A STUDY ON THE RELEVANCE OF BUDAPEST CONVENTION ON CYBERCRIME IN NIGERIA

BY

ABDULLAHI MU'AZU SAULAWA

A thesis submitted in fulfilment of the requirement for the degree of Doctor of Philosophy in Law

Ahmad Ibrahim Kulliyyah of Laws
International Islamic University Malaysia

SEPTEMBER 2018

ABSTRACT

This research focuses on the relevance of the Budapest Convention on Cybercrime in Nigeria and more particularly on the substantive criminal law offences in the Convention. The Internet and computer devices are increasingly being used as tools for committing local and international crimes at alarming rates and in every facet of society. This research analyses the relevance of the Nigerian laws on Cybercrime and how effective this laws are in terms of combating the crimes in Nigeria. The research also analyses the provisions of substantive criminal offences in the Budapest Convention with an effort to strengthen the Nigerian Cybercrime act 2015. The Nigerian Cybercrime Act is the existing legal framework meant to combat cybercrimes in Nigeria. This is evident from the manner in which the Internet has shaped human life and communities across the globe. The research objectives centre on the analysis of the theories of cybercrime and the classes of cybercrimes which are prevalent in Nigeria. The research also analyses the substantive criminal law offences in the Budapest Convention on Cybercrime, including the European Union Directive on Cybercrime as complement as well as the regional Convention on Cybercrime which cover African Union Convention and ECOWAS Directive. The research analyses the Shariah principles dealing with various classes of cybercrimes in Nigeria. The methodology mainly adopted in this research work is a doctrinal approach. However, the research made use of limited qualitative research methods by using structured and semi-structured interviews to elicit original feedback from respondents. The research reveals that most Nigerian citizens, parliament, stakeholders are not aware of the scope of cybercrime or the relevance of the Budapest Convention on Cybercrime in Nigeria. The thesis recommends that the government should, through the relevant institutions, enlighten the public to the menace of cybercrime and proposed few amendments to the existing Cybercrime Act 2015, in order to match with the realities of current practices. Furthermore, by adopting the Budapest Convention as a possible guide for Nigeria, it will help strengthen the legal framework in combating cybercrimes in the country.

ملخَّص البحث

يركز هذا البحث على أهمية اتفاقية بودابست بشأن الجريمة الإليكترونيّة في نيجيريا، ولا سيما فيما يتعلق بالجرائم الموضوعيّة للقانون الجنائي في الاتفاقية. ويجري استخدام الإنترنيت وأجهزة الكومبيوتر على نحو متزايد بوصفها أدوات لارتكاب جرائم محليّة، ودوليّة بمعدلات تنذر بالخطر وفي كل جانب من جوانب المجتمع. ويحلل هذا البحث الأثر المدمر للجريمة الإليكترونيّة في بيئة التكنولوجيا الرقميّة المعاصرة. ويتضّح ذلك من الطريقة التي شكّلت بها الإنترنيت الحياة البشريّة والمجتمعات في جميع أنحاء العالم. وتتركز أهداف البحث على تحليل نظريات الجريمة الإليكترونيّة، وتصنيف الجرائم الإليكترونيّة المنتشرة في نيجيريا. ويحلل البحث أيضًا الجرائم الموضوعيّة للقانون الجنائي في اتفاقية بودابست بشأن الجريمة الإليكترونيّة، بما في ذلك توجيه الاتحاد الأوروبي بشأن الجريمة الإليكترونيّة باعتباره مكملاً. كما يتناول التقرير التشريعات النيجيريّة ذات الصلة بالجرائم الإليكترونيّة، فضلاً عن الاتفاقية الإقليميّة بشأن الجريمة الإليكترونيّة التي تشمل اتفاقية الاتحاد الإفريقي وتوجيه الجماعة الاقتصادية لدول غرب إفريقيا. ويشرع البحث في تحليل المبادئ الشرعيّة التي تتناول الجرائم الإليكترونيّة المصنّفة في نيجيريا. المنهجيّة المعتمدة أساسًا في هذا البحث هي اتباع المنهج النوعي. ومع ذلك، فقد تناول الباحث أيضًا طرق بحثٍ مختلفة محدودة باستخدام المقابلات المنظمة، وشبه المنظمة لاستخلاص البيانات الأصلية من المستجيبين. وتكشف نتائج البحث أنَّ معظم المواطنين النيجيريين، والبرلمان، وأصحاب المصلحة ليسوا على بينة من نطاق الجريمة الإليكترونيّة، أو أهمية اتفاقية بودابست بشأن الجريمة الإليكترونيّة في نيجيريا. وعلاوة على ذلك، فإنَّ اعتماد اتفاقية بودابست بوصفها أنموذجًا تشريعيًّا محتملاً لنيجيريا سيساعد على تعزيز الإطار القانوني لمكافحة الجرائم الإليكترونيّة في البلد. وتوصي الأطروحة بأنْ تقوم الحكومة من خلال المؤسسات ذات الصلة، بتوعية الجمهور بخطر الجريمة الإليكترونيّة، وتقترح تعديلات طفيفة على قانون الجرائم الإليكترونيّة لعام 2015م، لكي تتناسب مع واقع الممارسات الحالية.

APPROVAL PAGE

The thesis of Abdullahi Muazu Saulawa has been approved by the following:

_____
Sonny Zulhuda
Supervisor

_____
Suzi Fadhilah Ismail
Co-Supervisor

_____
Ida Madieha Abdul Ghani Azmi
Co-Supervision

_____
Juriah Abd. Jalil
Internal Examiner

_____
Mohammed Lawal
External Examiner

_____
Mohamad Rizal Abdu Rahman
External Examiner

_____
Ismaiel Hassanien Ahmed
Chairperson

DECLARATION

I hereby declare that this thesis is the result of my own study, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Abdullahi Muazu Saulawa:

Signature……. Date ….....

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

A STUDY ON THE RELEVANCE OF BUDAPEST CONVENTION ON CYBERCRIME IN NIGERIA

I declare that the copyright holder of this dissertation are jointly owned by the student and IIUM

By signing this form, I acknowledged that I have read and understand the IIUM Intellectual Property Right and Commercialization policy.

Affirmed by Abdullahi Muazu Saulawa

……..……..…… ……..

Signature Date

This research work is dedicated to my Parents:
Professor Abdullahi Mu'azu Saulawa and Bilkisu A. M. Saulawa.
My lovely wife Aisha and my son Ahmad.
My brothers, sisters and my family.

ACKNOWLEDGEMENTS

All praise is due to Allah, the First without beginning and the Last without end. May His peace and blessing be upon His most superior creature, His Messenger Muhammad (S.A.W), members of his household and His Companions.

In undertaking this research, I owe an immense debt of gratitude to my supervisor, Dr. Sonny Zulhuda for his supervision, expertise, guidance afforded to me. My gratitude to the supervisor cannot be measured nor quantified because his words of encouragement were inspirational tools for my life in Malaysia. Without hesitation, I can attribute the success in the completion of this research work to him. The periods of supervision allocated to me are enormous.

My gratitude goes to my Co-Supervisor Dr. Suzi Fadhilah Ismail who has kindly gone through this thesis and given his invaluable comments. The advice given to me for developing the research has helped to boost to my confidence in carrying out the study. I also extend my gratitude to my Chairman, Prof. Ida Madieha Binti Abdul Ghani Azmi, who has gone through this work and rendered useful suggestions. She was there guiding and assisting me throughout the research and since the first time I came to this University.

I would like to thank Prof. Dr. Muhammad Naqib Ishan Jan, (Dean, Postgraduate Unit), Ahmad Ibrahim Kulliyah of Laws, IIUM for his fatherly advice and encouragement whenever I visited him. He made my life in the Postgraduate office, AIKOL wonderful. Further appreciation goes to the Prof. Mu'uta Ibrahim, former Vice-Chancellor, Umaru Musa Yar'adua University, Katsina-Nigeria for the award of PhD Fellowship. Equally, my appreciation goes to the management of Umaru Musa Yar'adua University, Katsina-Nigeria for processing my papers from the point of my fellowship application to the end of completing the research work.

I am grateful to the Faculty of Law, Umaru Musa Yar'adua University, Katsina-Nigeria for the courage given to me whilst studying, Prof. A. I. Bappah approved my application at the initial stage, for which I am truly grateful. Irfan and Abdullahi father inspires me to choose this specialty, and as such has made a tremendous impact on my versatility of knowledge: from human rights, international law, corporate law to copyright law and information technology law. He always spared time for my calls and emails in relation to academics, advice and instant responses. The research work could not be completed without your tremendous input.

I am also grateful to the academic staff and non-academic staff in the Faculty of Law, Umaru Musa Yar'adua University, Katsina-Nigeria. The Dean, Prof. A. S. R. Matazu is always there guiding my interest in the pursuit of this research, the Secretary to the Dean and the entire academic and non-academic staff in the Faculty of Law. I wish to record my gratitude to my brothers, Mahmud A.S., Ph. D, Mubarak A.S, Lukman A.S, Hafiz A.S.(May his soul rest in peace) and sisters, Hikmat A.S, Hajara A.S, Hafsat A.S and the younger ones. I also appreciate the advice of Prof. Dr. Rabi'u Umar in the entire research and Nura Magaji K/Soro for their prayers.

My appreciation also goes to Muhammad Fodio, Dr. Binta Dalha (Mrs), Samaila Isa, Mansir Bello, Zaharadeen Salisu Maska, Junaidu Bara'u, Abdulrahman Hassan, Ismail Zubairu, Jafar, Iro Barda, Kabir Usman UMYU, Alh. Sani (NITDA), Mal. Hassan Sada (NUC), Qasim Zargar, Idris Abubakar ESQ. My colleagues at IIUM. Dr. Mahdi Adamu, Dr. Ibrahim Danjuma, Dr. Garba Umaru Kwagyang, Dr. Muhammad Musa Saleh and Michael Kayang Esq.

TABLES OF CONTENTS

LIST OF TABLE

LIST OF STATUTES

Advance Fee Fraud and Other Fraud Related Offences Act No. 13 of 1995 as amended by Act No. 62 of 1999
Advance Fee Fraud and Other Fraud Related Offences Act of 2006
African Union Convention on Cybersecurity and Personal Data Protection
Budapest Convention on Cybercrime 2001
Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030
Computer Misuse Act 1990 (U. K)
Constitution of Federal Republic of Nigeria 1999, Amended
Copyright Act
Copyright, Designs and Patents Act 1988
Criminal Procedure Code
Cybercrime (Prevention, Prohibition etc.) Act 2015
Cybersecurity Information Sharing Act (CISA S. 2588), 2015
E U Directive on Attacks against Information Systems
ECOWAS Directives on fighting cybercrime
Evidence Act amended 2011
National Information Technology Development Agency Act 2007
Nigerian Communications Act 2003
Patriot Act 2001
Penal Code Act
Senior Courts Act 1981
Serious Crime Act of 2007

LIST OF CASES

LIST OF ABBREVIATIONS

A U	-	African Union
AFF	-	Advanced Fee Fraud
ATM	-	Automated Teller Machine
ALL- FWLR	-	All Federation Weekly Law Report
BVN	-	Bank Verification Number
CAC	-	Cybercrime Advisory Committee
CBN	-	Central Bank of Nigeria
CoE	-	Council of Europe
CTO	-	Commonwealth Telecommunications Organization
CRT	-	Criminal Transaction Report
CERT	-	Centre Emergency Response Team
DOS	-	Denial of Service
E U	-	European Union
EBSU	-	Ebonyi State University
EFCC	-	Economic Financial Crimes Commission
ECOWAS	-	Economic of West African States
FBI	-	Federal Bureau of Investigation
FRN	-	Federal Republic of Nigeria
GTB	-	Guarantee Trust Bank
GDP	-	Gross Domestic Product
ICT	-	Information and Communication Technology
ITU	-	International Telecommunication Union
ISP	-	Internet Service Providers
INEC	-	Independent National Electoral Commission
IITF	-	Information Infrastructure Task Force
JCA	-	Justice of the Court of Appeal
LEA	-	Law Enforcement Agencies
LPELR	-	Law Pavilion Electronic Law Report
MPO	-	Mobile Payment Operators
MMIA	-	Murtala Muhammad International Airport
N A	-	National Assembly
NCC	-	Nigerian Communication Commission
NSA	-	National Security Agency
NSA	-	National Security Adviser
NCII	-	National Critical Information Infrastructure
NDIC	-	National Deposit Insurance Corporation
NASA	-	National Aeronautics and Space Administration
NYSC	-	National Youth Service Corps
NITDA	-	National Information Technology Development Agency
NDLEA	-	National Drugs Law Enforcement Agency
NIBSS	-	Nigerian Inter-bank settlement scheme
OTT	-	Over The Top
OFI	-	Other Financial Institution
ONSA	-	Office of the National Security Adviser
POS	-	Point of Sale
PVC	-	Permanent Voting Card
PBUH	-	Peace Being Upon Him

RAT	-	Routine Transition Theory
SME	-	Small Medium Enterprise
SMS	-	Short Messaging service
STT	-	Space Transition Theory
STR	-	Suspicious Transaction Report
U S	-	United States
U K	-	United Kingdom
UN	-	United Nations
USD	-	United States Dollar
USNRC	-	United States Nuclear Regulatory Commission
USDOE	-	United States Department of Energy
USDOJ	-	United States Department of Justice
UNODC	-	United Nations Office on Drugs and Crime

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND TO THE RESEARCH

This study focuses on the relevance of the Budapest Convention on Cybercrime (which is popularly known as the "Budapest Convention") in Nigeria for the purposes of strengthening the Nigerian Cybercrime Act 2015. The Budapest Convention is useful to the nations as a prototype in establishing a legal framework for combatting cybercrimes. The study will examine the Budapest Convention as a guide in establishing its importance to curb cybercrime in Nigeria and more particularly, in analysing the substantive criminal offences of the Budapest Convention in order to improve the Nigerian's legal framework on cybercrime.

The Budapest Convention was established by the Council of Europe for the purposes of criminalising offences that come under information technology and other related matters across the globe. The offences under information technology are referred as to cybercrimes. Cybercrimes are offences that are perpetrated through the medium of computer and other related devices.

The focal point of the research is that on cybercrimes that are committed using the Internet. The categories of cybercrimes are, firstly crimes related to computer data and system (confidentiality, integrity and availability) which covers unauthorised access.[1] Secondly- crimes related to content covers cyber pornography, cyberstalking and cyber defamation.[2] Thirdly-crimes related to copyright and trademark covers online

[1] International Telecommunication Union, "Understanding Cybercrime: Phenomena, Challenges and Legal Response", prepared by Prof. Dr. Marco Gercke and is a new edition of a report previously entitled Understanding Cybercrime: A Guide for Developing Countries, (2012), p.16 , available at<https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf, aaccessed on 3/3/2014.

[2] *Ibid*, p. 21.

copyright and trademark infringement and software piracy.[3] Finally, crimes related to computer which covers identity theft and credit card fraud.[4]

The category of cybercrime includes unauthorised access, cyber pornography, cyberstalking and cyber defamation, online copyright and trademark infringement and software piracy. The most prevalent in Nigeria are identity theft and credit card fraud.

Cybercrimes in Nigeria are committed within and outside the country. The crimes are committed at great speed so that the crime spreads fast. Hence, the government faces many challenges in establishing a coherent legal framework to regulate crimes.

The Budapest Convention provides a legal framework that could be used by the nations in establishing the legal framework on cybercrimes. The Budapest Convention is divided into three segments: substantive criminal offences, procedures and international cooperation. However, the Budapest Convention addresses various offences that are prevalent in the Nigerian cyber domain.

The research examines related cybercrimes that are prominent in Nigeria, as well the scope of the existing Nigeria's Cybercrime Act, 2015 for the purpose of strengthening the Act. It is also imperative to analyse the structure of the Budapest Convention for the purposes of identifying its significance in relation to Nigeria's cybercrime problem and to determine their applicability to Nigeria. As such, it would enhance and greatly affect Nigerian cybercrime laws, as well as improve its relationship with the international community by ultimately implementing new measures to reduce cybercrime in Nigeria.

The increasing use of information and communication technology (ICT) enables businesses and individuals to communicate and engage in transactions with other parties electronically, instantaneously and internationally. This gives rise to a variety of legal

[3] *Ibid*, p. 27.
[4] *Ibid*, p. 29.

and regulatory issues for policymakers, from the validity of electronic methods of contracting and security risks associated with them, to concerns over cybercrime and the ability to protect intellectual property rights. Therefore, ICTs policymakers constantly facing challenges in dealing with these issues. The campaign conducted by relevant stakeholders to nations was to harmonise their local laws and reforms where relevant, as such, that it would facilitate the sound development of electronic commerce and related activities, and to ensure the rights of citizens are protected against any harmful act that may arise.

The application of electronic transactions or commerce has brought with it a number of legal and social-economic issues and has raised the significant challenge to police the Internet where cybercrime takes place. From the modest beginnings in the 1990's, internet penetration and use have continued to grow in Nigeria,[5] and apart from its impact in the banking and commercial sectors, it has also become very popular as a means of communication, through the electronic mail system, as well as means of generally accessing news and information.

Currently, the number of the internet users in Nigeria has increased which also supports the increase in cybercrimes. The number of internet users is 86, 219, 965 million. This constitutes 46.1 per cent of the Nigerian population of 186, 987, 563 Million.[6] With the number accumulating, there is a need to ensure the existing legal framework on cybercrime is strong and fully implemented in the country.

Furthermore, by way of another analogy, the importance of ICT in the communal setting has been advanced for instance, in the health sector. It has impacted on many diverse aspects of medical care, including the provision of medical information,

[5] According to latest internet usage statistics for Africa, as at 31st March, 2011, Nigeria had 43, 982,200 internet users, representing 28% of the population in Nigeria. The figure constitutes 37% of users in Africa. See Internet World Stats: Usage and Population Statistics, online at <http://www.internetworldstats.com/stats1.htm>, accessed 25/10/2011.

[6] Internet Users by Country, available at http://www.internetlivestats.com/internet-users-by-country/, accessed on 12/10/2015.

diagnosis and treatment, as well as the training of medical personnel.[7] Despite the positive aspects of ICT, it poses a major challenge to the legal institution of the country to address cybercrime.

The practice of advanced fee fraud is another dynamic set of cybercrime in Nigeria. It is also known as the "419 scam" which is named after the section of the Nigerian Criminal Code dealing with the crime of obtaining property by false pretence.[8] The 419 scam combines impersonation fraud with a variation of an advanced fee scheme, and relies on letters, emails, or faxes to potential victims from individuals representing themselves as government officials, offering the recipient the "opportunity" to share in a percentage of millions of dollars, while soliciting for help to place large sums of money in overseas bank accounts.[9]

The activities of cybercrime constitute dangerous acts committed through the use of a computer or network and its application differs in the types of crimes. The crimes are easily learnt and committed in a manner that a perpetrator remains invisible.[10] Cybercrime is the most common form of covert crime, largely unseen but highly powerful to visualize the network resources of individuals. Computers and other devices become the major sources of dissemination of information among the criminals as their central focus target for profit.[11]

---

[7] "Technology and Medicine." available at http://www.123HelpMe.com/view.asp?id=27669, accessed on 01/9/2017.

[8] Section 419 of the Nigerian Criminal Code, Cap C38, Laws of the Federation of Nigeria, 2004, which provides: "Any person who by any false pretense, 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..."

[9] See the International Crime Complaint (IC3) Centre, online at <http://www.ic3.gov/crimeschemes.aspx#item-13>, accessed 15th October, 2011.

[10] "Cyber Crime… and Punishment? Archaic Laws threaten Global Information", A Report prepared by McConnell International, (December 2000), p. 2-3.

[11] International Telecommunication Union, "Cybersecurity Guide for Developing Countries", Edition (2007), at 33.

At the global level, the increase in cybercrimes is widespread, targeting financial industries and applied to other computer-content related crimes against the confidentiality, integrity and accessibility of computer systems.[12]

1.2 STATEMENT OF THE PROBLEM

The research intends to examine the existence and adequate application of the legal framework to curb cybercrime in Nigeria, having considered that criminals are consistently infiltrating cyberspace with a wide knowledge in the field of ICT and its versatility. The relevance of the Budapest Convention in Nigeria's context is an important part of the research because it would be used as a guide in improving the provisions of Nigeria Cybercrime Act 2015. Cybercrimes in Nigeria are committed in and outside the country and this research expects that Convention will serve as a guide in addressing Nigerian cybercrime problems.

A major challenge is that Nigeria's Cybercrime (Prohibition, Prevention etc.,) Act 2015 is a new piece of law, having been passed by the Senate of the National Assembly in 2015 and assented to by the President. It has not been practically tested in law courts and there is no extensive jurisprudence on the subject in Nigeria.

The real issue concerning the Nigerian Cybercrime Act 2015 is that the government is slow in implementing the law; perhaps there is no political will to do that. As such requires some analysis for the purposes of finding the possible loopholes. The Act does not provide for the establishment of a Commission meant to handle the responsibility of the law and lack of such will render the objectivity of the Act insufficient.

The practices and abuses of ATM cards, online transaction crimes, fraud messages, and the critical national information infrastructure collectively constitute one

[12] United Nations Office on Drugs and Crime, "Comprehensive Study on Cybercrime", Draft, (February 2013), at xviii.

aspect that requires the full and immediate attention of the government. The case of the Independent National Electoral Commission (INEC) during the general election on March 23, 2015, is the latest example, where the INEC websites was hacked on the general election day[13] and it was subsequently restored.[14] This also presents a threat to the nation.

The activity of cybercafés without legal authorisation assists in the dissemination of fake information regarding government institutions. For instance, there is a number of government institutions purportedly engaged in job recruitment through the Internet although the advert was not initiated by the government agency. This is an intrusion to the websites without authorization and therefore amounts to an offence.

It is not every operator is aware of this regulation and procedure and this supported the perpetration of crimes from different corner. In addition, these prominent crimes in Nigeria, such as unauthorised access, cyber pornography, cyberstalking and cyber defamation, online copyright and trademark infringement and software piracy, have fundamental effects on the Nigerian economy and also have resulted into property and personal harm.

The expense of cybercrime is colossal and has resulted in the loss of billions of dollars. The United Nations Office on Drugs and Crime (UNODC) estimates that about $ 1 billion was stolen by identity thieves per year globally. In another estimation, online traders lost $3.5 billion due to fraud activities in 2012. The Center for Strategic and International Studies estimates that cybercrime and intellectual property theft was detrimental to the U.S. economy with an approximate loss of as much as $100 billion per

[13] Micheal Abimboye, "INEC website hacked", Premium Times Newspaper, available at http://www.premiumtimesng.com/news/top-news/179539-inec-website-hacked.html., accessed on 28/3/ 2015,

[14] Channels TV, "INEC Restores Hacked" available at http://www.channelstv.com/2015/03/28/inec-restores-hacked-website/. In an update news, accessed on 28/3/ 2015.

year. The amount lost is very high. This has a consequential effect on the economic value to abridge the trust in the Internet due to online crime.[15]

A recent update by the Federal Government of Nigeria projected that the annual cost of cybercrime to Nigeria is 0.08 per cent of the country's Gross Domestic Products (GDP), which represents about N127 billion. The National Security Adviser (NSA) further said that in an annual report by the Nigeria Deposit Insurance Corporation (NDIC) in 2014, between 2013 and 2014, the practices of fraud on the e-payment platforms of the Nigerian banking sector has increased by 183 per cent. In addition, another report by the Centre for Strategic and International Studies, UK, published in 2014 the projected the annual cost of cybercrime to Nigeria stood at about 0.08 per cent of its GDP totalling about N127 billion.[16]

These are all serious acts of fraudulent activities as a result of unsecured online activities. This insecurity in the online activities allows criminals to continue defrauding innocent citizens from their hard earnings while at the same time it is clear that there are no adequate laws to check-mate these fraudulent processes.

These are serious threats to the government, which have to be taken seriously. Where the government fails to act or apply the correct legal and institutional measures, the risk of the outcome will affect government national security.

---

[15] Office of the Coordinator For Cyber Issues (S/CCI) United States Department of State, "Cybercrime" Designed and Printed BY A/GIS/GPS AUGUST 2015, available at https://www.state.gov/documents/organization/255007.pdf, accessed on 20/7/2016.

[16] This was disclosed by the national security adviser (NSA), Maj-Gen. Babagana Munguno (rtd) on Monday during the inauguration of the cybercrime advisory council, at the office of NSA, Abuja. as reported by senator Iroegbu in Abuja, Thisday Newspaper, "Nigeria loses over n 127 bn annually through cybercrime", dated on April 19, 2016, available at http://www.thisdaylive.com/index.php/2016/04/19/nigeria-loses-over-n127bn-annually-through-cybercrime/, accessed on 20/10/2016 . In another statement quoted the NSA that "global tracking of cyber-attacks indicates that Nigeria is among countries with high cases of software piracy, intellectual property theft and malware attacks. the situation is a serious challenge to our resolve to take advantage of the enormous opportunities that internet brings, while balancing and managing its associated risks." and that "the situation was made possible due to lack of awareness of cyber-security and poor enforcement of guidelines and minimum standards for security of government websites, particularly those hosting sensitive databases of Nigerians". *Ibid.*

According to the head of NSA, Babagana Munguno, that there is the need to take immediate action after having understood the seriousness of cybercrime in order to effectively protect the national cyberspace as a national security requirement.[17]

The perpetration of cybercrimes across the nation has contributed to economic loss. It is in this context that the current research is aimed at examining the legal perspective and the significance of the Budapest Convention in Nigeria as a way of addressing these heinous cybercrimes.

1.3 HYPOTHESIS OF THE RESEARCH

The existing Nigerian Cybercrime Act 2015 must incorporate or meet the international standard set by the Budapest Convention in order to be effective in combating the acceleration of cybercrime in the country".

1.4 OBJECTIVES OF THE RESEARCH

The research has the following objectives:

(a) To study the development of IT and the growth of cybercrime in Nigeria from the cybercrime theories and the categorisation of cybercrime.

(b) To critically assess the substantive criminal offences in the Budapest Convention on Cybercrimes for the purposes of strengthening cybercrimes laws in Nigeria and to examine the use of the European Union Directive on cybercrime to complement the effectiveness of the Budapest Convention.

(c) To analyse the cybercrimes related legislation in Nigeria and to assess the effectiveness of regional Conventions, such as African Union Convention on cybercrime and the Economic Community of West African States (ECOWAS) Directive on cybercrime as complementing the Nigeria Cybercrime Act 2015.

[17] *Ibid*.