (2003). Why we need a new definition of information security, Computers & Security, 22(4), 308–313.

Venter, H. S., &Eloff, J. H. P. (2003). A taxonomy for information security technologies, Computers & Security, 22(4): 299–307.

Ladan M.T., (2015) Overview of the 2015 Legal and Policy Strategy on Cybercrime and Cybersecurity in Nigeria, M.T Ladan's Law and Policy Review Research working Paper, May – August, p.10.

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

Ribadu, E., (2007) Cyber Crime and Commercial Fraud; A Nigerian Perspective; A Paper Presented at the Modern Law for Global Commerce, Vienna, 9th -12th July.

The Concept of Information, Communication and Educational Technology and Communication Technology. M.A Education (part II) Group B-Paper-VII. Institute of Distance and Open learning, University of Mumbai

Garner A. B., (2009) Black's Law Dictionary 8th ed. p 414.

INTERNET

Marco M., etal (2014) Draft Pisa, https://www.academia.edu/7096442/ How would _you_ define_ Cyber space.

John, P. B. (1990) Crime and Puzzlement,http://www.carriaghen.com/2011/02/what-exactly-is-cyberspace-and-cybersecirity.

Strate, L. (1999). The varieties of cyberspace: Problems in definition and delimitation. Western Journal of Communication. 63 (3): 382–3. http://www.carriaghen.com/2011/02/what-exactly-is-cyberspace-and-cybersecirity

Anah, B.H., etal(2012) Cyber Crime in Nigeria: Causes, effects and the way out. ARPN Journal of Science and Technology, 2 (8) 626, http:/www.ejournalofscience.org

Brenner,(2004) Cybercrime Metrics: Old Wine Bottles? Virginia Journal of Law and Technology Vol.9, available at www.vjolt.net/Vol9/issue4/v9i4 - a13 -Brenner.pdf.

PrincipiaCybernetica"Cyberspace"https://en.wikipedia.org/wiki/cyberspacehttp://www.carriaghen.com/2011/02/what-exactly-is-cyberspace-and-cybersecirity

John P. B. (1990), Crime and Puzzlement retrieved from http://www.carriaghen.com/2011/02/what-exactly-is-cyberspace-and-cybersecirity

Kramer, F.D and Starr S. and Wentz L.K. (ed.) (2009),Cyberpower and National Security, National Defense University Press, Washington retrieved fromhttps://www.academia.edu/14336129/International_Politics_in_the_Digital_Agehttp://www.carriaghen.com/2011/02/ what-exactly-is-cyberspace-and-cybersecurity

Graham M. Geography/Internet: Ethereal Alternate Dimensions of Cyberspace or Grounded Augmented Realities. The Geographical Journal, 179(2): pp. 177-188.http://www.carriaghen.com/2011/02/what-exactly-is-cyberspace-and-cybersecirity

Flew, T.(2011) New Media: an Introductionhttp://www.carriaghen.com/2011/02/what-exactly-is-cyberspace-and-cybersecirity

Bruce S., Introduction to the Hacker Crackdown https://.wikipedia.org/wiki/computer-security.

Chawki, M. (2009) Nigeria tackles Advance Fee Fraud*; in Journal of Information, Law and Technology* (JILT), May 28, 2009. Accessed from http://go.warwick.ac.uk/jilt/2009-/chawki on 9/7/2016, p.13

Morningstar, C. and Farmer F. R. (2003)The Lessons of Lucasfilm's Habitat In: Wardrip-F. and Nick M. (Ed.) The New Media Reader. The MIT Press. PP. 664-667. Printhttp://www.carriaghen.com/2011/02/what-exactly-is-cyberspace-and-cybersecirity

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

Gillespie A., (2007) Cybercrime: *Key Issues and Debates* (Routledge 2016) Chapter 1; I Walden, *Computer Crimes and Digital Investigations* (Oxford University Press).

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

Abraham D. S. David C, Whitfield D. (2009) Cyber Security and International Agreements, Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy http://www.nap.edu/catalog/12997.html

Gordon/Ford, On the Definition and Classification of Cybercrime, *Journal in Computer Virology,* Vol. 2, No. 1, 2006, page 13-20; *Chawki,* Cybercrime in France: An Overview, 2005, available at: www.crimeresearch. org/articles/cybercrime-in-france-overview;

Gordon, L., Loeb, M. (2002). The Economics of Information Security Investment: ACM Transactions on Information and System Security. 5 (4): 438–457 retrieved from https://en.wikipedia.org/wiki/information-security

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

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

Lunker Manish:*Cyber Laws: A Global Perspective pg. 2(An article from Internet) See*http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN005846.pdf.Accessed on; 22 November 2015. 21:52:15.http://www.rediff.com/netguide/index.htmlaccessed on 01.12.2015.

Maitanmi Olusola et al, 'Impact of Cyber Crimes on Nigerian Economy*', the International Journal of Engineering and Sciences (*IJES) Volume 2, Issue 4, p. 47. ISSN 2319-1813. Available at http://www.theijes.com/papers/v2i4/part.%20%284%29/H0244045051.pdf. Accessed on 23/12/2015.

Meke E.S.N. (2012), Urbanization and cybercrime in Nigeria: Causes and Consequences: ARPN *Journal of Science and Technology*, 2 (8) 631, http:/www.ejournalofscience.org.

Nojeim, G.T. (2009), Cybersecurity: *Preventing Terrorist Attacks and Protecting Privacy in Cyberspace. Statement Before the Senate Committee on the Judiciary, Subcommittee on Terrorism and Homeland Security.* Oxford Dictionaries (2013, June) online available *at http://oxforddictionaries.com*.www.itu.int/en/ITUT/studygroups/com17/pages/cybersecurity.aspx. accessed on 19/12/2015 at 2:04pm.

Olugbodi, K., Fighting Cyber Crime in Nigeria, retrieved 10/08/15 from http//:www.guidenigeria.com/news_articles_about_nigeria, by5:35pm

Oyesanya., (2015) F. A performance Review of EFCC and the Nigerian Cybercrimes Working Group.' Accessed from http://www.nigeriavillagesquare.com/article/femi-oyesanya/...html on June 6, 2015, p.3

Smith, R.G., Holmes, M.N. & Kaufmann, P. (1999): Nigerian advance fee fraud. *Trends and Issues in Crime and Criminal Justice,* No. 121. Australian Institute of Criminology, Canberra. Available online at *http://www.aic.gov.au* accessed on 20/12/15 at 10:00am.

Oxford Dictionary www.oxforddictionaries.com/definition/english/telencies

NEWSPAPERS

Abdullahi, T. A., Hamza, I., Yahaya, I., Hamisu, K. M., and Zakariyya, A (2013). *"Cell phone service cut in Borno, Yobe",* Daily Trust Newspaper, May 17, 2013.

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

Ahmed, I. (2008) Nigeria: N10 Billion Lost to Bank Fraud in 2007 – *NDIC, Daily Trust,*28 October 2008

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

Muhammed, H., (2009) 'NCC Clamps down on Illegal ISPs, Cyber Cafes, '*Daily Trust*. Monday, February 23, *pp.55*

Swire, Peter & Hemmings, Justin. (2015) "Re-Engineering the Mutual Legal Assistance Treaty Process," presented at *Berkeley Center for Law and Technology Privacy Law Scholars Conference,* p. 11.

This Day Newspaper, "Non-Passage of Cyber Crime Bill Decried." Retrieved *fromhttp://www.thisdaylive.com/articles/non-passage*-of-c*yber-crime-bill-decried/88750/, published on March 31, 2011.*