National Journal of Advanced Research
Online ISSN: 2455-216X; Impact Factor: RJIF 3.42
www.allnationaljournal.com
Volume 2; Issue 2; March 2016; Page No. 28-38

Cyber crime and Nigerian business environment

[1] Dr. Onodugo Ifeanyi Chris, [2] Dr. Itodo SM

[1] Dept. of Public Administration and Local Government University of Nigeria Nsukka
[2] Department of Public Administration Nasarawa State University Keffi, Nigeria.

Abstract
Within the last decade, the use of the Internet in Nigeria has grown so rapidly with the explosion of Internet Service Providers (ISPs), Internet cyber cafés and access points. This has had several positive impacts on the social, economic and educational sectors in the country. Unfortunately, the country's image has also suffered as a result of the nefarious activities of some Nigerians, who instead of utilizing the Internet for constructive purposes; turn it into a cheap channel for the perpetration of criminal activities. With Nigeria venturing into cashless society, there is a need for cybercrimes menace to be minimized if not completely eradicated. This paper seeks to find out the curses of the scourge in cybercrimes, its effects on the economy and how to combat the evil. We adopted an expo factor descriptive methodology in the research. We found that Cybercrime involves using computers and Internet by individuals to commit crime. Cyber terrorism, identity theft and spam are identified as types of cybercrimes. The study identified some of the causes of cybercrimes to include urbanization, unemployment and weak implementation of cybercrime laws. The effects of cybercrimes on organizations, the society and the country in general include reducing the competitive edge of organizations, waste of production time and damage to the image of the country. We recommend that firms should take reasonable steps to protect their IT infrastructure like Networks and computer systems; government should assure that cybercrime laws are formulated and strictly adhered to and individuals should observe simple rules by ensuring antivirus protection on their computer systems.

Keywords: Cyber-space, Cyber-security, Cyber-crime, ICT, Internet *crimes, fraud and spam*

Introduction
IT revolution has brought about a vast array of aides and conveniences that have indelibly influenced modern communication, travel, security and commerce. However the massive gains brought by the information age are not perfect, with the pervasive correlation of human activity with electronic resources and infrastructure there is a crucial vulnerability, which is the ever present risk of abuse, insidious manipulation and sabotage of computer and computer networks. This distinct, unitary phenomenon is a new class of antisocial activity that cannot be dealt with through the application of extant laws. Most countries lack appropriate legislation to deal with internet/computer related crimes.

Cybercrime is a criminal activity involving the information technology infrastructure, including illegal access, illegal interception (by technical means of non-public transmission of computers data to, from or within a computer system), data interferences (unauthorised damaging deletion, deterioration, alteration or suppression of computer data), systems interferences (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting etc.) forgery (ID theft) and electronic fraud.

Theoretical Perspective
In sociological analysis, theories are indispensable. They form an integral part of sociological research as it is a general principle that explains or predict facts, observation or events. The theory of differential association was adopted for this study. This theory was propounded by Edwin Sutherland an American Sociologist. Differential association theory proposed that through interaction with others, individuals learn the values, attitudes, techniques and motives for criminal behaviour. According to this theory, the environment plays a major role in deciding which norms people learn to violate (Sutherland, 1939). The principle of differential association asserts that a person becomes delinquents because of an "excess" of definitions favourable to violation of law over definitions unfavourable to violation of law. What this means is that an individual will become a criminal because they are exposed to more favourable criminal behaviour. That is when one is exposed to more criminal influences rather than more favourable legal influences. In other word, criminal behaviour emerges when one is exposed to more social message favouring misconduct than pro – social messages. This can be seen in environments with poor socio-economic conditions which may encourage negative views towards the law and authority.

According to Sutherland (1939), criminal behaviour is learned. Criminal behaviour is learned in interaction with other persons in a process of communication. This would mean an individual is influenced to participate in criminal behaviour through watching and interacting with other individuals who are engaging in the criminal behaviour. The principal part of the learning of criminal behaviour occurs within intimate personal groups.

When criminal behaviour is learned, the learning includes techniques of committing the crime, which are sometimes very complicated, sometimes simple and they learn the specific direction of motives, drives, rationalizations and attitudes for committing a crime. This means that an individual will be influenced into believing that the behaviour which they may have previously believed was wrong, into believing that it is right through rationalization of their action. Furthermore, an individual will be pushed into deviant behaviour depending on

their view of the legal code as being favourable or unfavourable. A person becomes delinquent because of an excess of definitions favourable to violation of law over definitions unfavourable to violation of the law. Therefore, an individual will break a law if they see more reasons to break it than to stay in compliance with it. Differential Associations may also vary in frequency, duration, priority and intensity. The process of learning criminal behaviour by association with criminal and anti-criminal patterns involves all of the mechanisms that are involved in any other learning. This means that individuals learn criminal actions and legal through the same way. This theory states that while criminal behaviour is an expression of general needs and values, it is not necessarily the fulfilment of these needs and values which causes deviant behaviour since non-criminal behaviour is an expression of these same needs and values.

The theory of Differential Association can be applied to cybercrimes. The main premise behind this theory is that criminal behaviour is learned through social interactions with others. The profile of cyber criminals is one who is very smart, highly knowledgeable and who are computer savvy. Their social interactions may come through electronic communications with other individuals who share similar technological interests. If they do not currently have any desire to commit malicious acts through electronic means, such as an act in violation of the computer fraud and abuse act, then they may become influenced through another individual with whom they share electronic communications. This theory which was developed to help explain white collar crime fits in well with those who violate or commit cybercrime. According to a research conducted by Imhof (2010), a lot of systems hacking occur in colleges. Many of these individuals spend time with people who share similar interests.

Differential association is a theory with a number of postulations which help to explain the causes behind why cybercrimes are increasing so quickly in the society and how an individual learn to become a cybercriminal.

There are a wide spectrum of the different kind of offenders and motivations.

Literature Review

According to Vladimir (2005) internet is a global network which unites millions of computer located in different countries and open broad opportunities to obtain and exchange information but it is now been used for criminal purposes due to the economic factors. Nigeria a third world country is faced with so many economic challenges such as poverty, corruption, unemployment amongst others, thereby, making this crime thrive.

However, it will be inconclusive to base it only on economic challenge as the cause of cyber-crime in Nigeria; there might be other causes too. Agba (2002), is of the view that internet is the most technologically advanced medium of interaction. It is the information revolution that has turned the world into a global village.

As a result of this value, it is assumed that internet usage in Nigeria is growing due to increasing availability of broadband connections and by observation, a decrease in subscription fee. This observed increase of internet users in Nigeria has made the internet a popular medium of communication and interaction as well as forum for on – line enterprises, such as, internet service provision (ISP), cyber cafes and cybercrime which was described by Ayantokun (2006) as all unlawful activities involving computer and internet.

The internet services have reduced the world into a global village which makes it look as if everybody is in the same place at a particular point in time, aside from the fact that the internet has made communication to be easier and faster. A lot of other transactions are consummated at the speed of lightening. Oyewole and Obeta (2002), state that the internet is the inter connection of computer across the world thereby creating unlimited opportunities for mankind. According to Ehimen and Bola (2009), the internet has created a geometric growth and accelerated windows of opportunities for businesses and the removal of economic barriers hitherto faced by nations of the world. Considering these limitless advantages of the internet, one can easily subscribe to the fact that it is an important tool for national development in a developing country like Nigeria.

McConnel (2000), argued that cybercrimes differ from most terrestrial crimes in four ways which are: They are easy to learn; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present and they are often not clearly illegal. As such, cybercrime has become one of the major security issues for law enforcement agencies and the world in general. According to a publication by Economic and Other Financial Crime Commission in Nigeria named Zero

Tolerance (2006), stated that a retired civil servant with two (2) other accomplices defrauded a German citizen name Klaus Wagner a sum of USD 1, 714,080 through the internet. A 2007 internet crime report listed Nigeria third in terms of online crime activity and the prevalence of cybercrime among a sizeable number of young Nigerians (Sesan, 2010).

Ribadu (2007), stated that the prominent forms of cybercrime in Nigeria are cloning of websites, false representations, internet purchase and other e – commerce kinds of fraud. Olugbodi (2010), states that the most prevalent forms of cybercrime are website cloning, financial fraud, identity theft, credit card theft, cyber theft, cyber harassment, fraudulent electronic mails, cyber laundering and virus/ worms/ Trojans.

The internet creates unlimited opportunities for commercial, social and educational activities. However, it has introduced its own peculiar risk that poses danger to the economy. The danger could affect many sectors of the society and put the development of the country into peril. Some of these possible adverse effects could include the destruction of the country's image both at home and abroad, insecurity of both life and properties, fear of doing business with Nigerian's citizen, economic loss of spending substantial amount of money on the prevention and control of cybercrime amongst others.

Asokhia (2010) in his work, titled "Enhancing National Development and Growth through Combating Cybercrime/ Internet Fraud", carried out a comparative study of young adult's perception of cybercrime in two Local Government Area of Edo State. His findings were that cybercrime were very prevalent in two Local Government Areas. More revealing is the fact the impact of television that the young people are aware of and the uncensored video and radio programmes also evolve in one kind of cybercrime or the other.

Adam (2008) in his work, "The impact of internet crime on development", concludes that the internet is overwhelmingly a powerful tool for development. Paradoxically, the internet is a

"double- edged sword", providing many opportunities for individuals and organizations to develop but at the same time, has brought with it new opportunities to commit crime. He argues that the internet presents new challenges to law enforcement in both development and developing countries. However, developing countries suffer greatly from the activities of internet crime more than their developed counterparts as developing countries have inadequate technology, infrastructure and insufficient law enforcement expertise.

Ajayi (2006), he examined cybercrime as a phenomenon that is dysfunctional to the country. Evidence abound that is not only the persons that are duped that suffer for this, the immediate family dependants as well as the society where these victims are from, directly feel the effect of this act. The perpetrators country, also suffers the image problem, even to the extent of losing billions of naira, legitimate investment that is supposed to come to the country. Hence, the companies that ought have established and employed the unemployed Nigerian cannot come to the country. Thus, unemployment continues to rampage the country.

An Overview of Cybercrime

Cybercrime refers to any crime that involves a computer and a network. The computer may have been used in the commission of the crime or it may be the target. Cybercrime has also been defined by Dr Debarati Halder and Dr K. Jaishankar (2011) 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 directly or indirectly, using modern telecommunication networks such as internet (chat rooms, emails, notice boards and groups), and mobile phones (SMS/MMS). Such crimes may threaten nation's security and financial health. Issues surrounding these types of crime have become high- profile, particularly those surrounding cracking, copyright infringement, child pornography and child grooming. There are also problems of breaches of privacy, when confidential information is intercepted or disclosed lawfully or otherwise. Nigeria has the largest Internet population in Africa, estimated at about 56 million by Freedom House in Its 2013 Freedom on the Net report. 57.9% of the Internet traffic being via mobile phones and the latter is largely accountable for the surge in its penetration rate from 27% in 2011 to 33% in 2014. This buttresses the increasingly important role of the Internet across societal sector and the indispensable need for the provision of a legal.

The Nature of Cyber-crimes in Nigeria

The following categories of crime are the most common ones in the Nigerian cyber space.

(a) Hucksters: The hucksters are characterized by a slow turnaround from harvest to first message (typically at least 1 month), a large number of messages being sent to each harvested spam trapped addresses, and typical product based Spam (i.e. Spam selling an actual product to be shipped or downloaded even if the product itself is fraudulent).

(b) Fraudsters: The fraudsters are characterized by an almost immediate turnaround from harvest to first message (typically less than 12 hours), only a small number of messages are sent to each harvested addresses (e.g. phishing, "advanced fee fraud"-419 from the Nigerian perspective). Fraudsters often harvest addresses and send only a message to them all at a particular time. The major tool for getting addresses is the mailing address extractor [13,14]

(c) Piracy: Piracy involves the illegal reproduction and distribution of software applications, games, movies and audio CDs. [9, 10, 18, 16]. This can be done in a number of ways. Usually pirates buy or copy from the Internet an original version of a software, movie or game and illegally make copies of the software available online for others to download and use without the notification of the original owner of the software. This is known as Internet piracy or Warez. Modern day piracy may be less dramatic or exciting but is far subtler and more extensive in terms of the monetary losses the victim faces. This particular form of Cybercrime may be the hardest of all to curb as the common man also seems to be benefiting from it [6, 7].

(d) Hacking: Young Nigerians can be observed on daily basis engaging in brainstorming sessions at Cyber Cafés trying to crack security codes for ecommerce, ATM cards and e-marketing product sites. The surprising thing is that even with their low level of education or understanding of the intricacies of computing techniques, they get results!

(e) Phishing: Phishing is also becoming popular as criminals simulate product websites to deceive innocent Internet users into ordering products that are actually non-existent.

(f) Spam: 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 ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, television advertising and file sharing network spam. 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 (Saul, 2007).

(g) 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. 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 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.

(h) Drug Trafficking Deals: Another type of Cyber Crime is Drug Trafficking; it is a global trade involving cultivation, manufacture, 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. (www.wikipedia.com).

(i) Malware: Malware refers to viruses, Trojans, worms and other software that gets onto your computer without you being aware it's there. 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 stolen assets are removed one slice at a time.

(j) 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), Justin (2010). Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties. (www.wikipedia.com)

(k) 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 FTP (which is used to transfer files from one machine to another) or Telnet (which lets the user log in remotely to another machine)--the sniffer collects that information. Additional programs sift through the collected information, pull out the important pieces (e.g., the user names and passwords), and cover up the existence of the sniffers in an automated way. Best estimates are that in 1994 as many as 100,000 sites were affected by sniffer attacks. (David *et al*, 1995)

Emerging cyber tricks in Nigeria

- **Beneficiary of a Will Scam**: The criminal sends e-mail to claim that the victim is the named beneficiary in the will of an estranged relative and stands to inherit an estate worth millions.
- **Online Charity**: Another aspect of e-crime common in Nigeria is where fraudulent people host websites of charity organizations soliciting monetary donations and materials to these organizations that do not exist. Unfortunately, many unsuspecting people have been exploited through this means.
- **Next of Kin Scam**: Collection of money from various bank and transfer fees by tempting the victim to claim an inheritance of millions of dollars in a Nigerian bank belonging to a lost relative.
- **The "Winning Ticket in Lottery you never entered" Scam:** These scams lately include the State Department's green card lottery.
- **Bogus Cashier's Check**: The victim advertises an item for sale on the Internet, and is contacted
- **Computer/Internet Service Time Theft**: Whiz kids in Nigeria have developed means of connecting Cyber Cafes to Network of some ISPs in a way that will not be detected by the ISPs and thereby allow the Cafes to operate at no cost.
- **Lottery scam:** allowing users believe they are beneficiaries of an online lottery that is in fact a scam.

Causes of Cyber Crime in Nigeria

The Nigerian population census in 2006 reveals that Nigeria is a country with about 160 million people. This write up discusses some of the reasons that may cause cybercrime in Nigeria

a) Urbanization: Urbanization is one of the causes of Cybercrime in Nigeria; it is the massive movement of people from rural settlement to Cites. According to Wikipedia urbanization is looked at as the massive physical growth of urban areas as a result of rural migration in search for a better life. This result in a heavy competition amongst the growing populace more especially the elites, as such the elites find it lucrative to invest in the crime of cyber because it is a business that requires less capital to invest and they are popularly called "Yahoo Boys". Meke (2012), in his article "Urbanization and cybercrime in Nigeria" reiterated urbanization as one of the major causes of cybercrime in Nigeria and Urbanization will be beneficial if and only if good jobs can be created in the cities where population growth is increasing, in his article, he emphasized that urbanization without crime is really impossible. As such the elites amongst them find it lucrative to invest in the cybercrime because it is a business that requires less capital.

b) Unemployment: Cybercrime can be associated with high rate of unemployment, harsh economic conditions, and poor educational system. According to the Nigerian National Bureau of Statistics, Nigeria is saddled with almost 20 million unemployed people, with about 2 million new entrants into the dispirited realm of the unemployed each year. This clearly reveals that a lot of youths are not employed. There is an adage that says "an idle mind is the devils workshop", as such most of our youth will use their time and knowledge as a platform for

their criminal activity, in order to improve their livelihood and to make ends meet.

c) **Quest for Wealth:** Another cause of cybercrime in Nigeria is quest for wealth, there exist a large gap between the rich and the average, as such many strive to level up using the quickest means possible, since for any business to thrive well, the rate of return in the investment must be growing at a geometric rate with a minimal risk. Most cyber criminals require less investment and a conducive environment. Nigeria is such an environment and many cyber criminals take advantage of that.

d) **Weak Implementation of Cyber Crime Laws and Inadequate Equipped Law Agencies**
The Nigerian legislation must implement strict laws regarding cyber criminals and when criminal offences occur, perpetrators must be punished for the crime they've committed because cybercrimes reduces the nation's competitive edge, failure to prosecute, cyber criminals, can take advantage of the weak gaps in the existing penal proceedings. Weak /fragile laws regarding cyber criminals exist in Nigeria, unlike in the real world were criminals such as armed robbers are treated with maximum penalties. Unfortunate the nation is not well equipped with sophisticated hardware to track down the virtual forensic criminals. Laura (2012) state that "African countries have been criticized for dealing inadequately with cybercrime as their law enforcement agencies are inadequately equipped in terms of personnel, intelligence and infrastructure, and the private sector is also lagging behind in curbing cybercrime" Nigeria is not an exception to this rule. Furthermore, it is therefore paramount that the nation's legislation should ensure proper implementation of their laws against cybercrime.

e) **Negative Role Models** Youths are mirrors of the society, but it is quite unfortunate how parents neglect their rightful duties. Meke (2012) remarked that today many parents transmits crime values to their wards, via socialization as if it a socio cultural values which ought to be transmitted to the younger generation. Imagine a situation where the child supplies the father with vital information to wreck individual's banks account using the computer system, while the mother impersonates the account holder/owner at the bank. If this culture is imbibed among the younger generations most of them will see no wrong in cybercrime practices.

Challenges of cybercrime

Tunji Ogunleye, an ICT security consultant and a member of Nigeria Cyber Crime Working Group (NCWG) disclosed that the rate of e-crime in Nigeria has outgrown the rate of Internet usage in the country. He said Nigeria is the 56th out of 60 countries embracing Internet usage but third in the fraud attempt category. We are tempted to ask why there is such an upsurge of e-crime in Nigeria and what are the factors that made Nigerians so vulnerable to e-crime?

- **Domestic and international law enforcement**: A hostile party using an Internet connected computer thousands of miles away can attack internet- connected computers in Nigeria as easily as if he were next door. It is often difficult to identify the perpetrator of such an attack, and even when a perpetrator is identified, criminal prosecution across national boundaries is problematic.
- **Unemployment**: The spate of unemployment in Nigeria is alarming and growing by the day. Companies are folding up and financial institutions are going bankrupt. The federal government has proposed a mass sack of government workers. Companies are also embarking on mass sacks of staff. Financial institutions have put unreasonable age barriers on who is eligible to apply for jobs and embarked on mass lay-offs of staff based on ad-hoc decisions.
- **Poverty Rate**: On the global scale, Nigeria is regarded as a third world country. The poverty rate is ever increasing. The rich are getting richer and the poor are getting poorer. Insufficient basic amenities and an epileptic power supply have grounded small scale industries.
- **Corruption**: Nigeria was ranked third among the most corrupt countries in the world. Until 1999, corruption was seen as a way of life in Nigeria.
- **Lack of Standards and National Central Control**: Charles Emeruwa, a consultant to Nigeria Cyber Crime Working Group (NCCWG), said lack of regulations, standards and computer security and protection act are hampering true e-business. Foreign Direct Investment (FDI) and foreign outsourcing are encouraging computer misuse and abuse.
- **Lack of Infrastructure**: Proper monitoring and arrest calls for sophisticated state of the art Information and Communication Technology devices.
- **Lack of National Functional Databases**: National database could serve as a means of tracking down the perpetrators of these heinous acts by checking into past individual records and tracing their movements.
- **Proliferation of Cybercafés**: As a means of making ends meet, many entrepreneurs have taken to establishment of cybercafés that serve as blissful havens for the syndicates to practice their acts through night browsing service they provide to prospective customers without being guided or monitored.
- **Porous Nature of the Internet**: The Internet is free for all with no central control. Hence, the state of anarchy presently experienced.

Effects of Cyber Crimes on Business

1. **Intellectual Property Losses:** The most important area for loss is in the theft of intellectual property and business-confidential information—economic espionage. It is difficult, however, to precisely estimate the losses. This is in part because cyber spying is not a zero-sum game. Stolen information is not really gone. Spies can take a company's product plans, its research results, and its customer lists today, and the company will still have them tomorrow. The company may not even know that it no longer has control over that information.
2. **Business Confidential Information:** The line between Business Confidential Information and IP is inexact. Business Confidential Information can include trade secrets or "know how." These categories are similar to IP and their loss imposes similar costs. We distinguish between IP—information that makes it easier to produce a competing product and Business Confidential Information—information that give an advantage in commercial negotiations or in developing competing

business strategies. While it may take years for stolen IP to show up in a competing product, there is no delay in monetizing stolen confidential business information. Theft of oil exploration data, sensitive business negotiation data, or even, insider stock trading information can be used immediately by the acquirer. The damage to individual companies can be great.

3. **Reputational Damage:** While companies fear reputation damage, there has been little work to quantify it. Companies suffer reduced valuation after public reporting of their being hacked, usually in the form of a drop in stock prices. These losses can be significant— ranging from 1% to 5%—but appear not to be permanent. Stock prices usually recover by the next quarter. It would distort any calculation of loss to attempt to include these fluctuations in stock prices. However, it will be interesting to see if this changes as a result of new SEC regulations that require companies to report major hacking incidents, which may improve shareholder understanding about what hacks are commercially material.
4. **Increased Cost of Security:** It is also necessary to consider, as some studies have done, expenditures on cyber security as part of the total cost of cyber espionage and cybercrime. One estimate predicts that governments and companies spend perhaps 7% of their information technology budgets on security. Another estimate put annual spending globally on cyber security software at $60 billion, growing at about 8% a year. The US Office of Management and Budget reported that in 2012, federal agencies spent more than $15 billion on cyber security-related projects and activities, accounting for 20% of all federal spending on information technology.
5. **Opportunity Costs:** A calculation of the cost of malicious cyber activity would need to consider opportunity costs, forgone opportunities, or lost benefits that would otherwise have been obtainable for activities in cyberspace. Additional spending on cyber security that would not be required in a more secure environment is one example of an opportunity cost. Other examples include lost sales or lower productivity, a decision to avoid the internet for some activities.
6. **Reduces The Competitive Edge Of Organizations:** Computer crimes over the years have cost a lot of havoc to individuals, private and public business organization within and outside the country, causing a lot of financial and physical damage. Due to cyber-crime, there has being loss of billions of dollars annually globally speaking, such crimes may threaten a nation's security and financial health, a company can suffers losses due to computer crime when a hacker steals confidential information and future plans of the company. And he simply sells the information to a competitor company; this will automatically reduce the competitive strength of the company.
7. **Time Wastage and Slows Financial Growth:** Wastage of time is another problem because many IT personals may spend a lot of time on handling, rectifying harmful incidents which may be caused by computer criminals. The time spent should have earned a profit to the organization. One peculiar problem is that, when a hacker enter in an organization and steals confidential information from the company the people who entrust the company loses their confidence in the company as the company may contains confidential information like credit cards of customers and as the information is stolen the customer will not trust the company again and will move to someone else who could protect their confidential information.
8. **Slows Production Time and Add to Over Head Cost:** Computer crime reduces the productivity of a company, as a company will take measure to reduce cybercrime, by entering more password or other acts this will take time to do and therefore will affect productivity. Computer crime will increase the cost as to stop viruses and malware companies must buy strong security software to reduce the chances of attacks from such attacks.
9. **Defamation of Image:** With high level of cybercrime in the nation, the slogan "GOOD PEOPLE GREAT NATION" by Nigerians will be tarnished and global community will view the other side of the coin. Other effects include the consumption of computer and network resources, and the cost in human time and attention of dismissing unwanted messages.

Review of Offences and Penalties

Offences against Critical National Information Infrastructure

By the provisions of the Bill any person who commits any offence punishable under the Act against any critical national information infrastructure designated is liable on conviction to imprisonment for a term of not less than fifteen years without an option of fine.

Unlawful Access A Computer

A term of not less than two years or a fine of not less than N5,000,000 or to both fine and imprisonment is prescribed for any person, who without authorization or in excess of authorization, intentionally accesses in whole or in part, a computer system or network.

Unlawful Interception of Communication

The Bill also prescribed that any person, who intentionally. and without authorization or in excess of authority: intercepts by technical means, transmissions of non-public computer data, content data or traffic data, including electromagnetic emissions or signals from a computer, computer system or network carrying or emitting signals, to or from a computer, computer system or connected system or network; commits an offence and liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than N5,000,000.00 or to both fine and imprisonment.

Unauthorized Modification of Computer Data

The Bill stipulates a term of not less than 3 years or a fine of not less than N7, 000,000.00 or to both fine and imprisonment to anyone who directly or indirectly does an act without authority and with intent to cause an unauthorized modification of any data held in. any computer system or network.

Also the practice of engaging in the act of damaging, deletion, deteriorating, alteration, restriction or suppression of data within computer systems or networks, including data transfer from a computer system by any person without authority or in

excess of authority will attracts the punishment of a term not less than three years or an option of fine of not less than N7, 000,000.00 or to both fine and imprisonment.

Unlawful Interception of Communications
The relevant provision of the Bill on unlawful interception of communications stipulates that any person, who intentionally. and without authorization or in excess of authority: intercepts by technical means, transmissions of non-public computer data, content data or traffic data, including electromagnetic emissions or signals from a computer, computer system or network carrying or emitting signals, to or from a computer, computer system or connected system or network; commits an offence and liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than N5,000,000.00 or to both fine and imprisonment.

System Interference
The Bill prescribes that any person who without authority or in excess of authority, intentionally does an act which causes directly or indirectly the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference in the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose, commits an offence and liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than N5,000,000.00 or to both tine and imprisonment.

Misuse of Device
On the misuse of device the Bill provides that any person, who unlawfully produces, supplies, adapts, manipulates or procures for use, imports, exports, distributes, offers for sale or otherwise makes available:

a) any devices, including a computer program or a component designed or adapted for the purpose of committing an offence;
b) a computer password, access code or similar data by which the whole any part of a computer, computer system or network is capable of being accessed for the purpose of committing an offence; or
c) any device designed primarily to overcome security measures in any computer, computer system or network with the intent that the devices be utilized for the purpose of violating any provision of the bill, commits an offence and should be liable on conviction to imprisonment for a term of not less than three years or a fine of not less than N7, 000,000.00 or to both imprisonment and fine.

Computer Related Forgery
A term of not less than three years imprisonment or to a fine of not less than N7, 000,000.00 is prescribed by the Bill against any person who knowingly accesses any computer or network and inputs, alters, deletes or suppresses any data resulting in inauthentic data with the intention that such inauthentic data will be considered or acted upon as if it were authentic or genuine, regardless of whether or not such data is directly readable or intelligible.

Computer Related Fraud Identity Then and Impersonation
The Bill provides that any person who knowingly and without authority or in excess of authority causes any loss of property to another by altering, erasing, inputting or suppressing any data held in any computer, whether or not for the purpose of conferring any economic benefits for himself or another person, commits an offence and is liable on conviction to imprisonment for a term of not less than three years or to a fine of not less than N7, 000,000.00 or to both fine and imprisonment.

Identity and Theft Impersonation
The Bill provides that **any** person who in the course of using a computer, computer system or network:

a) knowingly obtains or possesses another person's or entity's identity information with the intent to deceive or defraud; or
b) fraudulently impersonates another entity or person, living or dead, with intent to:

1. gain advantage for himself or another person;
2. obtain any property or an interest in any property;
3. cause disadvantage to the entity or person being impersonated or another person; or will be liable to an imprisonment for a term of not less than three years or a fine of not less than N7,000,000.00 or to both fine and imprisonment

Child Pornography
For the purpose of the Bill, the term "child pornography" is said to include pornographic material that visually depicts:

a) a minor engaged in sexually explicit conduct;
b) a person appearing to be a minor engaged in sexually explicit conduct; and
c) Realistic images representing a minor engaged in sexually explicit conduct.

Also the bill defines the term "child" or "minor" to mean a person below 18 years of age.
"Sexually explicit conduct" was provided to include at least the following real or simulated acts:

a) sexual intercourse, including genital-genital, oral-genital, anal genital or oral-anal, between children, or between an adult and a child, of the same or opposite sex;
b) besliality;
c) masturbation;
d) sadistic or masochistic abuse in a sexual context: or
e) Lascivious exhibition of the genitals or the pubic area of a child. It is not relevant whether the conduct depicted is real or simulated; and

The Bill provides further that any person who intentionally uses any computer or network system in or for:

a) producing child pornography for the purpose of its distribution;
b) offering or making available child pornography;
c) distributing or transmitting child pornography;
d) procuring childpornography for oneself or for another person;

e) possessing child pornography in a computer system or on a computer-data storage medium; commits an offence and is liable on conviction an imprisonment for a term of ten years or a fine of not less than N20,000,000.00 or to both fine and imprisonment.

Cyber Squatting
The Bill provides that any person who, intentionally takes or makes use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by any individual, body corporate or belonging to either the Federal, State or Local Governments in Nigeria, on the internet or any other computer network, without authority or right, or for the purpose of interfering with their use by the owner, registrant or legitimate prior user, commits an offence and is liable on conviction to imprisonment for a term of not less than two years or a fine of not less than N5,000,000.00 or to both fine and imprisonment.

Cyber Terrorism
Life imprisonment is the penalty for any person that accesses or causes to be accessed any computer or computer system or network for purposes of terrorism.

Racist, Gender and Xenophobic
The Bill, provides that anyone who distributes or otherwise makes available, any racist, gender or offences xenophobic material to the public through a computer system or network; and shall be liable on conviction to imprisonment for a term of not less than five years or to a fine of not less than ten million naira or to both fine and imprisonment.
Also anyone who distributes or otherwise makes available, through a computer system to the public, material which denies, approves or justifies acts constituting genocide or crimes against humanity, as defined under the Rome Statute of the International Criminal Court, 1998; commits an offence and shall be liable on conviction to imprisonment for a term of not less than five years or to a fine of not less than ten million naira or to both fine and imprisonment.

Corporate Liability
A body corporate that commits an offence under the proposed Act is to be liable on conviction to a fine of not less than N 10,000,000.00 and any person who at the time of the commission of the offence was a chief executive officer, director, secretary, manager or other similar officer of the body corporate or was purporting to act in any such capacity shall be liable on conviction to imprisonment for a term of not less than two years or a fine of not less than N5,000,000.00 or to both fine and imprisonment;

Duties of Service Providers
The Bill provides that a service provider shall keep all traffic data and subscriber information as may be prescribed by the relevant authority for the time being responsible for the regulation of communication services in Nigeria.
A service provider shall also, at the request of the relevant authority or any law enforcement agency: preserve, hold or retain any traffic data, subscriber information or related content, or release any information required to be kept.

Interception of Electronic Communication
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 collect, record, permit or assist competent authorities with the collection or recording of content 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.

Failure of Service Provider to Perform Certain Duties
It is the duty of every service provider in Nigeria to comply with all the provisions of the proposed Act and disclose any information requested by any law enforcement agency or otherwise render assistance howsoever in any inquiry or proceeding in the court of law.
The proposed Act also provides that a service provider shall, at the request of any law enforcement agency in Nigeria or at its own initiative, provide assistance towards:
a) the identification, apprehension and prosecution of offenders;
b) the identification, tracking and tracing of proceeds of any offence or any property, equipment or device used in the commission of any offence; or
c) the freezing, removal, erasure Of cancellation of the services of the offender which enables the offender to either commit the offence or hide or preserve the proceeds of any offence or any property, equipment or device used in the commission of the offence.
(3) Any service provider who contravenes the provisions of subsection (I) and (2) of this section, commits an offence and shall be liable on conviction to a fine of not less than N I0,000,000.00.

Jurisdiction of Court
The Federal High Court located in any part of Nigeria regardless of the location where the offence is committed or High Court of Federal Capital Territory shall have jurisdiction to try offences under this Act committed:
a) in Nigeria;
b) on a ship or aircraft registered in Nigeria; or
c) by a Nigerian outside Nigeria if the person's conduct would also constitute an offence under a law of the country where the offence was committed; or
d) outside Nigeria, where:
1. the victim of the offence is a citizen or resident of Nigeria; or
2. The alleged offender is in Nigeria and not extradited to any other country for prosecution.

Also the Bill states that the Attorney-General of the Federation shall prosecute offences under the Act subject to the provisions of the Constitution of the Federal Republic of Nigeria, 1999.

Preventive Measures for Cyber Crimes and Technology Misuse
In order to reduce cybercrime and technology misuse to the

barest level if not entirely eliminated from our society, the following preventive measures are recommended:

(i). Awareness and Training
These are the first set of steps in alleviating cybercrimes. The citizens, consumers and organizations should create the awareness of cyber threats and the actions they can take to protect their information. Also, continuous training is necessary for business clients in order to share the responsibility in fighting against cybercrime.

(ii). Ethical and Moral Standards
Ethical standards should be upheld in organizations to ensure confidentiality is served and technology misuses are reduced (Basandra, 2005). Computer ethnics help us to identify offenders and create solutions to aid in the minimization of computer crimes and technology misuse (Moor, 1985).

(iii). Computer Forensics
Computer Forensics technically refers to the use of procedure centric approaches in the study of cyber-attack prevention, planning, detection and response with the goals of counteracting and conquering hacker attacks by logging malicious activity and gathering court admissible chains of evidence using various forensics tools that reconstruct criminally liable actions at the physical and logical levels (O' Connor, 2003; Mandia *el al*, 2001). According to Ibikunle (2005) an advanced computer forensics is the use of steganography, which is the art of hiding communications. Unlike encryption that uses an algorithm and a seed value to scramble or encode a message to make it unreadable; steganography makes the communication invisible. This takes concealment to the next level, which is to deny that the message even exists.

(iv). Cyber Crime Prevention Laws
According to Mc Connell (2000), National government remains the dominant authority for regulating criminal behaviour in most places in the world. If a nation has already struggled from and ultimately improved its legal authority after a confrontation with the unique challenge presented by cybercrime; it is crucial that other nations profit from this lesson and examine their current laws to discern whether they are composed in a technologically neutral manner that would not execute the prosecution of cyber criminals. In many cases, nations will find that current laws ought to be updated. Enactment of enforceable computer crime laws that also respect the rights of individuals are an essential next step in the battle against this emerging threat (Mc Connell, 2000). The attacker sophistication seems to be ahead of defensive tools. That is the nature of the war between hacker and defenders; the attackers are always a step ahead. But by making the attackers' job harder and harder, and by increasing the length of gaol sentences for cybercrime and improving international police co-operation and skill levels, we can combine to keep up with the attackers and over time begin to turn the tide (Paller *et al*, 2007)

(v). Encryption (or Cryptography)
This involves scrambling data into an unreadable format called cipher text before it is transmitted over a telecommunication link between two computers, and then unscrambling that data again when it gets to its destination computer. Only those who possess the secret key can decipher (or decrypt) the message into plain text. If data is not encrypted during transmission, it can easily be intercepted by unauthorized party thereby making the third party to have access to the information. Encrypted messages can sometimes be broken by cryptanalysis, also called code-breaking; although modern cryptography techniques are virtually unbreakable. Cryptography is used to protect e-mail messages, credit card information and corporate data.

(vi). Anti- Virus
Anti-virus is a software program that is used to protect computer system against the menace of viruses. The effect of this software is to detect and remove a virus from a computer system before it does any damage to it. These software programs can readily be purchased from software stores or downloaded from the internet. Examples of antivirus software are: Shield Deluxe, CA anti-virus, BitDefender, Avira, Kaspersky, Avast, Norton, NOD32, Dr. Solomon, MCAFFEE, MSAV and AVG.

(vii). Firewall
Firewalls are made up of software and hardware placed between an organization's internal and external networks to prevent outsiders from invading their networks. Firewalls are programmed to intercept and examine any message packet passing between the two networks and reject unauthorized messages.

(viii). Passwords
Passwords are unique set of characters that may be allocated to an individual, a particular system or facility that must be input to allow access. Passwords are security measure used by the majority of computer users which allows only authorized user to gain access to the system. The lack of password on a computer system increases the risk of unauthorized access. To prevent hackers and crackers from penetrating your network, it is recommended that you use passwords that are difficult to guess. It is better you make your passwords a mixture of letters, numbers and special characters such as: @, $, %, ', &, *, # etc. Moreover, you should always change your password at regular intervals and set a minimal length of passwords such as a minimum of six or eight characters (Olumoye, 2011).

Effects of Cyber Crime
- Financial loss: Cybercriminals are like terrorists or metal thieves in that their activities impose disproportionate costs on society and individuals.
- Loss of reputation: most companies that have been defrauded or reported to have been faced with cybercriminal activities complain of clients losing faith in them.
- Reduced productivity: this is due to awareness and more concentration being focused on preventing cybercrime and not productivity.
- Vulnerability of their Information and Communication Technology (ICT) systems and networks.

Solutions to cybercrime
- **Education:** Cybercrime in Nigeria is difficult to prove as

it lacks the traditional paper audit trail, which requires the knowledge of specialists in computer technology and internet protocols; hence We need to educate citizens that if they are going to use the internet, they need to continually maintain and update the security on their system. We also need to educate corporations and organizations in the best practice for effective security management. For example, some large organizations now have a policy that all systems in their purview must meet strict security guidelines. Automated updates are sent to all computers and servers on the internal network, and no new system is allowed online until it conforms to the security policy.

- **Establishment of Programs and IT Forums for Nigerian Youths:** Since the level of unemployment in the country has contributed significantly to the spate of e-crime in Nigeria, the government should create employments for these youths and set up IT laboratories/forum where these youths could come together and display their skills. This can be used meaningfully towards developing IT in Nigeria at the same time they could be rewarded handsomely for such novelty.
- **Address Verification System:** Address Verification System (AVS) checks could be used to ensure that the address entered on your order form (for people that receive orders from countries like United States) matches the address where the cardholder's billing statements are mailed.
- **Interactive Voice Response (IVR) Terminals:** This is a new technology that is reported to reduce charge backs and fraud by collecting a "voice stamp" or voice authorization and verification from the customer before the merchant ships the order.
- **IP Address tracking:** Software that could track the IP address of orders could be designed. This software could then be used to check that the IP address of an order is from the same country included in the billing and shipping addresses in the orders.
- **Use of Video Surveillance Systems:** The problem with this method is that attention has to be paid to human rights issues and legal privileges.
- **Antivirus and Anti spyware Software:** Antivirus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software. Anti-spy wares are used to restrict backdoor program, Trojans and other spy wares to be installed on the computer.
- **Firewalls:** A firewall protects a computer network from unauthorized access. Network firewalls may be hardware devices, software programs, or a combination of the two. A network firewall typically guards an internal computer network against malicious access from outside the network.
- **Cryptography:** Cryptography is the science of encrypting and decrypting information. Encryption is like sending a postal mail to another party with a lock code on the envelope which is known only to the sender and the recipient. [20] A number of cryptographic methods have been developed and some of them are still not cracked.
- **Cyber Ethics and Cyber legislation Laws:** Cyber ethics and cyber laws are also being formulated to stop cyber-crimes. It is a responsibility of every individual to follow cyber ethics and cyber laws so that the increasing cyber-crimes will reduce. Security software like anti viruses and anti-spy wares should be installed on all computers, in order to remain secure from cyber-crimes. Internet Service Providers should also provide high level of security at their servers in order to keep their clients secure from all types of viruses and malicious programs.[7]

Conclusion and recommendations

As the general population becomes increasingly refined in their understanding and use of computers and as the technologies associated with computing become more powerful, there is a strong possibility that cyber-crimes will become more common. Nigeria is rated as one of the countries with the highest levels of e-crime activities. Cyber security must be addressed seriously as it is affecting the image of the country in the outside world. A combination of sound technical measures tailored to the origin of Spam (the sending ends) in conjunction with legal deterrents will be a good start in the war against cyber criminals. Information attacks can be launched by anyone, from anywhere. The attackers can operate without detection for years and can remain hidden from any counter measures". This indeed emphasizes the need for the government security agencies to note that there is need to keep up with technological and security advancements. It will always be a losing battle if security professionals are miles behind the cyber criminals. Fighting cybercrime requires a holistic approach to combat this menace in all ramifications. There is need to create a security-aware culture involving the public, the ISPs, cybercafés, government, security agencies and internet users. Also in terms of strategy, it is crucial to thoroughly address issues relating to enforcement. Mishandling of enforcement can backfire.

References

1. Adebusuyi A. The Internet and Emergence of Yahooboys sub-Culture in Nigeria, International Journal Of Cyber-Criminology, 0794-2891, 2008; 2(2):368-381.
2. Agba PC. International Communication Principles, Concepts and Issues. In Okunna CS. (ed) Techniques of Mass Communication: A Multi-dimentional Approach. Enugu: New Generation Books, 2002.
3. Akogwu S. An Assessment of the Level of Awareness on Cyber Crime among Internet Users in Ahmadu Bello University, Zaria (Unpublished B.Sc project). Department of Sociology, Ahmadu Bello University, Zaria, 2012.
4. Anderson Ross. Measuring the cost of cybercrime, 11th Workshop on the Economics of Information Security 2012. Retrieved from http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf
5. Augustine C, Odinma MIEEE. Cybercrime & Cert: Issues & Probable Policies for Nigeria, DBI Presentation, 2010, 1-2.
6. Awe J. Fighting Cyber Crime in Nigeria. http://www.jidaw.com/itsolutions/security3.html. 2009.
7. Ayantokun O. Fighting Cybercrime in Nigeria, 2006. Information-system.www.tribune.com

8. Ehimen OR, Bola A. Cybercrime in Nigeria. Business Intelligence Journal. 2010; 3(1).
9. Federal College of Education Zaria Students Handbook Revised, 1999.
10. Imhof. Cybercrime and Telecommunication Law. Rochester Institute of Technology USA, 2010.
11. Kumar K. Cyber Laws, International Property and e-commerce Security. Dominant Publishers and Distributors, New Delhi. Global Information. www.mcconnellinformation.com. McConnell international L.L.C, 2003.
12. Halder D, Jaishankar K. Cybercrime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. 2011, ISBN 978-1-60960-830-9.
13. Justin Plot. Top five computer crime and how to protect yourself from them, Publication of Justin plot, 2010.
14. Laura Ani. Cyber Crime and National Security: The Role of the Penal and Procedural Law, 2011.
15. Littman J. The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Paulsen. Boston: Little Brown, 1997.
16. Longe OB, Chiemeke S. Cyber Crime and Criminality in Nigeria – What Roles Are Internet Access Points in Playing. European Journal of Social Sciences. 2008; 6(4).
17. Mbaskei Martin Obono Cybercrimes: Effect on Youth Development, 2008. http://www.i-genius.org accessed 26 the April 2012.
18. Mc Connell. Cybercrime and Punishment. Archaic Law Threaten, 2000.
19. Meke Eze Stanley N. An article Urbanization and Cyber Crime in Nigeria: Causes and Consequences, 2012.
20. Olaide, Adewole. Cyber Crime Embarrassing for Victims. 2004. Retrieved September 2011 from http//www.heraldsun.com.au
21. Olugbodi K. Fighting Cyber Crime in Nigeria. 2010, Retrieved September 10, 2011 from http//www.guide2nigeria,com/news_articles_About_ Nigeria
22. Oyewole, Obeta. An Introduction to Cyber Crime, 2002. Retrieved September 2011 from http//www.crimeresearch.org/articules/cyber-crime.
23. Parker D. Fighting Computer Crimes, U.S. Charles Scribner's Sons, 1983.
24. Http:// www.wikipedia.com.
25. Rathemell A. Cyber-terrorism: The Shape of Future Conflict? Royal United Service Institute Journal. 1997.
26. Ribadu E. Cyber Crime and Commercial Fraud; A Nigerian Perspective. A paper presented at the Modern Law for Global Commerce, Vienna 9th – 12th July. 2007.
27. Sesan G. The New Security War, 2010. http://www.pcworld.com/article/122492/the_new_security_war.htm#tk.mod-rel.
28. Shinder DL. Scene of the Cybercrime: Computer Forensics Handbook. Syngress Publishing Inc. Hingham Street, USA, 2002.
29. Sutherland E. Principles of Criminology. Fourth edition, 1939.
30. Vladimir G. International Cooperation in Fighting Cyber Crime, 2005.www.crimeresearch.org
31. Zero Tolerance Retiree in Trouble over Internet Fraud. Economic and Financial Crime Commission, 2006; 1(2)