International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 4 Issue 4, April 2017

ISSN: 2394-4404

# Cybercrimes In Nigeria And Counter Measures

**Shonubi Joseph Oluwafemi**
Department of Computer Science,
Federal Polytechnic, Ekowe, Bayelsa State, Nigeria

**Godwin-Obehiri Orumah**
Library Department,
Federal Polytechnic, Ekowe, Bayelsa State, Nigeria

***Abstract:*** ***It is of no doubt that Information and Communication Technology has greatly improved our way of living. Virtually every sector of the economy such as agriculture, health, education, oil and gas, maritime, law, banking, security and so on daily rely on this ubiquitous means and have received dynamic boost through the application and usage of ICT. However, there is a big disadvantage to the existence of ICT because it has also brought along with its very good role, evil deeds – crimes committed through the use of ICT which are being perpetuated by people around the world who have acquired technical expertise and technological-know-how for their selfish gains and purposes. This paper hopes to unravel the background of cybercrimes in Nigeria and how government can effectively combat the abuse of the new technology.***

***Keywords: Nigeria, Cybercrime, Cyber terrorism, Terrorism, Terrorist, Cyberspace, Cyber security, Cyber offenders, Cyber criminals, ICT***



## I. INTRODUCTION

Cybercrimes are defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim(s) directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones" (Halder & Jaishankar, 2011).

These crimes may be a threat to government establishments, financial institutions, corporate organizations or private entities. There is no limit, boundaries or geographical restrictions because cybercrime is a world-wide problem as cyber-attacks are witnessed in developed countries as well as developing nations.

The first cybercrime was committed in 1820 when Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened therefore; they committed acts of sabotage to discourage Jacquard from further use of the new technology. This became the first recorded cybercrime.

## II. LITERATURE REVIEW

Nigeria penetrated the cyberspace through the advent of mobile telephony in 2001. According to the National Communication Commission – NCC (Subscriber Staticstics) report, Nigeria had a total of 1,569,050 subscribers in 2002, and twelve years after the introduction of mobile telephony, total subscribers stood at 184,782,512. The direct impact of this is the astronomical advancement in all spheres of the Nigerian economy.

As time went by, competition arose in the telecommunication sector bringing down the cost of call and data services to the average consumers.

However, it is pertinent to note that the great advancement witnessed in our country has a huge side-effect which if not properly checked and addressed, it can and will definitely cripple the economy.

Developed countries have a better understanding of the risk of cybercrimes as (Gutsaluk, 2003) observed that Great Britain heavily funded and established National Hi-Tech Crime Unit (NHTCU) - the first in the history of Great Britain, a national law-enforcement organization on fighting computer crimes. Great Britain spent about 25 million pounds for three years on fighting cybercrimes. 10 million pounds on

developing corresponding departments on spots and 15 million - on creating the National Hi-Tech Crime Unit.

## III. TYPES OF CYBER CRIMES

### A. CYBER TERRORISM

Arguably, no international agreed definition exist for the term "terrorism" but numerous authors, have given various definitions for terrorism one of the definitions that are frequently encountered was opined by (Best, 2000) which says that terrorism is "the unlawful use or threatening use of force or violence by a person or an organized group against people or property with the intention of intimidating or forcing societies or governments, often for ideological or political reasons. The United States Federal Bureau of Investigation (FBI) also defines terrorism as, "The unlawful use of force or violence, committed by a group(s) of two or more individuals, against persons or property, to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." (FBI, 2002)

(Osho etal, 2013) reveals that terrorism in Nigeria is a direct upshot of the people's deep disenchantment with their government. The mishandling of national issues has given rise to several dissenting groups along our geographical lines, including the Movement for the Emancipation of Niger Delta (MEND) in the South; the Oodu'a People's Congress in the South West; the Bakassi Boys and the Movement for the Actualisation of the Sovereign State of Biafra in the South East, and the Jama'atu Ahlus Sunnah Lid Da'awati Wal Jihad, otherwise known as Boko Haram, in the North. Since 2012, Nigeria has had its undue share of this menace claiming lots of lives and properties except for recent times did the military got meaningful advancement against this terrorist group.

Dorothy Denning, a computer science professor, unambiguously explains: "Cyber terrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear". (Weimann, December 2004) affirms that attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

The terrorist group "Boko Haram" while acclaiming to fight western education still use cyberspace to broadcast their devilish propaganda by uploading shocking videos depicting killings of kidnapped people (including women and children) to the internet, recruit and re-orientate un-suspecting victims and also monitor government/military communication links amongst many other activities with the same education-technology they seem to vehemently oppose. It is alarming to know that Cyber terrorism is however daily gaining more grounds with little or no effort from the government in stopping or combatting the surge in cybercrimes perpetuated in our nation.

### B. CYBER STALKING

Cyber stalking is essentially using the Internet to repeatedly harass another person. This harassment could be sexual in nature, 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, a term that essentially refers to using the Internet to stalk (to illegally follow and watch somebody) (Plot, 2010).

(Oxford University Press, 2013) has a broader view which clarifies cybercrime as the use of the Internet or other electronic means to stalk or harass an individual, a group, or an organization. Yul Edochie, Nollywood popular actor –was cyber stalked for more than a year by a gay on the social media (twitter) and even by phone calls amounting up to 777 missed calls. His demand is that Yul Edochie compulsorily reveals his genitals to him or risk being disgraced in public as a gay and his wife labelled as a lesbian since he has put the picture of Yul's wife on lesbian websites (Nairaland, 2015). It could further be established that persistent mobile phone calls to a person for sexual harassment is a form of Cyber stalking which is a cybercrime.

### C. FRAUD - IDENTITY THEFT

Back in the early 90s, fraud in the Nigerian society was popularly called 419 in reference to the penal code that framed the criminal justice system in Nigeria. At the time, persons who were arrested in connection to that law were labelled '419ers'. Lax criminal law enforcement and a ponderous criminal justice system meant that the rampant practice of 419 was already a constant source of grief. Then along came the Internet, shortly after which a number of tech savvy cons successfully "exported" the 419 concept. While the popular 419 reference has since been extended to include cyber criminals, in Nigeria the name "Yahoo-Yahoo" is the most familiar informal usage that is employed to speak of people who perpetrate scams online. (Gbenga etal, 2013)

According to (Anah etal, August 2012) several youths engage in cybercrime with the aim of emerging as the best hacker, or as a profit-making venture since the tools for hacking in our modern world has become affordable to many. One of the ways fraudsters gain access to personal information asides hacking into financial institution websites is by designing online forms requesting for vital information such as ATM pin from unsuspecting victims. However, most Banks continually alert customers to ensure their pin numbers and bank details are kept secret. Often times, victims of these scammers find it very hard to get over the psychological trauma and the pains caused.

### D. SPAMMING

According to (Maitanmi etal, 2013) Spam is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately. Spamming was said to be one of

the most prevalent activities on the Nigerian Internet landscape accounting for 18% of all online activities amongst others. (Longe & Chiemeke, June, 2006). Email spam is often regarded as the most recognized form of spamming but it also includes instant messaging spam, Short Messaging Service (SMS) spam, blog-spam, search engines spam etc. Even media adverts (television adverts) are forms of spamming. Mobile Telecommunications Network providers in Nigeria such as MTN, GLOBACOM, Airtel and Etisalat in the name of advertising product offers, send unsolicited messages to mobile network subscribers more often than not, to the annoyance of these subscribers.

Internet users need to be more careful online since spamming is an effective tool used to hack into email addresses as rightly opined by (Saul, 2007), Email spam perpetrators use e-mail extractor to extract all users 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. Once a spam message is sent into an email box, it may contain malware, virus or a link that compromises the security of the computer system. The intruder gains access to classified documents in the computer system.

### E. PASSWORD SNIFFING

A password sniffer is a software application that scans and records passwords that are used or broadcasted on a computer or network interface. It listens to all incoming and outgoing network traffic and records any instance of a data packet that contains a password (Janssen, 2010). Crackers install them on networks used by systems that they especially want to penetrate, like telephone systems and network providers. It simply collects 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 (Peter etal, July, 2006). Serious security breach can be reached once a third party (intruder) gains access to a user's login details.

### F. MALWARE

Malware are programs such as viruses, Trojans, worms and other malicious software programmed to suspiciously encroach into a computer system without the knowledge of the user. Malware may be stealthy, intended to steal information or spy on computer users for an extended period without their knowledge, e.g. Regin, or it may be designed to cause harm, often as sabotage (e.g., Stuxnet), or to extort payment (CryptoLocker). 'Malware' is an umbrella term used to refer to a variety of forms of hostile or intrusive software (Robert, 2003). It often takes the form of executable code, scripts, active content, and other software.

(Hernandez, 2013) points out that many early infectious programs including the first Internet worm were written as experiments or pranks. Today, malware is used by both black hat hackers and governments, to steal personal, financial, or business information. When such software is downloaded, it infects the computer system and destroys valuable information.

## IV. CAUSES OF CYBERCRIME

Some of the prevalent and major causes of cybercrime are listed below:

### A. UNEMPLOYMENT

One of the major breeding ground for cybercrime in Nigeria is the high rate of unemployment which is prevalent in the country. Ratings by (Trade Economics, 2015) show that Nigeria has an all-time high rate of 23.9% which is about 20 million people. With our tertiary institutions reeling out graduates in their numbers each year, unemployment rate is increasingly becoming an issue needing urgent attention and proactive actions by Government. Many of these unemployed youths see the cyberspace as an opportunity to make fortune or privilege to commit crime without being suspected as the popular saying goes, "*An idle mind is the devil's workshop*".

### B. POOR EDUCATIONAL STANDARD

The continuous decay of Nigeria's educational standard is another attribute responsible for the increase in cybercrimes. Facilities in most public institutions (primary and post-primary) are either dilapidated or out-of-date. Students do not have access to modern facilities and they come out of school not having values for the usage and security of the cyberspace. There is no desire to protect the integrity of the nation's cyberspace because they passed through a system that is deformed and un-grounded in practical approach to cyber safety and etiquettes.

Furthermore, school curriculum right from primary level do not include cyber etiquette, safety and procedures which are a fundamental tool in technological development.

### C. LACK OF STERN GOVERNMENT POLICIES

Provision of the rule of law is critical and essential in cyber space in order to ensure that businesses can thrive in Nigeria without fear. It must be noted as opined by (Gbenga etal, 2013) that cybercrime in Nigeria will however continue to remain a problem until legislation that addresses it is passed. Clearly, the current state of cybercrime legislation is not helped by the lack of fervor and conviction that policymakers display when the subject comes up for discussion. It is hoped that the latest set of cybercrime draft bills will not meet the same obscure fate of their predecessors. Considering the huge cost of cybercrime to Nigeria and Nigerians, the need for firm and fair cybercrime legislation – that does not hurt Internet freedom – is evident.

Some of the draft bills initiated on cybercrime are highlighted below:

- ✓ Computer Security and Critical Infrastructure Bill (2005);

- ✓ Electronic Service Provision Bill (2008);
- ✓ Interception and Monitoring Bill (2009);
- ✓ NSA Cyber Security Bill (2011) – expected to be presented to the National Assembly as an Executive Bill;
- ✓ Criminal Code Amendment for Offences Relating to Computer Misuse and Cybercrimes (2011);
- ✓ Penal Code (Northern states) Federal Provisions Act, Cap. P3. Laws of the Federation of Nigeria, 2004, to Provide for Offences and Penalties Relating to Computer Misuse and Cybercrimes (2011) and;
- ✓ Electronic Transfer of Funds Crime Bill (2011).
- ✓ He further stressed that aside from similar purpose and overlapping scopes in many cases, these draft bills all have one thing in common – none of them has made it through to the other side of the elaborate law-making process.

### D. LAXITY IN CYBER SECURITY

The Nigerian cyberspace is very porous leaving a huge gap for cyber criminals to explore. This perceived challenge is a back-bone breaker for the Nigerian economy. Organised cybercrimes are prevailing today; terrorism has extended to our cyberspace as Boko Haram boldly and successfully post viral videos of kidnapped innocent people (both citizens and expatriates) and sometimes, the killing of some of these kidnapped people to the internet without a trace. Citizens of Nigeria have had their lives cut short just by making friends with cyber criminals on facebook and/or other social media platforms. The sad case of Cynthia Osokogu, the only daughter of an ex-General of the Nigerian Army who lost her life in 2012 to this menace as reported in Vanguard Newspaper, readily comes to mind. (Evelyn, 2012)

### E. LOW AWARENESS

There is practically no awareness program either on conventional or new media informing the general populace of the havoc being wroth on the internet on daily basis. An average Nigerian does not know how to spot a scam online until (s)he becomes a victim. The Nigerian masses should not be left to their fates when it comes to cybercrimes. It should be ensured that awareness of these crimes is more important than the crimes being committed.

## V. EFFECT OF CYBERCRIME ON THE NIGERIAN ECONOMY

If the Nigerian economy must survive and grow, then there is a need to identify the resultant effect of the threat poised to its development.

### A. SCARE FOREIGN INVESTORS AWAY

No one likes to money in a leaking bag. If prompt actions are not taken or perceived to be taken by government, there is a risk of losing major existing foreign investors and not only that, it will definitely scare other intending investors away who may more likely than not invest in neighbouring countries.

### B. THREAT TO NATIONAL SECURITY

A full-scale cyber terrorism attack is very likely to be successful in Nigeria. An example is the cyber-war between India and Pakistan. Indian hackers hacked the official website of Pakistan's Election Commission to retrieve sensitive data. Pakistani hackers retaliated by hacking and defacing a total of 1,059 website owned by Indian election bodies. As a result of this, Pakistan is working on effective cyber security system called "Cyber Secure Pakistan" (CSP) which was launched in April 2013. Currently, this program has been expanded to universities in Pakistan. The Nigerian government should take a cue from this to avoid national embarrassment in the future.

### C. NEGATIVE IMPACT ON THE AFRICAN CONTINENT

It is often said that "if Nigeria sneezes, the rest of other African nations catch a cold". It therefore needs to be put in remembrance that if our great country does not urgently fight cybercrime, the African continent is at jeopardy. It will not only strip us of the singular opportunity to be called the "Giant of Africa" or "Largest Economy in Africa", it will definitely drag the country's pride in the mud.

### D. DECAY OF MORAL STANDARDS

The teens and youths who are supposed to be the leaders of tomorrow are modelling themselves after well-known cyber criminals such as the "Yahoo boys" in perceiving them to be successful and wealthy. Therefore, the desire to go to school to acquire knowledge is diminishing at an alarming rate because they have seen an easy and more lucrative venture to actualise their dreams. The impact of this is that with no time, Nigeria will lose more creative minds.

## VI. CONCLUSION

The introduction of new technological prowess such as cashless policy, e-banking, mobile money etc. will be a booster to the growth of the economy but also a breeding ground for cybercrime if we fail to secure our cyber space. It is worth noting that cyber criminals will stop at nothing till they accomplish their aims therefore, we must rise up to the task before it is too late for the Nigerian nation.

## VII. RECOMMENDATIONS

Though cybercrimes cannot be totally eradicated, yet frantic efforts could be made to ensure it is reduced to the barest minimum. The recommendations below will be helpful in tackling cybercrimes meaningfully. These recommendations are in two phases. Phase one is the responsibility of the government of the Federal Republic of

Nigeria while Phase two is aimed at every individual residing within the borders of Nigeria.

PHASE I

A. INSTITUTIONALISING A CYBERCRIME AGENCY

It is hereby proposed that an institution empowered by an Act of Law should be established to combat every form of cybercrime, arrest and prosecute cyber-offenders. Nigeria should take a cue from the western world such as USA's Internet Crime Complaint Center (IC3), U.S. Computer Emergency Readiness Team (U.S. CERT) and England's National Cyber Crime Unit (NCCU). By the Act of Law that establishes this unit, it should be a stand-alone outfit such as the EFCC, NAFDAC etc. and not a sub-unit of any security agency. It is however necessary to stress that the freedom of Nigerians in cyberspace should be adequately protected.

B. PROVISION OF EMPLOYMENT OPPORTUNITIES

Employment opportunities should be provided for the teaming graduates of this country in order to deter them from seeking other illegal means of enriching themselves. Government can further encourage the provision of loan facilities for Small and Medium Scale Entrepreneurs (SMEs) to graduates and make them self-employed and employers of labours.

C. PROVISION OF CYBER SECURITY TRAINING

Adequate training and re-training should be provided to staff and employees at all levels in various organizations through partnership with Industrial Training Fund (ITF), Nigerian Communications Commissions (NCC), National Information Technology Development Agency (NITDA), National Orientation Agency under the Ministry of Information and the Office of the National Security Adviser (ONSA). Cyber security strategic plans (both in the mid-term and long-term) should be developed and imparted through trainings which should be geared towards handling of sensitive data, implementation of strong security measures in organizations such as intrusion detection systems, users' authentication system, firewall protection and the use of effective anti-virus software.

D. ORGANISE AWARENESS INFORMATION PROGRAMS

The National Orientation Agency (NOA) under the Ministry of Information and other relevant government agencies that are the mouth pieces of government should saddle up in their responsibility towards the reduction cybercrime rate in Nigeria – spreading the word to every nook and cranny of the country by every means possible should be paramount.

Cybercrime awareness should be in the form of:

- ✓ Warning cyber criminals and potential criminals to deter from cybercrimes;
- ✓ Informing the general masses to report cases of cybercrimes to the appropriate authorities with a promise to bring perpetrators to justice;
- ✓ Provide rewards/incentives for the information leading to the arrest and/or conviction of wanted cyber criminals;
- ✓ Notifying the entire populace to avoid doing business with these criminals, and ensuring that people who harbour them are also held liable.

E. STRICT ADHERENCE TO PENAL LAWS

Our penal codes should not be seen as a toothless – bull – dog which barks but cannot bite. It is very important to bring evil perpetrators using computers to achieve their malicious aims to justice. This will deter others from cybercrime and also improve our rating in the comity of nations.

F. MONITORING OF ISPS AND INTERNET CYBER CAFES

Internet Service Providers operating within the borders of Nigeria should be periodically monitored by appropriate agencies. There should be standardized laws requiring every cyber café in the country to be duly registered with the institutionalised cybercrime agency so that monitoring, tracing and detection of cybercrimes through IP addresses will be effective.

(Mbaskei, 2008) further suggested that Telecommunication Regulatory Agencies should enhance security on internet service providers' server.

PHASE II

G. COMPUTER SYSTEM'S PROTECTION AGAINST CYBERCRIME

Every Nigerian and corporate organizations using the internet must ensure that computers are adequately protected against malware intrusion. Potent anti-virus and internet security software should be used and updated frequently.

H. AVOID PIRATED SOFTWARE

Pirated software should be avoided because they often come with hidden malware which infects the computer systems. Corporate entities should have strict policies for software collections and usages.

I. DO NOT FILL FORMS ONLINE WITHOUT CROSS-CHECKING

Scammers design website to collect confidential information such as PIN numbers, Bank accounts details etc. for fraud. Never give out confidential information. Ensure a thorough background check is carried out on any website requesting forms to be filled for recruitment purposes. www.jiji.ng has a form page requesting applicants to fill forms for (Nigerian Customs Recruitment, 2015) while the NCS placed a disclaimer on recruitment scam.

J. AVOID DOWNLOADING SOFTWARE FROM UNTRUSTED WEBSITES

Untrusted websites are all over the internet. If software must be downloaded for any purpose, it must be from a trusted site. Otherwise, the computer system has just been made open to cyber-attacks.

K. CASES SHOULD BE REPORTED TO AUTHORITIES

Nigerians owe it as a responsibility to report cyber – attack cases to appropriate government agencies in order to swiftly tackle and arrest cyber offenders and as suggested by (Plot, 2010) report particularly evil spam to the appropriate authorities.

REFERENCES

[1] Anah etal. (August 2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. ARPN Journal of Science and Technology VOL. 2, NO. 7, 626-631.
[2] Best, S. (2000). Symantec. Retrieved May 20, 2015, from Symantec: http://www.drstevebest.org/Essays/Defining%20Terrorism.htm, www.symantec.com/avcenter/reference/cyberterrorism.pdf
[3] Evelyn, U. (2012, August 21). How ex-General's daughter, Cynthia, was killed by facebook 'friends'. Retrieved May 26, 2015, from Vanguard News Paper: http://www.vanguardngr.com/2012/08/how-ex-generals-daughter-cynthia-was-killed-by-facebook-friends/
[4] FBI. (2002). Code of Federal Regulations. 28 CFR. Section 0.85 on Judicial Administration. USA.
[5] Gbenga etal. (2013). Economic Cost of Cybercrime in Nigeria. Retrieved May 22, 2015, from Paradigim Initiative Nigeria: https://www.pinigeria.org/download/cybercrimecost.pdf
[6] Gutsaluk, M. (2003). Fighting Cybercrime. Retrieved May 21, 2015, from Crime Research: http://www.crime-research.org/library/Gutsaluk.html
[7] Halder, D., & Jaishankar, K. (2011). Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global.
[8] Hernandez, P. (2013, December 15). "Microsoft Vows to Combat Government Cyber-Spying". Retrieved May 25, 2015, from Federal Trade Commission: http://www.consumer.ftc.gov/articles/0011-malware
[9] Janssen, C. (2010). Password Sniffer. Retrieved May 24, 2015, from Techopedia: http://www.techopedia.com/definition/8798/password-sniffer
[10] Longe, O. B., & Chiemeke, S. C. (June, 2006). The design and implementation of an e-mail Encryptor for combating internet spam". Proceedings of the Ist International Conference of the International Institute of Mathematics and Computer Sciences., (pp. 1 - 7). Ota, Nigeria.
[11] Maitanmi etal. (2013). Cyber Crimes and Cyber Laws in Nigeria. The International Journal Of Engineering And Science (IJES) Volume 2, Issue 4, 19-25.
[12] Mbaskei, M. O. (2008). Cybercrimes: Effect on Youth Development. Retrieved May 26, 2015, from i-genius: http://www.i- genius.org
[13] Nairaland. (2015, May 20). Yul Edochie Receives 777 Missed Calls Daily From Gay Stalker [see Screenshot] - Celebrities - Nairaland. Retrieved May 21, 2015, from Nairaland.com: http://www.nairaland.com/2325860/yul-edochie-receives-777-missed
[14] Nigerian Customs Recruitment. (2015). Retrieved May 25, 2015, from Jiji: http://jiji.ng/login.html?url=http%3A%2F%2Fport-harcourt.jiji.ng%2Fother-jobs%2Fnigeria-custom-service-recruitment-447395.html&advert=447395&type=job&p=17&p=17
[15] Osho etal. (2013). Combating Terrorism with Cybersecurity: The Nigerian Perspective. World Journal of Computer Application and Technology.
[16] Oxford University Press. (2013, December 10). Wikepedia-Cyberstalking. Retrieved May 21, 2015, from Wikipedia: http://en.wikipedia.org/wiki/Cyberstalking#cite_note-oxford-1
[17] Peter etal. (July, 2006). SPAMALOT: A Toolkit for Consuming Spammers Resource. Proceedings of the 3rd Conference on E-mail and Antispam, Available online at www.ceas.org.
[18] Plot, J. (2010). Top five computer crime and how to protect yourself from them. Publication of Justin plot.
[19] Robert, M. (2003, October 1). Defining Malware: FAQ. Retrieved May 25, 2015, from Microsoft: https://technet.microsoft.com/en-us/library/dd632948.asp
[20] Saul, H. (2007). Social network launches worldwide spam campaign. New York Times.
[21] Subscriber Staticstics. Retrieved May 21, 2015, from Nigerian Communications Commission: http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=125&Itemid=73
[22] Trade Economics. (2015). Trade Economics. Retrieved 2015, from Trade Economics: http://www.tradingeconomics.com/nigeria/unemployment-rate
[23] Weimann, G. (December 2004). Cyberterrorism. How Real is the Threat? Washington DC: UNITED STATES INSTITUTE OF PEACE.