CHAPTER ONE

1.0 INTRODUCTION

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. With Nigeria venturing into cashless society, there is a need for cybercrimes menace to be minimized if not completely eradicated. Some of the ways of combating such crimes include taking reasonable steps to protect ones property by ensuring that firms 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.

Cyber Crime is one of the words frequently used by individuals in our contemporary Society. To understand the true meaning of cybercrime, there is the need to understand the slit meaning of Cyber and Crime. The term Cyber is a prefix used to describe an idea as part of the computer and Information age and Crime Can be described as any activity that contravenes legal procedure mostly performed by individuals with a criminal motive. 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 directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones". Such crimes may threaten a nation's security and financial health. Cybercrime can simply be explained as crimes carried out with the aid of a computer system. The internet has offered a lot of platform for useful research purposes; However, Cybercrime is a worldwide problem that's costing countries billions of dollars. According to crime-research.org, as early as 2003 the United States was already leading the world in percentage of cyber-attacks at 35.4 percent, followed by South Korea at 12.8 percent. Countries with high rates of computer piracy, such as Russia, have reacted slowly to cyber crime. As a result, many hackers and other cyber criminals can flourish in countries with few Internet

crime laws while attacking richer countries through their computer because it lacks rules and codes of a central authority which governs it as such internet has no geographical demarcation as remarked by Guillane and Fortinet (2009). In Nigeria, cybercrimes are perform by people of all ages ranging from young to old, but in most instances the young. Several youth 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 by many. Mbaskei in his publication on "Cybercrimes: Effect on Youth Development" noted that secret agents of the UPS (United Parcel Service) smashed a record scam with a face value of $2.1billion (about N252 billion) in Lagos. The interception was done within three months. Some of the instruments uncovered by the UPS were documents like Wal Mart Money orders, Bank of America cheques, U.S postal service cheques and American Express traveler's cheques. This record scam is made possible as a result of the large number of young people who now see Cybercrimes or internet fraud as a source of livelihood. This study tends to look at Cybercrime, its causes, effects and suggests ways to combat such crimes as it affects Nigeria. The world of internet today has become a parallel form of life and living. Public are now capable of doing things which were not imaginable few years ago. The Internet is fast becoming a way of life for millions of people and also a way of living because of growing dependence and reliance of the mankind on these machines. Internet has enabled the use of website communication, email and a lot of anytime anywhere IT solutions for the betterment of human kind.

Cybercrime is emerging as a serious threat. Worldwide governments, police departments and intelligence units have started to react. Initiatives to curb cross border cyber threats are taking shape. Indian police has initiated special cyber cells across the country and have started educating the personnel. Crime and criminality have been associated with man since his fall. Crime remains elusive and ever strives to hide itself in the face of development. Different nations have adopted different strategies to contend with crime depending on their nature and extent. One thing is certain, it is that a nation with high incidence of crime cannot grow or develop. That is so because crime is the direct opposite of development. It leaves a negative social and economic consequence. Cybercrime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. It is very difficult to classify crimes in general into distinct groups as many crimes evolve on a daily basis. Even in the real world, crimes like rape, murder or theft need not necessarily be separate. However, all cybercrimes involve both the

computer and the person behind it as victims; it just depends on which of the two is the main target. Hence, the computer will be looked at as either a target or tool for simplicity's sake. For example, hacking involves attacking the computer's information and other resources. It is important to take note that overlapping occurs in many cases and it is impossible to have a perfect classification system.

The term cybercrime is a misnomer. This term has nowhere been defined in any statute /Act passed or enacted by the Indian Parliament. The concept of cybercrime is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which cause breach of rules of law and counterbalanced by the sanction of the state

1.1 TYPES OF CYBER CRIMES

Cybercrimes simply put are crimes that are committed using the Computers and Networks. There are several types of cybercrimes some of which include:

A. CYBER TERRORISM

A cyber terrorist can be described as someone who launches attack on government or organization in order to distort and or access stored information stored on the computer and their networks. According to Wikipedia, a cyber terrorist is someone who intimidates a government or to advance his or her political or social objectives by launching computer-based attack against computers, network, and the information stored on them. For instance, a rumor on the Internet about terror acts. In addition, Parker (1983) defined Cyber terrorism as an act of terrorism committed through the use of cyberspace or computer resources. It means that any act intended to instill fear by accessing and distorting any useful information in organizations or Government bodies using Computer and Internet is generally referred to as Cyber Terrorism. Another form of cyber terrorism is cyber extortion is a form of cyber terrorism in which a website, e-mail server, computer systems is put under attacks by hackers for denial of services, demanding for ransom in return. Cyber extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service.

B. 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.

C. 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).

D. 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.

E. 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.

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). Spamming remains economically viable because advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high. A person who creates electronic spam is called a spammer, (Gyongyi, 2005). There are a number of ways that physical methods can breach networks and communications, for instance, if telephone and network wiring is often not protected as well as it should be, both from intruders who can physically damage it and from wiretaps that can pick up the data flowing across the wires. Criminals sometimes use wiretapping methods to eavesdrop on communications. It's unfortunately quite easy to tap many types of network cabling. For example, a simple induction loop coiled around a terminal wire can pick up most voices. Telephone fraud has always been a problem among crackers, but with the

increasing use of cellular phones, phone calling cards, and the ordering of merchandise over the phone using credit cards, this problem has increased dramatically in recent years. Communications Security, it's important to physically secure all networks cabling to protect it both from interception and from vandalism. It has been reported that the notorious American hacker Kevin Poulsen was able to gain access to law enforcement and national security wiretap data prior to his arrest in 1991 (Littman, 1997). In 1995, hackers employed by a criminal organization attacked the communications system of the Amsterdam Police. The hackers succeeded in gaining police operational intelligence, and in disrupting police communications (Rathmell, 1997).

G. LOGIC BOMBS

A typical logic bomb tells the computer to execute a set of instructions at a certain date and time or under certain specified conditions. The instructions may tell the computer to display "I gotcha" on the screen, or it may tell the entire system to start erasing itself. Logic bombs often work in tandem with viruses. Whereas a simple virus infects a program and then replicates when the program starts to run, the logic bomb does not replicate – it merely waits for some pre-specified event or time to do its damage. Time is not the only criterion used to set off logic bombs. Some bombs do their damage after a particular program is run a certain number of times. Others are more creative. There are several reported cases that a programmer told the logic bomb to destroy data if the company payroll is run and his name is not on it.; this is a sure-fire way to get back at the company if he is fired! The employee is fired, or may leave on his own, but does not remove the logic bomb. The next time the payroll is run and the computer searches for but doesn't find the employee's name, it crashes, destroying not only all of the employee payroll records, but the payroll application program as well. Logic bombs present a major threat to computer systems, not just because of the damage they themselves can do, but because they provide a technique to facilitate more devastating crimes.

H. 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)

1.2 EFFECTS OF CYBERCRIME

People in the whole world are affected by cybercrime all time but most of the cases are unreported. In the UK there were 92,000 cases of online identity fraud during 2006. Around 40% of all identity frauds are facilitated online. The most stolen documents used by fraudsters were utility bills, passports and bank statements. 10% people in Australia suffered by on-line frauds. In 2000, of the 45,950 computer crimes reported by the NIBRS2, 5,744 were crimes where the computer was the tool and 40,211 were crimes where the computer was the object. The most common type of computer crime for both definitions was larceny/theft. Internet Crime Complaint Center (IC3) reported that 206,884 complaints were filed online for an estimated $239 million loss in 2007. In Britain it is estimated that there were 207,000 cases of online financial fraud during 2006,among them Card-not-present (CNP) fraud was 49% and the total value of loss of CNP fraud are from £183.2M to £212.6M. About 42% financial fraud (Fraud, Credit Card, Money Laundering) occurred in Australia during the year 2005 and 2006. In the Middle East over the past few years banks lost approximately one billion dollars to organized cybercrime on online transactions and most banks in the region are vulnerable to phishing attacks. UK banking association APACs warned that online banking fraud losses were £21.4m in the six months to June 2008. FBI survey reported that the annual loss due to computer crime was estimated at $67 billion for U.S.A in 2005. By the innovation of the Internet and the World Wide Web (WWW) has created a fictitious world filled with an unlimited amount of information, which dramatically changed the underground world of child pornography. By unexpectedly becoming the new medium for intent, motive, and ambition, the Internet has become a vital part of the child pornographer’s criminal tradecraft. Half (49%) of Canadians have come across websites that contain pornography. Of those that have come across pornographic websites, 83%

came across it unexpectedly and 46% found it offensive. 13% of Internet users came across content that promotes hate or violence to a particular group. 8% of Canadians who used the Internet had received threatening or harassing e-mail. Australian Federal Police reported that about 35% Child

Pornography, 8% Child Grooming (using the internet and mobile phones), 4% Family Violence/Sexual Assaults occurred in Australia during the year 2005 and 2006. In Britain during 2008 there were 500 new cases of online child abuse reported every month. In

Tahlequah a criminal took some pictures of undressed girls illegally and posted the pictures to their family and showed them exposing themselves, after proving that this criminal was accused and sent her to jail and financial punishment. In Britain 1,944,000 cases of online harassment placed during 2006. Cisco Systems Inc. found an alarming increase in the amount of personalized spam, which online identity thieves create using stolen lists of e-mail addresses or other poached data about their victims. Spam is growing quickly nearly 200 billion spam messages are now sent each day, double the volume in 2007 and that targeted attacks are also rising sharply. About 800 million messages a day are attempts are spear phishing in SANFRANSISCO. One in four (23 per cent) of UK internet users surveyed reckon either they or their close friends and family had been a victim of phishing scams during the last 12 months. In Bangladesh, Prime Minister Sheikh Hasina got a threat by e-mail from a cybercafé and World Bank, Dhaka office got a threat through e-mail. Virus is the new dimension of cybercrime. About 6,000,000 virus incidents took place in Britain during 2006. A virus named “Love Bug” which destroyed files and stole passwords. The virus was ultimately estimated to have affected at least forty-five million users in more than twenty countries. NASA and CIA also affected through this virus. ”Hacking” is a specific concept of stolen data and information from any computer through network. In Bangladesh lots of incident occurred during last year such as stolen the transactions report of Dhaka Stock Exchange, Hacking the e-mail of BRAC Bangladesh, Inserted porno movies in the website of Bangladesh national parliament, Jamate Islami Bangladesh, the Daily Jugantor. Theft of telecommunication services occur everyday in the world .Computer hackers in the United States illegally obtained access to Scotland Yard's telephone network and made £620,000 worth of international calls and Scotland yards had to responsible to pay that bill. A hacker broke the voice-mail system of HUB Computer Solutions in Winnipeg and made calls worth of $43,000 and the company had to pay that unwanted bill. Thieves hacked the Internet

phone systems of WA businesses and used the phone system to make more than 11,000 international telephone calls in 46 hours that worth $120,000 and the Company paid that amount.

1.3 HISTORY OF CYBERCRIME

The first recorded cyber crime took place in the year 1820! That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage. In 1820, 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. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber crime! Today computers have come a long way, with neural networks and nano-computing promising to turn every atom in a glass of water into a computer capable of performing a Billion operations per second. Cyber crime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants is being run on computers, cyber crime has assumed rather sinister implications. Major cyber crimes in the recent past include the Citibank rip off. US $ 10 million were fraudulently transferred out of the bank and into a bank account in Switzerland. A Russian hacker group led by Vladimir Kevin, a renowned hacker, perpetrated the attack. The group compromised the bank's security systems. Vladimir was allegedly using his office computer at AO Saturn, a computer firm in St. Petersburg, Russia, to break into Citibank computers. He was finally arrested on Heathrow airport on his way to Switzerland

1.4 ADVANTAGES

1. It helps automate various tasks that cannot be done manually.
2. It helps organize data and information in a better way and it has much more computing and calculating power than human.
3. It may be the storage of important data and files.

1.5 DISADVANTAGES

1. It may damage your studies and social life.
2. The way it distracts can deviate our thoughts and activities towards unproductive activities.
3. It could cause violation of privacy.

Computer crime is the criminal activities that are committed on the internet which includes plotting a virus, hacking someone else's computer and stealing data. Today the internet is growing very rapidly and it has both advantages and disadvantages. Computer crime or Cybercrime is one of the major disadvantages. Computer Crime can be categorized into different types. Computer crimes targets computer devices or computer network directly and also targets independent computer devices or computer networks. This type of cyber crimes are identity theft, scams, stalking, fraud, and hacking. This paper generates the insight about the overall rise in losses occurring from the computer fraud. The main focus of this paper is to describe the types of computer crimes and its effect on individuals and businesses. This study focuses the extent of cyber stalking, victimizing, and the regulation of business on the internet.

1.6 DEFINITION OF TERMS

1. **CYBER:** Pertaining to the internet
2. **NETWORKS:** To connect two or more computers or other computerized devices
3. **INTERNET:** Any set of computer networks that communicate using the internet protocol
4. **DATA:** A representation of facts or ideas in a formalized manner capable of being communicated or manipulated by some process
5. **DEVICE:** Any piece of equipment made for a particular purpose, especially a mechanical or electrical one

CHAPTER TWO

2.0 LITERATURE REVIEW

Cybercrime, or computer related crime, is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Debarati Halder and K. Jaishankar (2002) define cybercrimes 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, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS). Cybercrime may threaten a person or a nation's security and financial health.[4] Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, unwarranted mass-surveillance, child pornography, and child grooming Saul H(2007):. There are also problem of privacy when confidential information is intercepted or disclosed, lawfully or otherwise. Debarati Halder and K. Jaishankar further define cybercrime from the perspective of gender and defined 'cybercrime against women' as "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones. Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyberwarfare.

Crime and criminality have been associated with man since his fall. Crime remains elusive and ever strives to hide itself in the face of development. Different nations have adopted different strategies to contend with crime depending on their nature and extent. One thing is certain, it is that a nation with high incidence of crime cannot grow or develop.

That is so because crime is the direct opposite of development. It leaves a negative social and economic consequence. Cybercrime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. It is very difficult to classify crimes in general into distinct groups as many crimes evolve on a daily basis. Even in the real world, crimes like rape, murder or theft need not necessarily be separate. However, all cybercrimes involve both the computer and the person behind it as victims; it just depends on which of the two is the main

target. Hence, the computer will be looked at as either a target or tool for simplicity's sake. For example, hacking involves attacking the computer's information and other resources. It is important to take note that overlapping occurs in many cases and it is impossible to have a perfect classification system.

2.1 CRIME AND CYBER CRIME

The crime committed in Cyber world is a common matter of present world. Basically Cybercrime is a complex crime and its range is so vast. There is no specific or all accepted definition of cybercrime because different agencies and researchers gave the definition according to their place and situation. It can say the cybercrimes are that crimes which have the involvement of computer and network (Fafinski and Kowalski 2002). To give the definition of cybercrime some researchers told that the crime committed with internet and information technology (Sheridan, 2004). It has some different name such as computer crime, computer-related crime, high-tech crime, Internet crime (Kowalski, 2002).

There are many types of cybercrime existing in present world. It is very difficult to find out all types of cybercrime because every day the new dimension of cybercrime is inventing. We can cite few types of cybercrime, which occur generally in every place of the world. Identity fraud is a type (Blindell, 2006), parliamentary joint committee on the Australian crime commission 2004:43, Brenner and Goodman 2002: 7). It is defined as the assumption of the identity of another person, living or dead, irrespective of the motivation underlying these courses of actions (Fafinski, 2008). Identity fraud is used as a means to commit drug, firearms and e-crime offences (parliamentary joint committee on the Australian crime commission 2004). Identity fraud refers to the gaining of money, goods, services or other benefits through the use of a false identity (ACPR 2006:14). In the United States of America, the term 'Identity theft' is generally used to cover all types of identity crime, The United Kingdom government appears to use 'identity fraud' as a generic term, In Australia, definitions adopted within policing entail the use of identity crime as a generic description to cover all types of identity crime (ACPR, 2006). Another type of cybercrime is "Financial Fraud" (Fafinski 2008 and Graycer, 2000). It is defined as the use of deception for direct or indirect Financial or material gain (Fafinski, 2008). It includes Internet banking, credit and debit card fraud, and money laundering (Graycer, 2000), parliamentary joint committee on the Australian crime commission 2004:47). In the context of credit card, financial

fraud defied as unlawfully obtained credit card numbers to order goods or services online (Kowalski, 2002). Offences against the person are a common type of cybercrime (Fafinski, 2008). It includes the use of a computer to cause an individual some form of personal harm such as anxiety, distress or psychological harm, precisely we can say threatening e-mails and the posting of derogatory information online is the best example of that crime (Fafinski, 2008). Another type Computer misuse means unauthorized access to a computer system such as basic hacking, aggravated hacking and unauthorized modification of computer material such as viruses (Fafinski, 2008). Sexual offences are most concerning types of cybercrime at present because of the availability of pornography (Fafinski, 2008). We can also give a relevant name that is Pornography and Other Offenses against Morality it includes child pornography and other offenses against minors, stalking, harassment, hate speech etc. (Brenner and Goodman, 2002). This category of cybercrime covers a range of conduct that has an objectively ascertainable sexual elements including pedophilic activity such as grooming a child for sexual activity. At present Spam, Phishing, Botnets are the matter of concern at Cyber world because it causes lots of harm of computer system and data management (Jaishankar P and Hyde 2007). Theft of Telecommunications Services The phone phreakers do it by gaining access to an organisation's telephone switchboard individuals or criminal organizations can obtain access to dial-in/dial-out circuits and then make their own calls or sell call time to third parties (Graycer, 2000). Telecommunications Piracy means the temptation to reproduce copyrighted material for personal use, for sale at a lower price, or indeed, for free distribution, has proven irresistible to many (Graycer, 2000).

2.2 THE INTERNET

Internet is becoming popular day by day because of its some special features. A revolutionary change has come in communication and socio-economic transaction by internet. Being facilitated with the virtue of it, people can communicate very easily national as well as international level. Generally it is called on-line communication. It is the vast source of information. We can get any information from the Internet. Though it is the easiest way of communication, now it is the matter of concern that misuse of computer and internet put together some people to commit crime. According to Council of Europe “Any criminal offence committed against or with the help of a computer network is identified as cybercrime (Council of Europe Convention on

Cybercrime, 2001). So computer is must for cybercrime. Generally Among the numerous crimes in today's society; cybercrime has become very common as well as very dangerous. The emergence of new technology has increased the number of perpetrators that take advantage of these resources to use them illegally for their own gain (Gjata, 2007).

The most dangerous aspect of cybercrime is that the victims fail to acknowledge the cause of their unfortunate fate. Not only should victims report any sort of suspicion and/or crime, but the victim needs to identify the suspected machine so police can confiscate it in order to have evidence gathered form the machine's hard drive.

Without having the computer form which the perpetrator committed his crime(s) then it is very hard to convict and persecute these perpetrators. Victims of cybercrime need to become aware of such crimes and they need to become more educated in how to protect and prevent not only themselves but others as well from such malicious acts. With today's advanced technology the urgent need of information security, ethical education and awareness programs cannot be emphasize enough in order to achieve the maximum protection from the hackers and also to protect Cyber world from our own abusive use (Gjata, cybercrime 2007) Numerous government agencies around the world have taken necessary precautions to detect and persecute perpetrators of cybercrime. Although, because of the vast amount of new technology being produces regularly government agencies have to stay alert and informed in order to control cybercrime. Cybercrime can be victimless, but it can also harm unfortunate individuals.

2.3 A NOTE ON CYBERCRIME

Cybercrime is a worldwide problem now; no country is immune (El-Guindy, 2008). The first cybercrimes occurred in India, Japan and china in 1820(Techno focus cybercrime-A looming threat 2008). After that it was increasing evolutionary and at mid of 20th century it became a problem of concern. Around the world and in

Middle East and third world countries the growth of Internet connectivity in recent years is significant and simultaneously similar increase in cybercriminal activities (El-Guindy, 2008). We see in 2001 approximately 28.5 million people in the UK use the Internet (Fafinski, 2008). Internet use in the Middle East had reached 2.5% of the total worldwide use by December 2007 (El-Guindy, 2008). 50% adult use Internet in Australia (Australian federal police: 4). In

Bangladesh Internet was first introduced in 1996 (Hossain, 2004). Foskett said Internet users are growing rapidly in Bangladesh especially in the metropolitan areas. In 2000, the number of Internet users were 100,000 and it shot up to 450,000 in 2007. In another report says about 2 million people use internet in Bangladesh (Hossain, 2004) In Canada by the year 2000 the 45,950 computer crimes reported by the NIBRS2 and noted that most common type of computer crime was larceny/theft (Kowalski, 2002). By the years cybercrimes develop besides technical development and by time it created new dimension of crime such as from telecommunication crime to electronic money laundering (Graycar, 2000). Because of cybercrime people lost their money, identity and many more. In the UK there were 92000 cases of on-line identity fraud during 2006 because of that average value of loss from 183.2 to 212.6 million pounds by card-not-present (CNP) fraud. 218.817 incidents of physical harassment were recorded. In 2006 850000 cases of unwanted online sexual approaches occurred (Fafinski, 2008). 38% Drug Importation cases, 34% Defraud the commonwealth cases, 25% Child Sex related cases, 3% Counterfeit currency/documents cases, 45% E-Crime, 11% Interpol, 2% Counter terrorism, 42% Others (Fraud, Credit Card, Money Laundering) occurred in Australia during 2005 and 2006 (Australian federal police: 4-5). The systems of NASA, US Army, Navy and Department of Defence were hacked right after the 9/11 attacks. Spam is now a great problem in cyber world everyday thousands of Spam spreading through e-mail and other way. Nearly 200 billion Spam messages are now sent each day, double the volume in 2007 and that targeted attacks are also rising sharply and 90 percent of all e-mails sent worldwide are Spam, this means 800 million messages a day are attempts are spear phishing. One in four (23%) of UK internet users had been victim of phishing scams during the last 12 months, compared to just eight per cent the year before. Similarly, more than one in six (16%) had fallen victim to other types of online scam. One of the most important issues is child pornography. Because of the Internet pornography industries generate approximately 3 billion US dollars annually and there are roughly100000 websites offering illegal child pornography (Young, 2008). In Tahlequah Michael Ray Wright had pictures of under aged girls during April 1 & Dec 18, 2008. Australian Broadcasting Authority found 54% credit card number theft, 45% personal data misuse, 39% privacy issues and 21% incidents because of viruses (Barbara, 2002). On the top of the list of cybercrimes registered in 2006 there are 1.94 million cases of harassment, this figures includes e-mails with threatening or abusive statements and offensive allegations left on websites and about

850,000sex crimes including cyber stalking occurred in Britain. Considering the contemporary and early history it is found, 1st world countries are most affected because they were reported but we have no chronological data about cybercrime in our country. The impact of cybercrime is not as alarming in Bangladesh because financial transactions have not yet been fully facilitated online, said Freddy Tan, chief security advisor of Microsoft Southeast Asia. He warned that, as soon as financial transactions are allowed, online computer crimes would increase at an unprecedented rate, unless the government acquires the tools and infrastructure to prevent, detect and prosecute them. 'Online financial scams are a major threat for banks, credit card holders and alike. Internet services provided through the local area network are vulnerable to similar attacks and intrusions by hackers more often when security level was inadequate. According to a government study conducted by the Bangladesh computer council, only 0.3 % of the total population own computers and 0.7% have access to the Internet. The government statistics for cybercrime are not remarkable, but district judge have been empowered to try cases in reference to the panel code of criminal procedure. The limited number of cybercrime apprehended is confined to e-mail threat (Hammadi, 2008). An example is that E-mail threatening to such organization and renowned person in Bangladesh (Borhan, 2006).

Bangladesh government has launched the initiative of making digital Bangladesh. But the use of internet is limited in this country. People mainly use internet for their educational purpose. Bangladesh is a safe haven for anyone committing a computer crime. From viruses (which infect computers to malfunction), Trojans (deceptive software or malware that appears to perform an action but instead performs another) and Spam to online threats, piracy, hacking (accounts), theft (of data or pin numbers) and pornography, all these facts of computer crime have advanced significantly beyond existing modes of detection So there is no doubt that how important matter that is for the contemporary situations in Bangladesh at the rising time of Internet technology.

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 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.

3.1 EFFECTS OF CYBER CRIME IN NIGERIA

A. 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 cybercrime, 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.

B. 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.

C. 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.

D. 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 includes the consumption of computer and network resources, and the cost in human time and attention of dismissing unwanted messages

3.2 COMBATING CYBER CRIME IN NIGERIA

Cybercrime cannot be easily and completely eliminated, but can be minimized. However, collaborative efforts of individuals, corporate organization and government could go a long way reduce it to a minimal level. Firms should secure their networked information. Other measures to taking include:

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

2. Governments should assure that their laws apply to cybercrimes. African countries are bedeviled by various socio-economic problems such as poverty, AIDS, fuel crisis, political and ethnic instability and other related crimes. This limits their strength to effectively combat cybercrime. Nevertheless, it is important that Nigeria as a nation take measures to ensure that its penal and procedural law is adequate to meet the challenges posed by cybercrimes. The Government must ensure laws are formulated and strictly adhered to. **3.** Individuals should observe simple rules Individuals on their part should ensure proper anti-malware protection on their computer systems, individuals should be encouraged to avoid pirated software, never to share their Personal Identification Number(PIN), bank account, email access code to unknown persons, never disclose any confidential information to anybody as none of these networks were design to be ultimately secure. Ignore any e-mail requiring any financial information. Report particularly evil spam to the appropriate authorities as suggested by Justin (2010). Mbasekei (2008) suggested that Telecommunication Regulatory Agencies should enhance security on internet service providers' server in other to detect and trace cybercrimes and creation of job opportunities for the teeming unemployed youths will go a long way in minimizing the menace.

3.3 PREVENTION OF CYBER CRIME

Prevention is always better than cure. It is always better to take certain precaution while operating the net. A should make them his part of cyber life. Saileshkumar Zarkar, technical advisor and network security consultant to the Mumbai Police Cyber crime Cell, advocates the 5P mantra for online security: Precaution, Prevention, Protection, Preservation and Perseverance. A netizen should keep in mind the following things

1. To prevent cyber stalking avoid disclosing any information pertaining to one self. This is as good as disclosing your identity to strangers in public place.
2. Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
3. Always use latest and update antivirus software to guard against virus attacks.
4. Always keep back up volumes so that one may not suffer data loss in case of virus contamination
5. Never send your credit card number to any site that is not secured, to guard against frauds.
6. Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.It is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.
7. Web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.
8. Use of firewalls may be beneficial.
9. Web servers running public sites must be physically separate protected from internal corporate network. Adjudication of a Cyber Crime - On the directions of the Bombay High Court the Central Government has by a notification dated 25.03.03 has decided that the Secretary to the Information Technology Department in each state by designation would be appointed as the AO for each state.

CHAPTER FOUR
SUMMARY AND CONCLUSION

4.0 SUMMARY

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 world of internet today has become a parallel form of life and living. Public are now capable of doing things which were not imaginable few years ago. The Internet is fast becoming a way of life for millions of people and also a way of living because of growing dependence and reliance of the mankind on these machines. Internet has enabled the use of website communication, email and a lot of anytime anywhere IT solutions for the betterment of human kind.

The term 'cybercrime' is a misnomer. This term has nowhere been defined in any statute /Act passed or enacted by the Indian Parliament. The concept of cybercrime is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which cause breach of rules of law and counterbalanced by the sanction of the state

4.1 CONCLUSION

Capacity of human mind is unfathomable. It is not possible to eliminate cybercrime from the cyber space. It is quite possible to check them. History is the witness that no legislation has succeeded in totally eliminating crime from the globe. The only possible step is to make people aware of their rights and duties (to report crime as a collective duty towards the society) and further making the application of the laws more stringent to check crime. Undoubtedly the Act is a historical step in the cyber world.

For Nigeria to serve as a fertile ground for economic break through, it must be built on a crime free society. But an ideal economy is virtually not possible, because as technology increases so also crime rate. Cyber criminals will always keep in pace with any technological advancement. It is true that Technology gives rise to cybercrime. The future of our economy lies in our hands, the future itself is the summation of our decisions so we should believe in ourselves and endeavor to

do the right thing at each point in time, following carefully the suggestions of this paper. Until then, the dreamed society will not become a reality.

REFERENCES

Guillaume F, (2009): Fighting Cybercrime: Technical, Juridical and Ethical Challenges VIRUS BULLETIN CONFERENCE Available at http://www.igenius.org. on 4th June 2003.

Halder, D., and Jaishankar, K. (2011): Cybercrime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9.

Littman, J. (1997): The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Paulsen. Boston: Little Brown. Available at http://www.igenius.org. on 12th May 2002

Mbaskei O. (2008): Cybercrimes: Effect on Youth Development Available at http://www.igenius.org accessed 26 April 2012.

Malware (2012) and Justin Plot (2010): Top five computer crime and how to protect yourself from them, Publication of Justin plot Available at www.wikipedia.com accessed 26 April 2003.

Parker D (1983): Fighting Computer Crimes, U.S. Charles Scribner's Sons. Available at Http:// www.wikipedia.com. On 3 June 2010.

Rathemell, A. (1997): Cyber-terrorism: The Shape of Future Conflict? Royal United Service Institute Journal Available at www.wikipedia.com on 9 September 1999.

Meke N. (2012): An article "Urbanization and Cyber Crime in Nigeria: Causes and Consequences" Available at http://www.igenius.org on 4 January 2001.

Saul H (2007): Social network launches worldwide spam campaign New York Times Available at www.crime-research.org on 12 July 2008.