The International Journal Of Engineering And Science (IJES)
||Volume||2 ||Issue|| 4 ||Pages|| 19-25||2013||
ISSN(e): 2319 – 1813 ISSN(p): 2319 – 1805

Cyber Crimes and Cyber Laws in Nigeria

[1,]Maitanmi Olusola , [2,]Ogunlere Samson, [3,]Ayinde Semiu [4,]Adekunle Yinka
[1,2,4,]*Computer Science Department, Babcock University, Ilisan Remo, Ogun State, Nigeria*
[3,]*Basic Sciences Department, Babcock University, Ilisan Remo, Ogun State, Nigeria*

----------Abstract----------

Cyber crime is a kind of crime that happens in cyberspace, that is, happens in the world of computer and the Internet. Cyber crime has become a global phenomenon; this kind of crime has the serious potential for severe impact on our lives, society, and economy because our society is becoming an information society where communication takes place in cyberspace. While there are several textbooks talking about cyber crime, but only few literatures focus on the relevant laws to combat these seemingly uncontrollable phenomenon. In other words, most materials talk about the crime of cyber crime, but this paper will talk more about cyber law. The discourse will start from origins, types, classifications, laws and propose recommendations to possibly reduce the growing problems in our society.

Keywords :*Cyber crime, Cyber, Computer crime, cyber laws.*

Date Of Submission: 05 April 2013 Date Of Publication: 05,May.2013

I. INTRODUCTION

The world has seen a remarkable transformation in terms of the use of information communication technology (ICT) with the advent of Internet based companies. Goods and services are routinely purchased and delivered electronically leading to significant changes in industries like journalism, travel, and banking. Online payments cut across all industries and are being used by a significant portion of U.S. households. For example, eBay reports that literally millions of people make their entire living solely on the eBay platform [1].It is obvious that the large portion of the population relies on the Internet, either directly or indirectly, for an ever increasing set of services. Seemingly nothing can slow this trend, with the possible exception of some catastrophic failure. It is unlikely that the Internet as a whole will experience such a catastrophic technical failure, and in fact the author believes these borders on the impossible.

What is possible, and perhaps even likely should current trends continue? Is the perception by Internet users that the Internet is unsafe and therefore unsuitable for everyday use even as we migrate towards cloud computing? Should this perception become widespread?

The author believed that cyber crime, and other cyber issues are the one area that could cause this type of loss of faith in the safety of the Internet. This paper begins with the premise that cyber crime is slowly getting worse, and that technical measures alone, while necessary and helpful, cannot significantly move the trend line in a positive direction. There is much data to support this position, and we do not think it is helpful to simply regurgitate that here. We believe that action is needed mostly from the government and non-governmental officials to counteract these negative trends, and the author present arguments in favour of a multifaceted regulatory approach to dealing with the problems, as the only viable way to proceed in the long term [2]
While this is an issue of global importance and will require international cooperation, this paper takes a fairly U.S. centric viewpoint in order to demonstrate the range of concrete steps that must be taken to significantly mitigate the impact of cyber crime. It is believed that many of the ideas presented here can be applied globally and that national solutions are not enough. International cooperation is essential for the continued health and vitality of the Internet. In order to solve the perceived problems, the paper is divided into the following sections including the introduction, reasons for the crime, , classification of cyber crimes, types of cyber crime, Cyber laws in Nigeria recommendations and conclusion.

II. REASONS FOR CYBER CRIME

A paper presented by [3] highlighted some of the reasons why we have these crimes in Nigeria today. The followings are excerpts from the discussion; two main factors aided this pattern: the free travel protocol which was granted by the Economic Community of West African State (ECOWAS) treaty; as well as the increasingly developed information technology (IT) infrastructure in the sub region.

These two factors combined with the poor attitude initially shown towards this fraud because it presumably preyed on foreign victims. These factors originally provided little incentive to do anything about the scammers, whose boiler rooms were growing by the day in other ECOWAS nations that had now become particularly attractive to the scammers such as Togo, Benin, Ghana, Burkina Faso, Senegal, and Cote d'Ivoire among others. But the researcher thinks that the causes are more than the above mentioned reasons by Ribadu, he believes there are other contributing factors such as greed, the uncontrollable desire for massive wealth (get quick rich syndrome) and mass employment were perceived as additional factors.

It was discovered that the categories of people who practice these nefarious act mostly fell among the followings:

- the perpetrators are youths and thousands of them are unemployed but highly knowledgeable and skilful in the use of computer, they actually drive the process.
- they are well connected through local insider conspiracy in the financial institutions locally as well as with Nigerian immigrant community elements abroad.
- knowing fully well that Nigerian have reinforced her security process they have migrated to mostly West African and other African nations with weak enforcement mechanisms [3]
- they also use a mechanism of re-shippers mostly in Dubai, the UK, and the West African way stations.
- they enjoy the fact that there are no cyber crime laws in any of these African jurisdictions that they have chosen as their relay stations [3]

2.1Classification of cyber crime

Cyber crimes against persons: Cyber crimes committed against persons include various crimes like harassment of any one with the use of a computer such as e-mail phishing. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important Cyber crimes known today. The potential harm of such a crime to humanity can hardly be amplified. This is one Cyber crime which threatens to undermine the growth of the younger generation as also leave irreparable scars and injury on the younger generation, if not controlled.

Similarly, in Nigeria before the gruesome murder of Cynthia Osokogu in July this 2012 as reported by an online news magazine [4] people have experienced a similar fate a case study of Uzondu for instance, as reported by the magazine happens to be an undergraduate student of a private Christian university in Ogun State allegedly contracted the dreaded Human Immune Virus, HIV, from a man she thought was her future husband. The victim met the con man on the popular social media, Facebook, and before she knew what was happening, she was taken to a dream vacation where she was showered with expensive gifts such as ipad, the latest blackberry phone amongst other things. In the course of these romantic trips, however, the young lady became pregnant, but her man was nowhere to be found. Unfortunately, she has no information on who the man was, no contact address or place of work. Worse still, she tested positive to HIV.

2.2.Cyber crimes against property: The second category of Cyber-crimes is that of Cyber crimes against all forms of property. These crimes include computer vandalism (destruction of others' property), transmission of harmful programmes such as virus or denial of the entire service.

2.3.Cyber crimes against government: The third category of Cyber-crimes relate to Cyber crimes against Government. Cyber terrorism is one distinct kind of crime in this category. The growth of Internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to terrorize the citizens of a country. This crime manifests itself into terrorism when an individual cracks into a government or military maintained website. More points on this classification will be unveiled under the types of cyber crime.

2.4 .Types of cyber crime

Cyber Terrorism

A cyber terrorist can be described as someone who launches attack on government or organization in order to distort and or access stored information stored on the computer and their networks. According to Wikipedia, a cyber-terrorist is someone who intimidates a government or to advance his or her political or social objectives by launching computer-based attack against computers, network, and the information stored on them. For instance, a rumour on the Internet about terror acts. In addition, a research carried out by [5] defined Cyber terrorism as an act of terrorism committed through the use of cyberspace or computer resources.

It means that any act intended to instil fear by accessing and distorting any useful information in organizations or Government bodies using Computer and Internet is generally referred to as Cyber Terrorism.Another form of cyber terrorism is cyber extortion is a form of cyber terrorism in which a website,e-mail server, computer systems is put under attacks by hackers for denial of services, demanding for ransom in return. Cyber extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service.

2.5 Malware

Malware refers to viruses, Trojans, worms and other software that gets onto your computer without your knowledge. Back in the early part of the century, most such software's primary aim was thrill. The people writing the software found it amusing to write a program that exploited security flaws just to see how far it could spread. Today the incentive for making such software is generally more dangerous. In some cases a piece of malware will pretend to be a legitimate piece of software. When such software is downloaded, it infects the computer system and destroys valuable information. The Trojan horse is also a technique for creating an automated form of computer abuse called the salami attack, which works on financial data. This technique causes small amounts of assets to be removed from a larger pool. The solution to salami attack is to avoid all unsolicited mails except is sure that the source is known or verified. We are recommended to avoid the use of trial versions of antivirus because we not given full database certification required for taking total control of virus, user are encouraged to go for proprietary software.

2.6 .Drug Trafficking Deals

Drug trafficking is another prominent cyber crime; it is a global trade involving cultivation, manufacturing, distribution and sale of substances which are subject to drug prohibition law. Drug traffickers are increasingly taking advantage of the Internet to sell their illegal substances through encrypted e-mail and other Internet Technology. Some drug traffickers arrange deals at internet cafes, use courier Web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms. The rise in Internet drug trades could also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimidated individuals to make comfortably purchase of illegal drugs [6].

2.7 Cyber Stalking

Cyber stalking is essentially using the Internet to repeatedly harass another person. This harassment could be sexual in nature as explained earlier, or it could have other motivations including anger. People leave a lot of information about themselves online. Such information can leave one vulnerable to cyber stalking; for instance, [7]analyzed the Facebook profiles of more than 4000 students and found out that only a small percentage had changed the default privacy settings. According to [8] who downloaded the Facebook profiles of a whole class of a private American university and found out that only one third was set to private. This means that for all those Facebook left on default settings all information can be view by all.

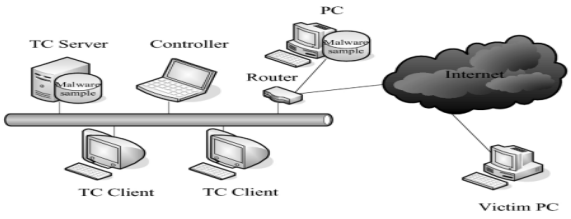

Figure 1: Security awareness is essential. Source: [9]

This is just to complement what was explained above, once one is on the Internet, extra security measures are needed to ensure that one's information is not broadcasted outside his/her public domain

2.8 Spam/Phishing

Spam is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified adds spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, television advertising and file sharing network spam. Perpetrators of such evil use e-mail extractor to extract all user of a particular domain and this is mostly common with yahoo mails. Some of these address harvesting approaches rely on users not reading the fine print of agreements, resulting in them agreeing to send messages indiscriminately to their contacts. This is a common approach in social networking spam such as that generated by the social networking site [10].

2.9 Fraud - Identity Theft

Fraud is a criminal activity in which someone pretends to be somebody and retrieve vital information about someone. For instance, making a false bank webpage to retrieve information of account of someone, or calling and pretending to be who you are not with the aim of cheating the caller. The concept is simple; someone gains access to your personal information and uses it for his own benefit. This could range from a black-hat hacker stealing online banking account login and password to getting access to automatic teller machine (ATM) and using such people can make themselves a lot of money with personal information. In Nigeria, people design web links forms requesting users to fill in their basic information including, unique details like pin numbers and use that to commit crimes.

2.10. Logic Bombs

A typical logic bomb tells the computer to execute a set of instructions at a certain date and time or under certain specified conditions. The instructions may tell the computer to display gotcha (an authentication method) on the screen, or it may tell the entire system to start erasing itself. Logic bombs often work like viruses. Whereas a simple virus infects a program and then replicates when the program starts to run, the logic bomb does not replicate, it merely waits for some pre-specified event or time to do its damage. Time is not the only criterion used to set off logic bombs. Some bombs do their damage after a particular program has run in a certain number of times.

2.11. Password Sniffing

Password sniffers are able to monitor all traffic on areas of a network. Crackers have installed them on networks used by systems that they especially want to penetrate, like telephone systems and network providers. Password sniffers are programs that simply collect the first 128 or more bytes of each network connection on the network that's being monitored. When a user types in a user name and a password as required when using certain common Internet services like file transfer protocol (FTP) or Telnet the sniffer collects that information [11].

III. CYBER LAWS IN NIGERIA

The researcher quite disagree with the research carried out by [12] who taught that Nigeria has no legislation against these crimes, this was actually what gave birth to this research work. But further reading testifies that it is not actually true. In reference to the paper quoted earlier by Ruanda where he mentioned as the chairman of Economic and Financial Crime Commission (EFCC) that cyber crime and its vices are under the jurisdiction of EFCC. Also supported by [13] that Economic and Financial Crimes Commission (EFCC) is the body empowered by government to fight all forms of financial crimes including cyber crimes in Nigeria. They are working together with the cyber crime prevention working group. Therefore, the above expression by Wada Odulaja would better be restructured as to believe that it is not the state of absolute lawless but perhaps rarely mentioned and practiced by EFCC[14] which is charged with the responsibility of investigating and prosecuting of all economic and financial crimes.

It is further believed that cyber laws need to be updated in Nigeria. It is a fact that Nigeria has legislative laws such as the criminal code volume iv laws of Ogun State of Nigeria. However, the criminal code seems to have been overlooked by [12] who claimed absolute lawlessness for Internet related crimes. The federal and state government need to update the criminal code laws. It must also be noted according to the [15] that the criminal code was enacted to sooth the West while the penal code was for the North, and this would be revisited below. The National Assembly is the legislative body which must as a matter of urgency modify/amend certain sections of the criminal code to deal with cyber crimes. Cyber crimes are being perpetuated on daily basis leading to serious crimes. This researcher is of the view that though the EFCC deals with Financial and Economic crimes, it is the criminal code that has all powers to deal effectively with cyber crimes.

3.1.The Nigeria Criminal Code Act 1990

The Criminal Code Act of 1990 criminalizes any type of stealing of funds in whatever form, an offence punishable under the Act. Although cyber crime 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 cyber crime is section 419, while section 418 gave a definition of what constitutes an offence under the Act. Section 418 states that any representation made by words, writing, or conduct, of a matter of fact, either past or present, which representation is false in fact, and which the person making it knows to be false or does not believe to be true, is a false pretence.

Also, section 419 states that any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years [15]

3.2The Economic and Financial Crime Commission Act, 2004 (Source: National Assembly of Nigeria, 2004)

The Economic and Financial Crime Commission Act [16] provide the legal framework for the establishment of the Commission. Some of the major
responsibilities of the Commission, according to part 2 of 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, among others;
- 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 al1 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;
- the Commission is further charged with the responsibility of enforcing the provisions of the Money Laundering Act 1995; [18];
- the Failed Banks (Recovery of Debts) and Financial Malpractices in Banks Act 1994, as amended;
- the Banks and other Financial Institutions Act 1991, as amended; and Miscellaneous Offences Act [17].

3.3Advance Fee Fraud and Related Offences Act 2006 (Source: National Assembly of Nigeria, 2006)

According to Section 23 of the advance fee fraud Act (Laws of the Federation of Nigeria, 2006): **'**False pretence means a representation, whether deliberate or reckless, made by word, in writing or by conduct, of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe to be true.**'** Section 383 sub-section 1 of the Nigerian Criminal Code states: A person who fraudulently takes anything capable of being stolen, or fraudulently converts to his own use or to the use of any other person anything capable of being stolen, is said to steal that thing[18]

Economic crime is defined by the Act as " the nonviolent criminal and illicit activity committed with the objectives of earning wealth illegally, either individually or in a group or organized manner thereby violating existing legislation governing the economic activities of government and its administration to include any form of fraud, narcotic drug trafficking, money laundering, embezzlement, bribery, looting, and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking and child labour, oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and policy, open market abuse, dumping of toxic wastes and prohibited goods." [18] is currently the only law in Nigeria that deals with Internet crime issues, and it only covers the regulation of Internet service providers and cybercafés, it does not deal with the broad spectrum of computer misuse and cyber crimes[19] as cited by [12]

3.4. Laws are only part of the solution to Cyber crimes

Extending the rule of law into cyberspace is a critical step to create a trustworthy environment for people and businesses. Because that extension remains a work in progress, organizations today must first and foremost defend their own systems and information from attack, be it from outsiders or from within. They may rely only secondarily on the deterrence that effective law enforcement can provide. To provide this self-protection, organizations should focus on implementing cyber security plans addressing people, process, and technology issues. Organizations need to commit the resources to educate employees on security practices, develop thorough plans for the handling of sensitive data, records and transactions, and incorporate robust security technology such as firewalls, anti-virus software, intrusion detection tools, and authentication services-throughout the organizations' computer systems. Besides all these, the followings are further recommendations for Nigerian government.

3.4.1 Reliance on terrestrial laws is an untested approach. Despite the progress being made in many countries, most countries still rely on standard terrestrial law to prosecute cyber crimes. The majority of countries are relying on archaic statutes that predate the birth of cyberspace and have not yet been tested in court.

3.4.2 Weak penalties limit deterrence. The weak penalties in most updated criminal statutes provide limited deterrence for crimes that can have large-scale economic and social effects.

3.4.3 Self-protection remains the first line of defense. The general weakness of statutes increases the importance of private sector efforts to develop and adopt strong and efficient technical solutions and management practices for information security.

3.4.4 A global patchwork of laws creates little certainty. Little consensus exists among countries regarding exactly which crimes need to be legislated against. In a networked world, no island is an island. Unless crimes are defined in a similar manner across jurisdictions, coordinated efforts by law enforcement officials to combat cyber crime will be complicated.

3.4.5 A model approach is needed. Most countries, particularly those in the developing world, are seeking a model to follow. These countries recognize the importance of outlawing malicious Computer-related acts in a timely manner in order to promote a secure environment for ecommerce.
But few have the legal and technical resources necessary to address the complexities of adapting terrestrial criminal statutes to cyberspace. A coordinated, public-private partnership to produce amodel approach can help eliminate the potential danger from the inadvertent creation of cyber crime refuge.

IV. RECOMMENDATIONS

The weak state of global legal protections against cyber crime suggests three kinds of action.

4.1. Firms should secure their networked information.

Laws to enforce property rights work only when property owners take reasonable steps to protect their property in the first place. As one observer has noted, if homeowners failed to buy locks for their front doors, should towns solve the problem by passing more laws or hiring more police? Even where laws are adequate, firms dependent on the network must make their own information and systems secure. And where enforceable laws are months or years away, as in most countries, this responsibility is even more significant.

4.2 Governments should assure that their laws apply to cyber crimes.

National governments remain the dominant authority for regulating criminal behaviour in most places in the world. One nation already has struggled from, and ultimately improved, its legal authority after a confrontation with the unique challenges presented by cyber crime. It is crucial that other nations can copy this lesson, and examine their current laws to discern whether they are composed in a technologically neutral manner that would not exclude the prosecution of cyber criminals.

4.3 Firms, governments, and civil society should work cooperatively to strengthen legal frameworks for cyber security.

To be prosecuted across a border, an act must be a crime in each jurisdiction. Thus, while local legal traditions must be respected, nations must define cyber crimes in a similar manner. An important effort to craft a model approach is underway in the Council of Europe (www.coe.int), comprising 41 countries. The Council is crafting an international Convention on Cyber crime. The Convention addresses illegal access, illegal interception, data interference, system interference, computer-related forgery, computer-related fraud, and the aiding and abetting of these crimes. It also addresses investigational matters related to jurisdiction, extradition, the interception of communications, and the production and preservation of data.
Finally, it promotes cooperation among law enforcement officials across national borders.
The following are additional information for both stakeholders and Nigerian government if cyber crimes are actually going to be minimized:

- Insufficient funding for cyber crime law enforcement should be looked into
- Lack of trained cyber experts within law enforcement officials
- Lack of effective international cooperation and data sharing
- Lack of universality of laws against cyber crime
- Statutory minimums in cyber crime cases hamper effective enforcement
- The growing nature of mass unemployment in Nigeria is worrisome.

V. CONCLUSION

This paper examined the impact of the information communication technology (ICT) revolution on business, industry, government and country's image in the light of the unintended consequences such as criminal activities, spamming, phishing, identity theft and other related cyber crimes. The author assessed cyber crime and its impact the users of ICT and proffer possible solutions. The author also unveiled what the laws of Federal Republic of Nigeria have to say about cyber crimes and its consequences. The authors concluded that the criminal code laws should be modified to include offences of cyber crimes. In the same vein, stiffer punishments to be included in those laws as well.

VI. ACKNOWLEDGEMENT

We wish to acknowledge the efforts of Professor Omotosho, O. J for his untiring effort to see us through this far and Barrister Sodipo, Olutoye for accepting to make his input where necessary, may God bless you and your families.

REFERENCES

[1] D.,Halderand K., Jaishankar, Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9. (2011)
[2] M., Ngugi Legal week: Law on Cyber Crime Overdue, available at *www.crimeresearch.org(*2005)
[3] N., Rubadu Modern Law for Global Commerce, Congress to celebrate the fortieth annual session of UNCITRAL Vienna, 9-12 July 2007 Cyber crime and Commercial Fraud: A Nigerian Perspective. (2007)
[4] S., Osokogu Sourcehttp://news.naij.com/6049.html DEATH BY FACEBOOK: The Story Of The Late Cynthia Osokogu
[5] D., Parker Fighting Computer Crimes, U.S. Charles Scribner's Sons. (1983)
[6] Http://www.wikipedia.com.
[7] A,. Acquisti and R., Gross Predicting Social Security numbers from public data.*Proceedings of the National Academy of Sciences,* 106: 10975-10980 (2009).
[8] K., Lewis, J., Kaufman and N., Christakisin press. The taste for privacy: an analysis of college student privacy settings in an online social network. Journal of Computer-Mediated Communication. (2005)
[9] J. Zhang, Q,.Wu and J. Chen.Research on design method of dynamic partial reconfigurable system.J. Software Eng., 6: 21-30. (2012)
[10] H., Saul Social network launches worldwide spam campaign New York Times (2007)
[11] C., Peter, P., Kenneth, M., Lucasz, P., Tom, and W. Michael, SPAMALOT: A Toolkit for Consuming Spammers Resources. Proceedings of the 3rd Conference on E-mail and Antispam, July, 2006. Available online at www.ceas.org.
[12] G. O, Odulajaand F.Wada AssessingCyber crime and its Impact on E-Banking In Nigeria Using Social Theories (2012)
[13] O.BLonge, S.CChiemeke, S. Fashola, F.Longe, and A. Omilabu, "Internet ServiceProviders and Cyber crime in Nigeria Balancing Services and ICT Development(2007)
[14] Criminal Code Act Chapter 77, Laws of the Federation of Nigeria. (1990)
[15] Nigerian Constitution available at *ww.ngex.com/**nigeria**/govt/**constitution**/default.htm*(199)
[16] Advance Fee Fraud and Other Fraud Related Offences Act 2006, Laws of the Federation of Nigeria
[17] EFCC available at www.**efcc**nigeria.org/**efcc**_homepage.../establishment_act_**2004**.pdf(2004)
[18] Advanced free fraud available at http://www.nigeria-law.org/Advance%20Fee%20Fraud%20and%20other%20Fraud%20Related%20Offences%20Act%202006.htm (2006)
[19] N. Ewelukwa, This Day Newspaper, Nigeria, March 31.2011