CHAPTER ONE

1.0 INTRODUCTION

1.1 BACKGROUND OF THE STUDY

Internet referred to as a network of networks is a global network of computers for the sole purpose of information sharing and dissemination. The relevance of information in almost every works of life makes access to the internet a very crucial aspect to everyone. As far back as the early 1990s, the Internet was argued to be a unique medium showing the fastest speed of diffusion in human history (Nguyen and Alexander, 1996). Today, there are very few people whose lives are not affected beneficially and/or harmfully by the technology of the Internet era. On the positive side, the ability to share and exchange information instantaneously has provided unprecedented benefits in the areas of education, commerce, entertainment and social interaction. On the negative side, it has created increasing opportunities for the commission of crimes – information technology has enabled potential offenders to commit large-scale crimes with almost no monetary cost and much lesser risk of being caught. Compared to perpetrators of traditional economic-motivated crimes (e.g., burglaries, larcenies, bank robberies), online fraudsters are relatively free of worry from directly encountering law enforcement and witnesses (Internet Journal of Criminology, 2011).

According to Prof. Dr. Marco Gercke (2012), the Internet is one of the fastest-growing areas of technical infrastructure development. Today, information and communication technologies (ICTs) are omnipresent and the trend towards digitization is growing. The demand for Internet and computer connectivity has led to the integration of computer technology into products that have usually functioned without it, such as cars and buildings. Electricity supply, transportation infrastructure, military services and logistics – virtually all modern services depend on the use of ICTs. Although the development of new technologies is focused mainly on meeting consumer demands in western countries, developing countries can also benefit from new technologies. With the availability of long-distance wireless communication technologies such as WiMAX5 and computer systems that are now available for less than USD 2006, many more people in developing countries should have easier access to the Internet and related products and services. The influence of ICTs on society goes far beyond establishing basic information infrastructure. The availability of ICTs is a foundation for development in the creation, availability and use of network-based services. E-mails have displaced traditional letters; online web representation is nowadays more important for businesses than printed publicity materials; and Internet-based communication and phone services are growing faster than landline communications. The availability of ICTs and new network-based services offer a number of advantages for society in general, especially for developing countries. ICT applications, such as e-government, e-commerce, e-education, e-health and e-environment, are seen as enablers for development, as they provide an efficient channel to deliver a wide range of basic services in remote and rural areas. ICT applications can facilitate the achievement of millennium development targets, reducing poverty and improving health and environmental conditions in developing countries. Given the right approach, context and implementation processes, investments in ICT applications and tools can result in productivity and quality improvements. In turn, ICT applications may release technical and human capacity and enable greater access to basic services. In this regard, online identity theft and the act of capturing another person's credentials and/or personal information via the Internet with the intent to fraudulently reuse it for criminal purposes is now one of the main threats to further deployment of e-government and e-business services.

With the continuous advancement of Internet technology and personal computing devices in recent years, Internet crimes have risen to an alarming level. For instance, in the U.S., the National White Collar Crime Center (2008, p. 2) reported a 33.1% increase in citizen complaints of Internet crimes between 2007 and 2008, and this figure is reflective particularly of the increased incidence of identity theft. Another source of information also indicated that the number of identity thefts increased more than tenfold within a 9-year period – growing from 31,140 incidents in year 2,000 to 313,982 in 2008 (Federal Trade Commission, 2009). In addition, identity theft remained the top one complaint category filed by the victims across years (Federal Trade Commission, 2009, 2010, 2011). Evidence from victimization survey also pointed out that about 5% of Americans aged 16 and above were victims of successful and attempted identity theft within two years, and the direct financial damage to the victims were as high as 16 billion dollars (Bureau of Justice Statistics, 2010). These statistics coincide with the notion of ―Crime of the New Millennium as the phenomenon quickly emerged in the 21st century (Hoar, 2001; Poster, 2006).

As crimes have advanced with technology, the breadth of online services and the number of users have continued to increase. We have witnessed that the Internet has made users‘ lives easier and has begun to link together varied segregated services (e.g., telecommunications, banking, investing, pharmacy, social interaction, education, entertainment) and devices (e.g., computers, servers, smart phones, even electronic chips in individual household air conditioning).

The integration of such diverse technological applications coupled with the rapid growth of online users make fraudulent activities likely to rise further, if no intervention is proposed and implemented.

The costs of Internet services are often also much lower than comparable services outside the network. E-mail services are often available free of charge or cost very little compared to traditional postal services. The online encyclopaedia Wikipedia15 can be used free of charge, as can hundreds of online hosting services. Lower costs are important, as they enable services to be used by many more users, including people with only limited income. Given the limited financial resources of many people in developing countries, the Internet enables them to use services they may not otherwise have access to outside the network.

On the basis of this upward trend, this project aims to examine identity theft from an analytic angle with a focus on the expanded versatilities of this contemporary crime. In the present article, the mechanism of identifying an individual is first discussed, followed by the definition and typology of identity theft. Elements and methods of identity theft will be deconstructed for classification, and subsequent discussions will be emphasized on recent variations in online fraud. The study will conclude with the implications of the close relations between identity theft and the fast growing Internet, and suggestions for improved means of identity protection.

1.2 STATEMENT OF THE PROBLEM

Despite the need for the internet, its emergence in Nigeria birthed the major heart-break of cybercrime. The following are the problem posed by the emergence of internet in Nigeria:

- **Data interference: -** i.e. interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data; misuse of devices, forgery (ID theft) and electronic fraud (Paul Taylor, 1999).
- **Fraudulent Business Transactions:** A very few criminally minded youth in the country (Nigeria), who are mostly not educated or graduates, are stealing and committing atrocity through the aid of the internet online business transactions. The internet online business services, which ordinarily supposed to be a blessing as it exposes one to a lot of opportunities in various field of life is fast becoming a source of discomfort and worry due to the atrocity being perpetrated through it.
- **Impersonation/ False Pretence**
- **Storming of the stock exchange market by the cyber criminals called "Yahoo-boys"**

- **Creation of false bank accounts for fraudulent online transactions:-** Punjab National Bank suffered a loss of close to Rs. 1. 39 chore when the recorders were manipulated to create false debits and credits. In bank of Baroda, Rs 2.5 lakh was misappropriated through the computerized creation of false bank accounts (Krishna Kumar. 2003)
- **Telecommunication Line reversal**
- **Cyber murder**
- **Socio-economic Breakdown as a result of too many criminal activities taking place on the internet**

All stated above are the problems associated with the use of the internet. When we measure the advantages of using the internet against its disadvantages, we can draw a conclusion that there is a need for proper check of all these problems. A quick action must be invoked in order to appreciate the advantages of internet to the Nigerian citizens, most especially students (the youths).

1.3 AIMS AND OBJECTIVES OF THE STUDY

The reasons and assumed products of this project are as follows:

- To provide a clear overview of cyber-crime and cyber-security.
- To provide methods through which cyber security can be improved.
- To outline the challenges associated with cybercrime in Nigeria.
- To carry out a research on the view of Nigerian students on cyber-crime.
- To identify the most perpetrators of cyber-crime in Nigeria.
- To provide the unemployed Nigerian ICT expert with alternatives to cyber-crime.

1.4 BENEFITS OF THE STUDY

Some of the benefits of this study include:

- Increased knowledge of the current trend of cyber-crime and cyber security to computer users as well as programmers.
- Computer programmers' ability to design a more secure application with low overhead.
- This study will enable users reduce the vulnerability of their information and communication technology (ICT) to attack.
- Unemployment of Nigerian IT professionals will be reduced by giving them alternative source of livelihood.

1.5 SCOPE OF THE STUDY

This project is limited to students in senior secondary schools in Shomolu Local Government area, especially students offering computer science as a subject. It is intended to measure their involvement in cyber-crime through series of approaches ranging from their personal views to a more general view. The study also intends to highly respect the opinion of the students in order to achieve maximum results.

1.6 RESEARCH METHODOLOGY

One or more of following methods would be used in carrying out this research work for the purpose of data gathering and analysis:

1. **Interview**: Various students within the scope of this research will be interviewed to get their views about the subject matter.

2. **Direct Observation**: Another method is carrying out a close watch of the population under consideration in order to gather some information which are general or common to several people.

3**. Questionnaire**: A questionnaire is designed for data collection and analysis.

1.7 DEFINITION OF TERMS

- **CYBER CRIME**: Cybercrime are criminal activities carried out through the internet.
- **CYBER SPACE**: Cyberspace is a world that contains just about anything one is searching for. Cyber-space refers to the boundless space known as the internet.
- **CYBER MURDER**: This is a cybercrime that involves the death of its victim.
- **CYBER SECURITY**: Cyber-security is the body of rules put in place for the protection of the cyber space
- **E-MAIL**: Electronic mail is the transmission of messages over telecommunication networks.
- **ICT**: Stands for Information and Communication technology, it refers to all the technology used to handle telecommunications, broadcast media, intelligent building management system, audiovisual processing and transmission systems, and network based control and monitoring functions.
- **IT (Information Technology)**: It is a combination of computing and telecommunication facility.
- **NETWORK**: A network is a group of two or more computer systems linked together.
- **PROGRAMMER**: This is an IT professional who writes programs.
- **TELECOMMUNICATION**: Telecommunications refers to the exchange of information by electronic and electrical means over a significant distance
- **BACK DOOR***:* secret (undocumented), hard-coded access codes or procedures for accessing information. Some back doors exist in commercially-provided software packages; e.g., consistent (canonical) passwords for third-party software accounts. Alternatively, back doors can be inserted into an existing program or system to provide unauthorized access later. A program with an undocumented access method is an example of a Trojan Horse.

- **BOT**: for “robot” – a program used for a specific function such as keeping a port open or launching a flood of packets in a distributed denial-of-service attack.

- **BOTNET**: a set of bots installed (usually surreptitiously) on a number of victimized computers (zombies or slaves) to launch distributed denial-of-service attacks or to send spam.

- **CRACKING**: malicious or criminal hacking. Unauthorized penetration of computer systems and networks, abuse of privilege, unauthorized use of services.

- **DATA DIDDLING**: modifying data for fun and profit; e.g., modifying grades, changing credit ratings, altering security clearance information, fixing salaries, or circumventing book-keeping and audit regulations.

- **DATA LEAKAGE**: uncontrolled, unauthorized transmission of classified information from a data center or computer system to the outside. Such leakage can be accomplished by physical removal of data storage devices (diskettes, tapes, listings, printouts and photographs of screen copies or handwritten notes) or by more subtle means such as data hiding (steganography) or even plain old human memory.

- **DENIAL-OF-SERVICE (DOS) ATTACK***:* overwhelming or saturating resources on a target system to cause a reduction of availability to legitimate users. On the Internet, usually involves spoofing packets or e-mail headers.

- **DISTRIBUTED DOS (DDOS) ATTACK**: Internet-mediated attack accomplished by enlisting the services of many compromised systems to launch a denial of service (DoS).

- **DNS CACHE POISONING**: modifying data in a Domain Name System (DNS) server so that calls to particular Websites or even entire domains are misdirected for fraudulent purposes.

- **EASTER EGG**: undocumented, unauthorized program functions in a production program; a kind of Trojan Horse.

- **EXPLOIT**: a method for exploiting a vulnerability to take control of a system or otherwise compromise it. Exploits are sometimes automated in scripts.

- **HACKING**: for many years, a noble endeavor involving intense study, dedicated analysis and hands-on learning about any technical field, including computing. Unfortunately, despite the best efforts of computer hobbyists worldwide, since the early 1980s, thanks largely to the ignorance of undereducated journalists, the term has become almost synonymous with cracking. Some die-hards continue the battle by referring to “criminal hacking” but it’s probably too late to reverse the shift in meaning.

- **HACKTIVISM (SOMETIMES SPELLED HACTIVISM):** politically- or ideologically-motivated vandalism. Defacing a Web site for no particular reason is vandalism; the same defacement to post political propaganda or to cause harm to an ideological opponent is hacktivism.

- **IDENTITY THEFT**: creating a false identity using someone else’s identifying information (e.g., name, Social Security Number, birthday) to create new credit cards or establish loans which then go into default and affect the original victim’s credit record.

- **IMPERSONATION**: pretending to be authorized to enter a secure location. Examples include swaggering into a site equipped with what look like tool kits of the manufacturer of computer equipment, or pretending to be a janitor. Impersonation is a key element of social engineering.

- **LATENCY**: the period during which a time bomb, logic bomb, virus or worm refrains from overt activity or damage (delivery of the payload). Long latency coupled with vigorous reproduction can result in severe consequences for infected or otherwise compromised systems.

- **LOGIC BOMB**: A program in which damage (the payload) is delivered when a particular logical condition occurs; e.g., not having the author's name in the payroll file. Logic bombs are a kind of Trojan Horse; time bombs are a type of logic bomb. Most viruses are logic bombs.

- **MAIL-BOMBING**: sending large numbers of unwanted e-mail messages to a single recipient or to a group of such recipients. To be distinguished from spamming. Mail-bombing is a form of denial of service.

- **MALWARE**: malicious software, including Trojan Horses, viruses, worms, logic bombs, exploits and time bombs.

- **MASTER PROGRAM**: in distributed denial-of-service (DDoS) attacks, a program that communicates with implanted zombie or slave programs on compromised systems. The master program usually transmits encrypted instructions to zombies with details of which targeted system to swamp with junk transmissions at exactly what time.

- **PAYLOAD**: the unauthorized activities of malicious software.

- **PENETRATION**: unauthorized access to restricted systems or resources.

- **PIGGYBACKING**: entering secure premises by following an authorized person through the security grid; also unauthorized access to information by using a terminal that is already logged on with an authorized ID (identification).

- **PHARMING**: misdirecting traffic from one Website to a Website controlled by a criminal hacker by altering the domain name system (e.g., by DNS cache poisoning) or by altering configuration files on a victim's computer.

- **PHISHING**: using a forged or spoofed e-mail or Web site that imitates or duplicates an official communication or page to trick victims into revealing logon or other confidential information that can be used for penetration, financial fraud or identity theft.

- **ROOT KIT:** a script or set of scripts for gaining unauthorized *root* privileges (or equivalent supervisory powers) on a compromised system. Much used by *script kiddies.*

- **SABOTAGE**: the word comes from the French for wooden shoe (*sabot*). Such footwear made a handy weapon for throwing into the gears of new mechanical systems that were causing unemployment during the industrial revolution of the 18th and 19th centuries. The term now means any deliberate damage to operations or equipment.

- **SALAMI THEFT**: technique of accumulating round-off errors or other small quantities in calculations and saving them up for later withdrawal; usually applied to money, although it can be part of an inventory-theft scheme (for example).

- **SCAVENGING**: using discarded listings, tapes, or other information storage media to determine useful information such as access codes, passwords, or sensitive data. Finding a listing for the source code for a new version of a popular proprietary program could be highly profitable for a computer crook. Also known as D*umpster® diving*.

- **SCRIPTS**: any simple program, especially using a *scripting* or *macro* language; in computer crime work, however, scripts usually refer to automated systems for executing *exploits*.

- **SIMULATION**: using computers to simulate a complex system in order to defraud it; e.g., inventing transactions to produce a pre-arranged bottom line in a financial report.

- **SPAMMING**: a popular name for e-mail sent to many unwilling recipients in order to sell products or services (or sometimes to cheat naïve customers). Those wishing to avoid offending the innocent Hormel Corporation, owners of the Spam® trademark, may refer to this indiscriminate bulk e-mail as junk e-mail or as UCE (unsolicited commercial e-mail).

- **SPIM**: spam over instant messenger

- **SPIT**: spam over internet telephony

- **SPOOFING**: using incorrect identification; usually applied to electronic misrepresentation such as putting the wrong originating address on a TCP/IP packet. Much used in denial-of-service (DoS) and distributed DoS (DDoS) attacks.

- **SUPERZAPPING**: using powerful utility software (originally the superzap utility on IBM mainframes) to access secure information while bypassing normal controls. Debug programs, and disk editors are examples of tools used for superzapping.

- **TIME BOMB**: program or batch file waits for a specific time before causing damage. Often used by disgruntled and dishonest employees who find out they're to be fired or by dishonest consultants who put unauthorized time-outs into their programs without notifying their clients. Logic bombs and time bombs are Trojan Horse programs; time bombs are a type of logic bomb.

- **TROJAN HORSE**: innocent-looking program that has undocumented and nefarious functions. So called by reference to Odysseus' wooden horse filled with soldiers that helped to capture Troy. Trojan Horse programs can, for example, alter data in a particular way, record passwords for later inspection, send confidential information to unauthorized destinations or open *back doors* into compromised systems.

- **VANDALISM**: obvious, unauthorized, malicious modification or destruction of data such as information on Web sites.

- **VIRUS**: Viruses infect executable code such as programs (e.g., .EXE and .COM files under DOS), boot sectors on disks and macro programs. The viral code reproduces with the *host* code is loaded into memory. So called by analogy with biological viruses, which subvert the functions of normal cells. Viruses are similar to worms but reside inside programs at all times. A virus can transform an ordinary program into an unintended Trojan horse.

- **VULNERABILITY**: a weakness or flaw permitting an attack on a computer system or network.

- **WIRETAPPING**: eavesdropping on data or voice transmissions by attaching unauthorized equipment or software to the communications medium (in the case of wires, coaxial metal cables and optical cables) or by intercepting and interpreting broadcast data (in the case of wireless phones, cellular phones, and wireless networks).

- **WORM:** program which spreads through a computer system or network by replicating (like a virus) but without integrating itself into other executable code.

- **ZOMBIE**: a program inserted into a vulnerable system to await further instructions; usually part of a distributed denial-of-service (DDoS) attack.

CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 HISTORY OF THE INTERNET

The Internet has revolutionized the computer and communications world like nothing before. The invention of the telegraph, telephone, radio, and computer set the stage for this unprecedented integration of capabilities. The Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location.

The Internet represents one of the most successful examples of the benefits of sustained investment and commitment to research and development of information infrastructure. Beginning with the early research in packet switching, the government, industry and academia have been partners in evolving and deploying this exciting new technology. Today, terms like “bleiner@computer.org” and “http://www.acm.org” trip lightly off the tongue of the random person on the street (V. G. Cerf and R. E. Kahn, 1974). Technological evolution that began with early research on packet switching and the ARPANET (and related technologies), and where current research continues to expand the horizons of the infrastructure along several dimensions, such as scale, performance, and higher level functionality. There is the operations and management aspect of a global and complex operational infrastructure. There is the social aspect, which resulted in a broad community of Internauts (users of the internet) working together to create and evolve the technology. And there is the commercialization aspect, resulting in an extremely effective transition of research results into a broadly deployed and available information infrastructure. The Internet today is a widespread information infrastructure, the initial prototype of what is often called the National (or Global or Galactic) Information Infrastructure. Its history is complex and involves many aspects - technological, organizational, and community. And its influence reaches not only to the technical fields of computer communications but throughout society as we move toward increasing use of online tools to accomplish electronic commerce, information acquisition, and community operations.

The first recorded description of the social interactions that could be enabled through networking was a series of memos written by J.C.R. Licklider of MIT in August 1962 discussing his “Galactic Network” concept (J.C.R. Licklider & W. Clark, 1962). He envisioned a globally interconnected set of computers through which everyone could quickly access data and programs from any site. In spirit, the concept was very much like the Internet of today. Licklider was the first head of the computer research program at DARPA (IEEE, 1978), starting in October 1962. While at DARPA he convinced his successors at DARPA, Ivan Sutherland, Bob Taylor, and MIT researcher Lawrence G. Roberts, of the importance of this networking concept. Leonard Kleinrock at MIT published the first paper on packet switching theory in July 1961 (L. Kleinrock, 1961) and the first book on the subject in 1964 (L. Kleinrock, 1964). Kleinrock convinced Roberts of the theoretical feasibility of communications using packets rather than circuits, which was a major step along the path towards computer networking. The other key step was to make the computers talk together. To explore this, in 1965 working with Thomas Merrill, Roberts connected the TX-2 computer in Mass. to the Q-32 in California with a low speed dial-up telephone line creating the first (however small) wide-area computer network ever built (L. Roberts & T. Merrill, 1966). The result of this experiment was the realization that the timeshared computers could work well together, running programs and retrieving data as necessary on the remote machine, but that the circuit switched telephone system was totally inadequate for the job. Kleinrock's argument for packet switching was confirmed. The Advanced Research Projects Agency (ARPA) changed its name to Defense Advanced Research Projects Agency (DARPA) in 1971, then back to ARPA in 1993, and back to DARPA in 1996. We refer throughout to DARPA, the current name. In late 1966 Roberts went to DARPA to develop the computer network concept and quickly put together his plan for the "ARPANET", publishing it in 1967 [L, Roberts, 1967). At the conference where he presented the paper, there was also a paper on a packet network concept from the UK by Donald Davies and Roger Scantlebury of NPL. Scantlebury told Roberts about the NPL work as well as that of Paul Baran and others at RAND. The RAND group had written a paper on packet switching networks for secure voice in the military in 1964 (P. Baran, 1964). It happened that the work at MIT (1961- 1967), at RAND (1962-1965), and at NPL (1964 1967) had all proceeded in parallel without any of the researchers knowing about the other work. The word "packet" was adopted from the work at NPL and the proposed line speed to be used in the ARPANET design was upgraded from 2.4 kbps to 50 kbps6. In August 1968, after Roberts and the DARPA funded community had refined the overall structure and specifications for the ARPANET, an RFQ was released by DARPA for the development of one of the key components, the packet switches called Interface Message Processors (IMP's). The RFQ was won in December 1968 by a group headed by Frank Heart at Bolt Beranek and Newman (BBN). As the BBN team worked on the IMP's with Bob Kahn playing a major role in the overall ARPANET architectural design, the network topology and economics were designed and optimized by Roberts working with Howard Frank and his team at Network Analysis Corporation, and the network measurement system was prepared by Kleinrock's team at UCLA. Due to Kleinrock's early development of packet switching theory and his focus on analysis, design and measurement, his Network Measurement Center at UCLA was selected to be the first node on the ARPANET. All this came together in September 1969 when BBN installed the first IMP at UCLA and the first host computer was connected. Doug Engelbart's project on "Augmentation of Human Intellect" (which included NLS, an early hypertext system) at Stanford Research Institute (SRI) provided a second node. SRI supported the Network Information Center, led by Elizabeth (Jake) Feinler and including functions such as maintaining tables of host name to address mapping as well as a directory of the RFC's. One month later, when SRI was connected to the ARPANET, the first host-to-host message was sent from Kleinrock's laboratory to SRI. Two more nodes were added at UC Santa Barbara and University of Utah. These last two nodes incorporated application visualization projects, with Glen Culler and Burton Fried at UCSB investigating methods for display of mathematical functions using storage displays to deal with the problem of refresh over the net, and Robert Taylor and Ivan Sutherland at Utah investigating methods of 3-D representations over the net. Thus, by the end of 1969, four host computers were connected together into the initial ARPANET, and the budding Internet was off the ground. Even at this early stage, it should be noted that the networking research incorporated both work on the underlying network and work on how to utilize the network. This tradition continues to this day. Computers were added quickly to the ARPANET during the following years, and work proceeded on completing a functionally complete Host-to-Host protocol and other network software. In December 1970 the Network Working Group (NWG) working under S. Crocker finished the initial ARPANET Host-to-Host protocol, called the Network Control Protocol (NCP). As the ARPANET sites completed implementing NCP during the period 1971-1972, the network users finally could begin to develop applications. In October 1972 Kahn organized a large, very successful demonstration of the ARPANET at the International Computer Communication Conference (ICCC). This was the first public demonstration of this new network technology to the public. It was also in 1972 that the initial "hot" application, electronic mail, was introduced. In March Ray Tomlinson at BBN wrote the basic email message send and read software, motivated by the need of the ARPANET developers for an easy coordination mechanism. In July, Roberts expanded its utility by writing the first email utility program to list, selectively read, file, forward, and respond to messages. From there email took off as the largest network application for over a decade. This was a harbinger of the kind of activity we see on the World Wide Web today, namely, the enormous growth of all kinds of “people-to-people” traffic.

.

It was from the RAND study that the false rumor started claiming that the ARPANET was somehow related to building a network resistant to nuclear war. This was never true of the ARPANET, only the unrelated RAND study on secure voice considered nuclear war. However, the later work on Internetting did emphasize robustness and survivability, including the capability to withstand losses of large portions of the underlying networks.

2.2.0 OVERVIEW OF CYBER CRIME AND COMPUTER CRIME

2.2.1 DEFINITIONS

Most reports, guides or publications on cybercrime begin by defining the terms “computer crime” and “cybercrime” (Goodman/Brenner, 2002). In this context, various approaches have been adopted in recent decades to develop a precise definition for both terms. Before providing an overview of the debate and evaluating the approaches, it is useful to determine the relationship between “cybercrime” and “computer-related crimes”. Without going into detail at this stage, the term “cybercrime” is narrower than computer related crimes as it has to involve a computer network. Computer-related crimes cover even those offences that bear no relation to a network, but only affect stand-alone computer systems (Prof. Dr. Marco Gercke, 2012)

During the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders, two definitions were developed within a related workshop: Cybercrime in a narrow sense (computer crime) covers any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them. Cybercrime in a broader sense (computer-related crimes) covers any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network (Kumar, 2009).

One common definition describes cybercrime as any activity in which computers or networks are a tool, a target or a place of criminal activity (FBI Law Enforcement Bulletin, 1995). There are several difficulties with this broad definition. It would, for example, cover traditional crimes such as murder, if perchance the offender used a keyboard to hit and kill the victim. Another broader definition is provided in Article 1.1 of the Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism (the “Stanford Draft”), which points out that cybercrime refers to acts in respect to cyber systems. Some definitions try to take objectives or intentions into account and define cybercrime more precisely, such as "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks" (Hayden, Cybercrime's impact on Information security). These more refined descriptions exclude cases where physical hardware is used to commit regular crimes, but they risk excluding crimes that are considered as cybercrime in international agreements such as the Commonwealth Model Law on Computer and Computer-related Crime or the Council of Europe Convention on Cybercrime. For example, a person who produces USB94 devices containing malicious software that destroys data on computers when the device is connected commits a crime as defined by Article 4 of the Convention on Cybercrime (CETS No. 185).

The variety of approaches, as well as the related problems, demonstrates that there are considerable difficulties in defining the terms "computer crime" and "cybercrime". The term "cybercrime" is used to describe a range of offences including traditional computer crimes, as well as network crimes. As these crimes differ in many ways, there is no single criterion that could include all acts mentioned in the different regional and international legal approaches to address the issue, whilst excluding traditional crimes that are just facilitated by using hardware. The fact that there is no single definition of "cybercrime" need not be important, as long as the term is not used as a legal term. Instead of referring to a definition, the following chapters will be based on a typology-related approach i.e. the form the crime takes.

2.2.2 TYPOLOGY OF CYBER CRIME

The term "cybercrime" is used to cover a wide variety of criminal conduct (Sieber, 2014). As recognized crimes include a broad range of different offences, it is difficult to develop a typology or classification system for cybercrime (Gordon/Ford 2006). One approach can be found in the Convention on Cybercrime (CETS No. 185), which distinguishes between four different types of offences:

1. Offences against the confidentiality, integrity and availability of computer data and systems; (CETS No. 185, Art 2-6);
2. Computer-related offences (CETS No. 185, Art 7&8);
3. Content-related offences (CETS No. 185, Art 9) and
4. Copyright-related offences (CETS No. 185, Art 10).

This typology is not wholly consistent, as it is not based on a sole criterion to differentiate between categories. Three categories focus on the object of legal protection: "offences against the confidentiality, integrity and availability of computer data and systems"; content-related offences; and copyright related offences. The fourth category of "computer-related offences" does not focus on the object of legal protection, but on the method used to commit the crime. This inconsistency leads to some overlap between categories. In addition, some terms that are used to describe criminal acts (such as "cyber terrorism" or "phishing") cover acts that fall within several categories. Nonetheless, the four categories can serve as a useful basis for discussing the phenomena of cybercrime.

2.3 DEVELOPMENT OF COMPUTER CRIME AND CYBERCRIME

The criminal abuse of information technology and the necessary legal response are issues that have been discussed ever since the technology was introduced. Over the last 50 years, various solutions have been implemented at the national and regional levels. One of the reasons why the topic remains challenging is the constant technical development, as well as the changing methods and ways in which the offences are committed.

2.3.1 The 1960s

In the 1960s, the introduction of transistor-based computer systems, which were smaller and less expensive than vacuum-tube based machines, led to an increase in the use of computer technology (Slivka/Darrow, 1974). At this early stage, offences focused on physical damage to computer systems and stored data (McLaughlin, 1978). Such incidents were reported, for example, in Canada, where in 1969 a student riot caused a fire that destroyed computer data hosted at the university (Kabay, 2008). In the mid-1960s, the United States started a debate on the creation of a central data-storage authority for all ministries (Ruggles/Miller/Kuh/Lebergott/Orcutt/Pechman, 1965). Within this context, possible criminal abuse of databases and the related risks to privacy were discussed.

2.3.2 The 1970s

In the 1970s, the use of computer systems and computer data increased further (Quinn, 1978). At the end of the decade, an estimated number of 100 000 mainframe computers were operating in the United States. With falling prices, computer technology was more widely used within administration and business, and by the public. The 1970s were characterized by a shift from the traditional property crimes against computer systems that had dominated the 1960s, to new forms of crime (McLaughlin, 1978). While physical damage continued to be a relevant form of criminal abuse against computer systems, new forms of computer crime were recognized. They included the illegal use of computer systems and the manipulation of electronic data. The shift from manual to computer-operated transactions led to another new form of crime – computer-related fraud((McLaughlin, 1978). Already at this time, multimillion dollar losses were caused by computer-related fraud. Computer-related fraud, in particular, was a real challenge, and law enforcement agencies were investigating more and more cases. As the application of existing legislation in computer-crime cases led to difficulties, a debate about legal solutions started in different parts of the world. The United States discussed a draft bill designed specifically to address cybercrime (Federal Computer Systems Protection Act of 1977). Interpol discussed the phenomena and possibilities for legal response (Third Interpol Symposium on International Fraud, France 1979).

2.3.3 The 1980s

In the 1980s, personal computers became more and more popular. With this development, the number of computer systems and hence the number of potential targets for criminals again increased. For the first time, the targets included a broad range of critical infrastructure. One of the side effects of the spread of computer systems was an increasing interest in software, resulting in the emergence of the first forms of software piracy and crimes related to patents. The interconnection of computer systems brought about new types of offence. Networks enabled offenders to enter a computer system without being present at the crime scene. In addition, the possibility of distributing software through networks enabled offenders to spread malicious software, and more and more computer viruses were discovered. Countries started the process of updating their legislation so as to meet the requirements of a changing criminal environment. International organizations also got involved in the process. OECD and the Council of Europe set up study groups to analyse the phenomena and evaluate possibilities for legal response.

2.3.4 The 1990s

The introduction of the graphical interface (“WWW”) in the 1990s that was followed by a rapid growth in the number of Internet users led to new challenges. Information legally made available in one country was available globally – even in countries where the publication of such information was criminalized (Sofaer/Goodman, 2001). Another concern associated with online services that turned out to be especially challenging in the investigation of transnational crime was the speed of information exchange. Finally, the distribution of child pornography moved from physical exchange of books and tapes to online distribution through websites and Internet services (CSEC, 2001). While computer crimes were in general local crimes, the Internet turned electronic crimes into transnational crime. As a result, the international community tackled the issue more intensively. UN General Assembly Resolution 45/121 adopted in 1990145 and the manual for the prevention and control of computer-related crimes issued in 1994 are just two examples (UN manual on Prevention and control of computer-related crime).

2.3.5 The 21st Century

As in each preceding decade, new trends in computer crime and cybercrime continued to be discovered in the 21st century. The first decade of the new millennium was dominated by new, highly sophisticated methods of committing crimes, such as “phishing”, and “botnet attacks”, (Wilson, 2007) and the emerging use of technology that is more difficult for law enforcement to handle and investigate, such as “voice-over-IP (VoIP) communication” (Simon/Slay, 2006) and “cloud computing” (Velasco San Martin, 2009). It is not only the methods that changed, but also the impact. As offenders became able to automate attacks, the number of offences increased. Countries and regional and international organizations have responded to the growing challenges and given response to cybercrime high priority.

2.4 TYPOLOGY/FORMS OF CYBER CRIME

This section describe various forms which cyber-crime takes ranging from activities that result in degradation of data or data loss to activities that leads to lack of data confidentiality and even fraud.

2.4.1 Illegal access (hacking, cracking)

The offence described as “hacking” refers to unlawful access to a computer system191, one of oldest computer-related crimes.

In the early years of IT development, the term “hacking” was used to describe the attempt to get more out of a system (software or hardware) than it was designed for. Within this context, the term “hacking” was often used to describe a constructive activity.

Following the development of computer networks (especially the Internet), this crime has become a mass phenomenon. Famous targets of hacking attacks include the US National

Aeronautics and Space Administration (NASA), the US Air Force, the Pentagon, Yahoo, Google, eBay and the German Government. Examples of hacking offences include breaking the password of password-protected websites and circumventing password protection on a computer system. But acts related to the term "hacking" also include preparatory acts such as the use of faulty hardware or software implementation to illegally obtain a password to enter a computer system, setting up "spoofing" websites to make users disclose their passwords and installing hardware and software-based keylogging methods (e.g. "keyloggers") that record every keystroke – and consequently any passwords used on the computer and/or device.198 The motivation of offenders varies. Some offenders limit their activities to circumventing security measures only in order to prove their abilities (Sieber, 2004). Others act through political motivation (known as "hacktivism"200) – one example is a recent incident involving the main United Nations website. In most cases, though, the motivation of the offender is not limited to illicit access to a computer system. Offenders use this access to commit further crimes, such as data espionage, data manipulation or denial-of-service (DoS) attacks. In most cases, illegal access to the computer system is only a vital first step. Many analysts recognize a rising number of attempts to illegally access computer systems, with over 250 million incidents recorded worldwide during the month of August 2007 alone (The Online-Community HackerWatch, 2007). Three main factors have supported the increasing number of hacking attacks: inadequate and incomplete protection of computer systems, development of software tools that automate the attacks, and the growing role of private computers as a target of hacking attacks.

Inadequate and incomplete protection of computer systems

Hundreds of millions of computers are connected to the Internet, and many computer systems are without adequate protection in place to prevent illegal access (Wilson, 2007). Analysis carried out by the University of Maryland suggests that an unprotected computer system that is connected to the Internet is likely to experience attack within less than a minute (Professor Cukier, 2007). The installation of protective measures can lower the risk, but successful attacks against well-protected computer systems prove that technical protection measures can never completely stop attacks (Joyner/Lotrionte, 2002).

Development of software tools that automate the attacks

Recently, software tools are being used to automate attacks. With the help of software and preinstalled attacks, a single offender can attack thousands of computer systems in a single day using one computer. If the offender has access to more computers – e.g. through a botnet– he/she can increase the scale still further. Botnets is a short term for a group of compromised computers running programs that are under external control. Since most of these software tools use preset methods of attacks, not all attacks prove successful. Users that update their operating systems and software applications on a regular basis reduce their risk of falling victim to these broad-based attacks, as the companies developing protection software analyse attack tools and prepare for the standardized hacking attacks. High-profile attacks are often based on individually-designed attacks. The success of those attacks is often not the result of highly sophisticated methods, but the number of attacked computer systems. Tools enabling these standardized attacks are widely available over the Internet (Websense Security, 2004) – some for free, but efficient tools can easily cost several thousand US dollars. One example is a hacking tool that allows the offender to define a range of IP-addresses (e.g. from 111.2.0.0 to 111.9.253.253). The software allows for the scanning for unprotected ports of all computers using one of the defined IP-addresses.

The growing role of private computers as a target of hacking attacks

Access to a computer system is often not the primary motivation of an attack (Walden, 2006). Since business computers are generally better protected than private computers, attacks on business computers are more difficult to carry out using pre-configured software tools (Erickson, 2003). Over the past few years, offenders have focused their attacks increasingly on private computers, since many private computers are inadequately protected. Further, private computers often contain sensitive information (e.g. credit card and bank account details). Offenders are also targeting private computers because, after a successful attack, offenders can include the computer in their botnet and use the computer for further criminal activities. Illegal access to a computer system may be viewed as analogous to illegal access to a building and is recognized as a criminal offence in many countries. Analysis of different approaches to the criminalization of computer access shows that enacted provisions in some cases confuse illegal access with subsequent offences or attempt to limit criminalization of illegal access to grave violations only. Some provisions criminalize the initial access, while other approaches limit the criminal offence only to those cases where the accessed system is protected by security measures or the perpetrator has harmful intentions or data was obtained, modified or damaged. Other legal systems do not criminalize mere access, but focus on subsequent offences.

2.4.2 Illegal data acquisition (data espionage)

Sensitive information is often stored in computer systems. If the computer system is connected to the Internet, offenders can try to access this information via the Internet from almost any place in the world. The Internet is increasingly used to obtain trade secrets (Sieber, 2004). The value of sensitive information and the ability to access it remotely makes data espionage highly interesting. In the 1980s, a number of German hackers succeeded in entering US government and military computer systems, obtaining secret information and selling this information to agents from a different country. Offenders use various techniques to access victims' computers, including software to scan for unprotected ports or circumvent protection measures, as well as "social engineering" (Granger, 2007). The last approach especially, which refers to a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people into breaking normal security procedures, is interesting as it not based on technical means (Global Strategic Report, 2008). In the context of illegal access it describes the manipulation of human beings with the intention of gaining access to computer systems. Social engineering is usually very successful, because the weakest link in computer security is often the users operating the computer system. One example is "phishing", which has recently become a key crime committed in cyberspace and describes attempts to fraudulently acquire sensitive information (such as passwords) by masquerading as a trustworthy person or business (e.g. financial institution) in a seemingly official electronic communication. Although the human vulnerability of users opens the door to the risk of scams, it also offers solutions. Well-educated computer users are not easy victims for offenders using social engineering. As a consequence, user education should be an essential part of any anti-cybercrime strategy. In addition, technical measures can be taken to prevent illegal access. OECD highlights the importance of cryptography for users, as cryptography can help improve data protection. If the person or organization storing information uses proper protection measures, cryptographic protection can be more efficient than any physical protection. The success of offenders in obtaining sensitive information is often due to the absence of protection measures. Since important information is increasingly being stored in computer systems, it is essential to evaluate whether the technical protection measures taken by the users are adequate, or if law-makers need to establish additional protection by criminalizing data espionage. Although offenders usually target business secrets, data stored on private computers are also increasingly targeted. Private users often store bank-account and credit-card information on their computer. Offenders can use this information for their own purposes (e.g. bank-account details to make money transfers) or sell it to a third party (Chawki/Abdel Wahab, 2006). Credit-card records are for example sold for up to USD 60 (2005 Identity Theft). Hackers' focus on private computers is interesting, as the profits from business secrets are generally higher than the profits to be made from obtaining or selling single credit-card information. However, since private computers are generally less well protected, data espionage based on private computers is likely to become even more profitable.

There are two approaches to obtaining information. Offenders can access a computer system or data storage device and extract information; or try to manipulate the user to make them disclose the information or access codes that enable offenders to access information ("phishing"). Offenders often use computer tools installed on victims' computers or malicious software called spyware to transmit data to them (Hackworth, 2006). Various types of spyware have been discovered over recent years, such as keyloggers (Hackworth, 2006). Keyloggers are software tools that record every keystroke typed on an infected computer's keyboard. Some keyloggers send all recorded information to the offender, as soon as the computer is connected to the Internet. Others perform an initial sort and analysis of the data recorded (e.g. focusing on potential credit-card information) to transmit only major data discovered. Similar devices are also available as hardware devices that are plugged in between the keyboard and the computer system to record keystrokes on the keyboard. Hardware-based keyloggers are more difficult to install and detect, as they require physical access to the computer system. However, classical anti-spyware and anti-virus software is largely unable to identify them. Apart from accessing computer systems, offenders can also obtain data by manipulating the user.

Recently, offenders have developed effective scams to obtain secret information (e.g. bank-account information and credit-card data) by manipulating users using social engineering techniques. "Phishing" has recently become one of the most important crimes related to cyberspace. The term "phishing" is used to describe a type of crime that is characterized by attempts to fraudulently acquire sensitive information, such as passwords, by masquerading as a trustworthy person or business (e.g. financial institution) in an apparently official electronic communication (Prof. Dr. Marco Gercke, 2012)

2.4.3 Illegal interception

Offenders can intercept communications between users (such as e-mails) or other forms of data transfers (when users upload data onto webservers or access web-based external storage media) in order to record the information exchanged. In this context, offenders can in general target any communication infrastructure (e.g. fixed lines or wireless) and any Internet service (e.g. e-mail, chat or VoIP communications).

Most data-transfer processes among Internet infrastructure providers or Internet service providers are well protected and difficult to intercept. However, offenders search for weak points in the system. Wireless technologies are enjoying greater popularity and have in the past proved vulnerable (Kang, 2006). Nowadays, hotels, restaurants and bars offer customers Internet access through wireless access points. However, the signals in the data exchanges between the computer and the access point can be received within a radius of up to 100 metres. Offenders who wish to intercept a data-exchange process can do so from any location within this radius. Even where wireless communications are encrypted, offenders may be able to decrypt the recorded data.

To gain access to sensitive information, some offenders set up access points close to locations where there is a high demand for wireless access (e.g. near bars and hotels) (Kang, 2006). The station location is often named in such a way that users searching for an Internet access point are more likely to choose the fraudulent access point. If users rely on the access provider to ensure the security of their communication without implementing their own security measures, offenders can easily intercept communications. The use of fixed lines does not prevent offenders from intercepting communications. Data transmissions passing along a wire emit electromagnetic energy. If offenders use the right equipment, they can detect and record these emissions and may be able to record data transfers between users' computers and the connected system, and also within the computer system. Most countries have moved to protect the use of telecommunication services by criminalizing the illegal interception of phone conversations. However, given the growing popularity of IP-based services, lawmakers may need to evaluate to what extent similar protection is offered to IP-based services.

2.4.4 Data interference

Computer data are vital for private users, businesses and administrations, all of which depend on the integrity and availability of data. Lack of access to data can result in considerable (financial) damage. Offenders can violate the integrity of data and interfere with them by deleting, suppressing or altering computer data (Sieber, 2004). One common example of the deletion of data is the computer virus. Ever since computer technology was first developed, computer viruses have threatened users who failed to install proper protection (Kabay, 2008). Since then, the number of computer viruses has risen significantly. Not only has the number of virus attacks increased, but also the techniques and functions of viruses (payload) have changed.

Previously, computer viruses were distributed through storage devices such as floppy disks, whilst today most viruses are distributed via the Internet as attachments either to e-mails or to files that users download. These efficient new methods of distribution have massively accelerated virus infection and vastly increased the number of infected computer systems. The computer worm SQL Slammer was estimated to have infected 90 per cent of vulnerable computer systems within the first 10 minutes of its distribution (BBC News, 2003). The financial damage caused by virus attacks in 2000 alone was estimated to amount to some USD 17 billion.270 In 2003, it was still more than USD 12 billion. Most first-generation computer viruses either deleted information or displayed messages. Recently, payloads have diversified (Szor, 2005). Modern viruses are able to install back-doors enabling offenders to take remote control of the victim's computer or encrypt files so that victims are denied access to their own files, until they pay money to receive the key (Bates, 1990).

2.4.5 System interference

The same concerns over attacks against computer data apply to attacks against computer systems. More businesses are incorporating Internet services into their production processes, with benefits of 24-hour availability and worldwide accessibility. If offenders succeed in preventing computer systems from operating smoothly, this can result in great financial losses for victims. Attacks can be carried out by physical attacks on the computer system (Sieber, 2004). If offenders are able to access the computer system, they can destroy hardware. For most criminal legal systems, remote physical cases do not pose major problems, as they are similar to classic cases of damage or destruction of property. However, for highly profitable e-commerce businesses, the financial damages caused by attacks on the computer system are often far greater than the mere cost of computer hardware. More challenging for legal systems are web-based scams. Examples of these remote attacks against computer systems include computer worms and denial-of-service (DoS) attacks (Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni, 2001) A denial-of-service (DoS) attack aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. Computer worms are a subgroup of malware (like computer viruses). They are self-replicating computer programs that harm the network by initiating multiple data-transfer processes. They can influence computer systems by hindering the smooth running of the computer system, using system resources to replicate themselves over the Internet or generating network traffic that can close down availability of certain services (such as websites). While computer worms generally influence the whole network without targeting specific computer systems, DoS attacks target specific computer systems. A DoS attack makes computer resources unavailable to their intended users. By targeting a computer system with more requests than the computer system can handle, offenders can prevent users from accessing the computer system, checking e-mails, reading the news, booking a flight or downloading files. In 2000, within a short time, several DoS attacks were launched against well-known companies such as CNN, eBay and Amazon (Sofaer/Goodman, 2001). Similar attacks were reported in 2009 on government and commercial websites in the US and South Korea. As a result, some of the services were not available for several hours and even days. The prosecution of DoS and computer-worm attacks poses serious challenges to most criminal law systems, as these attacks may not involve any physical impact on computer systems. Apart from the basic need to criminalize web-based attacks, the question of whether the prevention and prosecution of attacks against critical infrastructure needs a separate legislative approach is under discussion.

2.4.6 *Erotic or pornographic material (excluding child pornography)*

Sexually-related content was among the first content to be commercially distributed over the Internet, which offers advantages to retailers of erotic and pornographic material including:

- exchange of media (such as pictures, movies, live coverage) without the need for cost-intensive shipping;
- worldwide access, reaching a significantly larger number of customers than retail shops;
- the Internet is often viewed as an anonymous medium (often erroneously) – an aspect that consumers of pornography appreciate, in view of prevailing social opinions.

Recent research has identified as many as 4.2 million pornographic websites that may be available on the Internet at any time (Ropelato). Besides websites, pornographic material can be distributed through file-sharing systems and instant messaging systems (Ropelato). Different countries criminalize erotic and pornographic material to different extents. Some countries permit the exchange of pornographic material among adults and limit criminalization to cases where minors access this kind of material, seeking to protect minors. Studies indicate that child access to pornographic material could negatively influence their development (Nowara/Pierschke, 2008). To comply with these laws, “adult verification systems” have been developed. Other countries criminalize any exchange of pornographic material even among adults, without focusing on specific groups (such as minors). For countries that criminalize interaction with pornographic material, preventing access to pornographic material is a challenge. Beyond the

Internet, authorities can in many instances detect and prosecute violations of the prohibition of pornographic material. On the Internet, however, as pornographic material is often readily available on servers outside the country, enforcement is difficult. Even where authorities are able to identify websites containing pornographic material, they may have no powers to enforce removal of offensive content by providers. The principle of *national sovereignty* does not generally permit a country to carry out investigations within the territory of another country, without permission from local authorities (Roth, 2005). Even when authorities seek the support of countries where offensive websites are hosted, successful investigation and criminal sanctions may be hindered by the principle of "dual criminality". To prevent access to pornographic content, countries with exceptionally strict laws are often limited to prevention (such as filter technology) to limit access to certain websites (Weekes, 2003)

2.4.7 Child pornography

The Internet has become a prime channel for the distribution of child pornography. In the 1970s and 1980s, offenders engaging in the exchange of child pornography faced serious threats (Lanning, 2001). At that time, the commercial child pornography market focused mainly on Europe and the US and the material was locally produced, expensive and difficult to obtain (Wortley/Smallbone, 2006). Approaches to buy or sell child pornography entailed a number of risks that no longer – or at least not to a degree – exist today. In the past, producers did not have the capability to develop photography and films. They were dependent on services offered by businesses, which increased the chances of law-enforcement agents identifying child pornography through reports from businesses handling the development. The availability of video cameras changed this situation for the first time (Lanning, 2001). But the risks were not only related to production. Getting access to child pornography was similarly fraught with risks for the offender. Orders were placed by responding to advertisements in newspapers. Means of communication between seller and collector, and hence the market itself, were limited. Until the mid-1990s, child pornography was primarily transported through postal services, and successful investigations led to the detection of a significant number of offenders (US House of Representatives, 109th Congress, 2007). In the view of experts, law enforcement was at that time able to meet the challenges. The situation changes dramatically with the availability of Internet-based data-exchange applications. While in the past, law enforcement was confronted with analogue material, today the vast majority of discovered material is digital. Since the mid-1990s, offenders have increasingly used network services for the distribution of such material. The resulting problems in terms of detecting and investigating child-pornography cases have been acknowledged. The Internet is today the main channel for trading regular pornography as well as child pornography (Bloxsome/Kuhn/Pope/Voges, 2007) Several reasons for the shift from analogue to digital distribution can be identified. The Internet gives less technically skilled users the impression they can act invisibly from others. If the offender does not employ anonymous communication technology, this impression is erroneous. But the fact that using sophisticated means of anonymous communication can hinder the identification of the offender is a matter of concern in respect of the exchange of child pornography online. In addition, this development has been supported by the decreasing price of technical devices and services used for the production and trading of child pornography, such as recording equipment and hosting services. Since websites and Internet services are open to around two billion Internet users, the number of potential customers has also expanded (ITU, 2010). There are concerns that the fact that access is easier attracts people who would not have taken the risk of being caught trying to obtain child pornography outside the Internet. With the shift from analogue to digital media, an increasing number of child-pornography images discovered through investigations were reported (Carr, 2004). Another aspect that probably supported this development is the fact that digital information can in general be duplicated without a loss of quality. While in the past consumers of child pornography wishing to duplicate and trade the material were hindered by the loss in quality from reproduction, today a downloaded file can become the source for further duplications. One of the consequences of this development is that, even when the offender who produced the material in the first place is arrested and his files are confiscated, it becomes difficult to "remove" files once they have been traded over the Internet (US House of Representatives, 109th Congress, 2007).

2.4.8 Religious offences

A growing number of websites present material that is in some countries covered by provisions related to religious offences, e.g. anti-religious written statements (Walden, 2006). Although some material documents objective facts and trends (e.g. decreasing church attendance in Europe), this information may be considered illegal in some jurisdictions. Other examples include the defamation of religions or the publication of cartoons.

The Internet offers advantages for those who wish to debate or deal critically with a subject – people can leave comments, post material or write articles without having to disclose their identity. Many discussion groups are based on the principle of freedom of speech

(Tedford/Herbeck/Haiman, 2005). Freedom of speech is a key driver behind the Internet's success, with portals that are used specifically for user-generated content. Whilst it is vital to protect this principle, even in the most liberal countries the application of principles of freedom of speech is governed by conditions and laws.

The differing legal standards on illegal content reflect the challenges of regulating content. Even where the publication of content is covered by provisions relating to freedom of speech in the country where the content is available, this material can be accessed from countries with stricter regulations. The "cartoon dispute" in 2005 demonstrated the potential for conflict. The publication of twelve editorial cartoons in the Danish newspaper Jyllands-Posten led to widespread protests across the Muslim world (Times Online, 2005). As with illegal content, the availability of certain information or material is a criminal offence in some countries. The protection of different religions and religious symbols differs from country to country. Some countries criminalize the use of derogatory remarks in respect of the Holy Prophets or the defiling of copies of the Holy Quran, while other countries may adopt a more liberal approach and may not criminalize such acts.

2.4.9 Illegal gambling and online games

Internet games and gambling are one of the fastest-growing areas in the Internet (Rown/Raysman, 2006). Linden Labs, the developer of the online game Second Life, reports that some ten million accounts have been registered. Reports show that some such games have been used to commit crimes, including the exchange and presentation of child pornography, fraud, gambling in virtual online casinos and libel (e.g. leaving slanderous or libellous messages) (Christiansen). Some estimates project growth in estimated online gambling revenues from USD 3.1 billion in 2001 to USD 24 billion in 2010 for Internet gambling (although compared with revenues from traditional gambling, these estimates are still relatively small). The regulation of gambling over and outside the Internet varies between countries – a loophole that has been exploited by offenders, as well as legal businesses and casinos. The effect of different regulations is evident in Macau. After being returned by Portugal to China in 1999, Macau has become one of the world's biggest gambling destinations. With estimated annual revenues of USD 6.8 billion in 2006, it took the lead from Las Vegas (USD 6.6 billion) (BBC News). Macau's success derives from the fact that gambling is illegal in China and thousands of gamblers travel from Mainland China to Macau to play. The Internet allows people to circumvent gambling restrictions. Online casinos are widely available, most of them hosted in countries with liberal laws or no regulations on Internet gambling. Users can open accounts online, transfer money and play games of chance. Online casinos can also be used in money laundering and activities financing terrorism. If offenders use online casinos within the laying phase that do not keep records or are located in countries without money-laundering legislation, it is difficult for law enforcement agencies to determine the origin of funds.

It is difficult for countries with gambling restrictions to control the use or activities of online casinos. The Internet is undermining some countries' legal restrictions on access by citizens to online gambling. There have been several legislative attempts to prevent participation in online gambling: notably, the US Internet Gambling Prohibition Enforcement Act of 2006 seeks to limit illegal online gambling by prosecuting financial services providers if they carry out settlement of transactions associated with illegal gambling.

2.4.10 Libel and false information

The Internet can be used to spread misinformation, just as easily as information. Websites can present false or defamatory information, especially in forums and chat rooms, where users can post messages without verification by moderators. Minors are increasingly using web forums and social networking sites where such information can be posted as well. Criminal behaviour can include (for example) the publication of intimate photographs or false information about sexual behaviours (Sieber, 2005). In most cases, offenders take advantage of the fact that providers offering cheap or free publication do not usually require identification of authors or may not verify ID. This makes the identification of offenders complicated. Furthermore, there may be no or little regulation of content by forum moderators. These advantages have not prevented the development of valuable projects such as the online user-generated encyclopaedia, Wikipedia, where strict procedures exist for the regulation of content. However, the same technology can also be used by offenders to publish false information (e.g. about competitors) or disclose secret information (e.g. the publication of state secrets or sensitive business information).

It is vital to highlight the increased danger presented by false or misleading information. Defamation can seriously injure the reputation and dignity of victims to a considerable degree, as online statements are accessible to a worldwide audience. The moment information is published over the Internet, the author often loses control of this information. Even if the information is corrected or deleted shortly after publication, it may already have been duplicated ("mirroring") and made available by people that are unwilling to rescind or remove it. In this case, information may still be available on the Internet, even if it has been removed or corrected by the original source. Examples include cases of "runaway e-mails", where millions of people can receive salacious, misleading or false e-mails about people or organizations, where the damage to reputations may never be restored, regardless of the truth or otherwise of the original e-mail. Therefore the freedom of speech (Tedford/Herbeck/Haiman, 2005) and protection of the potential victims of libel needs to be well balanced.

2.4.11 Spam and related threats

"Spam" describes the emission of unsolicited bulk messages (ITU, 2005). Although various scams exist, the most common one is e-mail spam. Offenders send out millions of e-mails to users, often containing advertisements for products and services, but frequently also malicious software. Since the first spam e-mail was sent in 1978, (Tempelton, 1978) the tide of spam e-mails has increased dramatically (Sunner, 2007). Today, e-mail provider organizations report that as many as 85 to 90 per cent of all e-mails are spam (Postini, 2007). The main sources of spam e-mails in 2007 were: the United States (19.6 per cent of the recorded total); People's Republic of China (8.4 per cent); and the Republic of Korea (6.5 per cent) (Postini, 2007). Most e-mail providers have reacted to rising levels of spam e-mails by installing anti-spam filter technology. This technology identifies spam using keyword filters or blacklists of spammers' IP addresses. Although filter technology continues to develop, spammers find ways around these systems – for example, by avoiding keywords. Spammers have found many ways to describe "Viagra", one of the most popular products offered in spam, without using the brand name. (Lui/Stamm, 2007). Success in the detection of spam e-mails depends on changes in the way spam is distributed. Instead of sending messages from a single mail server (which is technically easier for e-mail providers to identify, due to the limited number of sources), many offenders use botnet to distribute unsolicited e-mails. By using botnets based on thousands of computer systems, each computer might send out only a few hundred e-mails. This makes it more difficult for e-mail providers to identify spam by analysing the information about senders and more difficult for law-enforcement agencies to track offenders. Spam e-mails are highly profitable as the cost of sending out billions of e-mails is low – and even lower where botnets are involved. Some experts suggest the only real solution in the fight against spam is to raise transmission costs for senders. A report published in 2007 analysed the costs and profits of spam e-mails. Based on the results of the analysis, the cost of sending out 20 million e-mails is around USD 500 (Heise News, 2007). Since costs for offenders are low, sending spam is highly profitable, especially if offenders are able to send billions of e-mails. A Dutch spammer reported a profit of around USD 50 000 by sending out at least 9 billion spam e-mails (Thorhallsson).

In 2005, the OECD published a report analysing the impact of spam on developing countries. Developing countries often express the view that Internet users in their countries suffer more from the impact of spam and Internet abuse. Spam is a serious issue in developing countries, where bandwidth and Internet access are scarcer and more expensive than in industrialized countries. Spam consumes valuable time and resources in countries where Internet resources are rarer and more costly.

2.4.12 Other forms of illegal content

The Internet is not only used for direct attacks, but also as a forum for soliciting, offers and incitement to commit crimes unlawful sale of products and providing information and instructions for illegal acts (e.g. how to build explosives) (Sieber, 2004).

Many countries have put in place regulations on the trade of certain products. Different countries apply different national regulations and trade restrictions to various products such as military equipment. A similar situation exists for medicines – medicines which are available without restriction in some countries may need prescription in others (Council of Europe, 2007). Cross-border trade may make it difficult to ensure that access to certain products is restricted within a territory. Given the popularity of the Internet, this problem has grown. Web shops operating in countries with no restrictions can sell products to customers in other countries with restrictions, undermining these limitations. Prior to the Internet, it was difficult for most people to access instructions on how to build weapons. The necessary information was available (e.g. in books dealing with chemical aspects of explosives), but time consuming to find. Today, information on how to build explosives is available over the Internet and ease of access to information increases the likelihood of attacks (Conway, 2006).

2.5 THE INTERNET IN NIGERIA AND CYBER CRIME

Despite the need for internet, the emergence of internet in Nigeria birthed the major heart-break of Cyber-crime. According to Dr. Ibikunle Frank, Department of Electrical & Information Engineering, Covenant University, Nigeria (2013), Cyber-crime refers to a series of organized crime attacking the internet (Cyber-space) and its security. Cyberspace is a world that contains just about anything one is searching for. With the advent of these advancements in information accessibility and the advantages and applications of the internet comes an exponentially growing disadvantage- Cyber Crime. Cyber security has risen to become a national concern as threats concerning it now need to be taken more seriously.

Computer crime can broadly be defined as criminal activity involving an information technology infrastructure: including illegal access or unauthorized access; illegal interception that involves technical means of non-public transmissions of computer data to, from or within a computer system; data interference that include unauthorized damaging, deletion, deterioration, alteration or suppression of computer data; systems interference that is interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data; misuse of devices, forgery (ID theft), and electronic fraud (Paul Taylor 1999).The advent of digital technology gave birth to modern communication hard-wares, internet service and powerful computer systems to process data (Ramjit Singh Hunda, Kawajeet Singh and M. D. Singh. 2004). Hence, cyberspace has provided a safe haven for internet platform, which has created geometric growth and accelerated windows of opportunities for businesses and the removal of economic barriers hitherto faced by nations of the world. People from diverse areas of human endeavour can now freely access and utilize the advantages offered by internet platform. However, information technology revolution associated with the internet in Nigeria has brought about a new wave of crime. A very few criminally minded youth in the country, who are mostly not educated or **graduates**, are stealing and committing atrocity through the aid of the internet online business transactions. The internet online business services, which ordinarily supposed to be a blessing as it exposes one to a lot of opportunities in various field of life is fast becoming a source of discomfort and worry due to the atrocity being perpetrated through it. Cybercrime has come as a surprise and a strange phenomenon that for now live with us in Nigeria. Computer crimes encompass a broad range of potentially illegal activities. Generally it may be categorize into two major groups: (Paul Taylor 1999) crimes that target computer networks or devices directly; (Ramjit Singh Hunda, Kawajeet Singh and M. D. Singh. 2004) crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device. Nigeria was recently identified as the innocent and ignorant passive player in cyberspace knowledge Olympiad (The Guardian Wednesday, July 9, 2008). The capture of Al Qaeda's operative, Muhammad Naeem Noor Khan, provided the Pakistani and American Intelligence Authority with some of Al Qaeda's Internet Communication Strategy. It also identified that Nigerian Websites and Email System were used by Al Qaeda to disseminate internet information. This has once again brought up the pertinent questions of the safety and security of Nigeria's national cyberspace. This project therefore addresses, from our investigation the aspect that deals with cybercrime based on false pretence or impersonation. An area that is likely to be fertile to the cyber criminals also is the stock exchange market. Proper mechanism needs to be put in place to control the activities of these criminals in this area otherwise Nigeria economy may be brought down, particularly with trading on the country's stock exchange market going online. Without proper security methods in place, it is just like building a house without locks. Any person can gain access. The category and nature of cybercrime in Nigeria is endless. Cybercrime is a global phenomenal that is threatening the economy of nations. It is a major threat in India as it is in Nigeria. Punjab National Bank suffered a loss of close to Rs. 1. 39 chore when the recorders were manipulated to create false debits and credits. In bank of Baroda, Rs 2.5 lakh was misappropriated through the computerized creation of false bank accounts (Krishna Kumar. 2003). In Mahanager Telephone Nigam Limited (MTNL) in Delhi, a junior telecom official was charged for reversing electronic telephone meter system thereby allowing some commercials export houses to make overseas calls without the charges being directed to their telephone numbers.

It has been established that Nigeria is an impressionable country. The advent of the internet to her was both welcome and full of disadvantages. The exceptional outbreak of cyber-crime in Nigeria in recent times was quite alarming, and the negative impact on the socio-economy of the country is highly disturbing. Over the past twenty years, immoral cyberspace users have continued to use the internet to commit crimes; this has evoked mixed feelings of admiration and fear in the general populace along with a growing unease about the state of cyber and personal security. This phenomenon has seen sophisticated and extraordinary increase recently and has called for quick response in providing laws that would protect the cyber space and its users (Dr. Ibikunle Frank, 2013).

The first recorded cyber murder was committed in the United States seven years ago. According to the Indian Express, January 2002, an underworld don in a hospital was to undergo a minor surgery. His rival went ahead to hire a computer expert who altered his prescriptions through hacking the hospital's computer system. He was administered the altered prescription by an innocent nurse, this resulted in the death of the patient (Mohsin, A., 2006: *Cyber Crimes And Solutions)*. Statistically, all over the world, there has been a form of cyber-crime committed every day since 2006 (Schaeffer, B. S., et al. 2009)

Technology has integrated nations and the world has become a global village. The economy of most nations in the world is accessible through the aid of electronic via the internet. Since the Electronic market is opened to everybody it also includes eavesdroppers and criminals. False pretence, finds a fertile ground in this situation. Some perpetrators of this crime usually referred to in Nigeria as “yahoo boys” are taking advantage of e-commerce system available on the internet to defraud unsuspected victims who are mostly foreigners thousands and sometimes millions of dollars. They fraudulently represent themselves as having particular goods to sell or that they are involved in a loan scheme project. They may even pose to have financial institution where money can be loaned out to prospective investors. In this regard, so many persons have become a duped. Merchants who take orders from merchandise on credit are also facing mounting losses from rip offs. Investigations revealed that “yahoo boys” also take undue advantage of some people that are looking for spouse through the aid of Internet. These criminally minded individuals usually have discussion with their victims via the internet. These criminals pretend to be interested and loving. And before the victim realizes what is happening,

the criminals would have succeeded in cajoling them to send some dollars to enable them facilitate traveling documents. These criminals falsify document and tell all sort of lies to get money from their victims, when their victims begin to suspect foul play, they will immediately stop interacting with them and shift their target elsewhere. 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. Specific computer crimes are Spam, Fraud, Obscene or offensive content, Harassment, Drug trafficking, and Cyber terrorism (Okonigene Robert Ehimen, Adekanle Bola, 2009).

2.6. E-CRIMES THAT ARE PECULIAR TO NIGERIA

There is no doubt that e-crime is an image trauma for Nigeria. Cyber-crime is a source of concern and embarrassment for the nation. The Internet creates unlimited opportunities for commercial, social, and educational activities. But as we can see with cyber-crime the Internet also introduces its own peculiar risks. The instances reported here ranges from fake lotteries to the biggest internet scams. Elekwe, a chubby-faced 28-year-old man made a fortune through the scam after two years of joblessness despite having diploma in computer science. He was lured to Lagos from Umuahia by the chief of a fraud gang in a business center. He has three sleek cars and two houses from his exploits. In July 2001, four Nigerians suspected to be operating a “419” scam on the internet to dupe unsuspecting foreign investors in Ghana were arrested by security agencies. Their activities are believed to have led to the loss of several millions of foreign currencies by prospective investors. Two young men were recently arrested after making an online purchase of two laptops advertised by a woman on her website under false claims. They were arrested at the point of delivery by government officials. Mike Amadi was sentenced to 16 years imprisonment for setting up a website that offered juicy but phony procurement contracts. The man impersonated the EFCC Chairman, but he was caught by an undercover agent posing as an Italian businessman. The biggest international scam of all was committed by Amaka Anajemba who was sentenced to 2½ years in prison. She was equally ordered to return $25.5 million of the $242 million she helped to steal from a Brazilian bank.

On recent internet scam case was reported on the Sunday PUNCH newspaper of July 16, 2006 involving a 24-year-old Yekini Labaika of Osun State origin in Nigeria and a 42-years-old nurse of American origin, by name Thumbelina Hinshaw, in search of a Muslim lover to marry. The young man deceived the victim by claiming to be an American Muslim by the name, Phillip Williams, working with an oil company in Nigeria and he promised to marry her. He devised dubious means to swindle $16,200 and lots of valuable materials from the victim. The scammer later was sentenced to a total of 19½ years having been found guilty of eight-counts against him. Incidences like these are on the increase. Several young men unabated are still carrying out these illegal acts successfully, ripping off credulous individuals and organizations (Longe, O. B, Chiemeke, S., 2008). Recently, a report indicated that Nigeria is losing about $80 million yearly to software piracy. The report was the finding of a study conducted by Institute of Digital Communication, a market research and forecasting firm, based in South Africa, on behalf of Business Software Alliance of South Africa. The American National Fraud Information Centre reported Nigerian money offers as the fastest growing online scam, up to 90% in 2001. The Centre also ranked Nigerian cyber-crime impact per capita as being exceptionally high (The Economic Times, 2004) Those involved are between 18-25 years mostly resident in the urban centers. The internet has help in modernizing fraudulent practices among the youths. Online fraud is seen as the popularly accepted means of economic sustenance by the youths involved. The corruption of the political leadership has enhanced the growth of internet crime subculture. The value placed on wealth accumulation has been a major factor in the involvement of youths in online fraud. (Adebusuyi, A., 2008)

2.7 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 (Thompson, D., 1989)

2.8 CYBER SECURITY

Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. Cyber-security is the body of rules put in place for the protection of the cyber space. But as we become more dependent on cyberspace, we undoubtedly face new risks.

2.9 GOALS OF CYBER SECURITY

The following are the objectives of Cyber-security.

- To help people reduce the vulnerability of their Information and Communication Technology (ICT) systems and networks.
- To help individuals and institutions develop and nurture a culture of cyber security.
- To work collaboratively with public, private and international entities to secure cyberspace.
- To help understand the current trends in IT/cybercrime, and develop effective solutions.
- Availability.
- Integrity, which may include authenticity and non-repudiation.
- Confidentiality.

2.10 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

2.11 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.

2.12 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. 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.

CHAPTER THREE

3.0 RESEARCH METHODOLOGY

The statistical tool used for the analyses of the statement of hypothesis was frequency table analysis. It was used to test the dependable and independable variables.

3.1 METHOD OF DATA COLLECTION

Data for this research work were provided from both primary and secondary sources. Information were gathered using research questionnaire to get facts, views and feelings of respondents as it relates to their appraisal and a number of related issues, which was primary data collected from respondents from the sample selected from the study. Secondary data was collected from journals, textbooks, magazines, articles and handbooks relevant to the subject of discussion.

3.2 JUSTIFICATION/ CERTIFICATION OF QUESTIONNAIRE

To ensure the justification of the questionnaire, the questions asked in the questionnaires distributed corresponds with the statement of problem, research questions and literature review to a great extent before it will be forwarded to the supervisor for corrections and approval.

The first section of the questionnaire deals with demographic responses from the respondents. A total of one hundred and fifty (150) questionnaires will be administered among various Secondary Schools in Shomolu Local Government area of Lagos. These schools include Shomolu Senior High School, Igbobi College Yaba and Angus Memorial Senior High School. These therefore constitute part of the sampling size used in successful conduct of this research. Random sampling method was used because the whole population could not be reached individually.

3.3 METHOD OF DATA ANALYSIS

The data obtained through the questionnaires was analysed systematically using statistical tools such as percentage, frequency, bar charts and pie charts. The data collected were collated using tally technique to obtain frequency count, and percentage comparison technique was used to form our opinion.

$$Percentage = \frac{NumberoOf\ \mathrm{Re}\,sponse}{Total\ \mathrm{Re}\,sponses} x100$$

Graphs were also plotted from the data for easy relative comparison.

3.4 RESEARCH QUESTIONS

In this study we designed a questionnaire (see Appendix), to gather data to be used to provide answers to the following research questions:

1. What is the rate of cyber-crime in Nigeria?
2. Who are the most perpetuators of cyber-crime in Nigeria?
3. What is the level of awareness of cyber laws in Nigeria?
4. What is the level of occurrence of cyber-crime in Nigeria?

3.5 POPULATION SIZE

One hundred and fifty questionnaires were designed as population sample size of this study. They were distributed among students in the three schools. Random sampling was used to choose students at random without bias.

SCHOOL	**QUESTIONNAIRES ADMINISTERED**	**VALID QUESTIONNAIRES RETURNED**	**INVALID QUESTIONNAIRES RETURNED**
Shomolu Senior High School	50	50	0
Igbobi College	60	60	0
Angus Memorial High School	40	40	0
Total sampling size	150		

CHAPTER FOUR

4.0 DATA PRESENTATION AND ANALYSIS

4.1 RESULT AND DISCUSSION

The basic focus of this chapter is the presentation of collected data from the field of study. These data are analyzed using the simple statistical tables, graphs and comprehensible language. Both demographic and psychographic variables of respondents, as they are contained in the study instrument (i.e. questionnaires) are employed.

SECTION A

4.2 DEMOGRAPHIC ANALYSIS

Table 1: Gender of respondents

		Frequency	Percent
Valid	Female	54	36.0
	Male	96	64.0
	Total	150	100.0

Source: Field survey 2015

Interpretation

As shown in Table 1 above, 54 respondents, thus constituting 36% of the sample populations are female and 64% of the respondents are male. This shows that there are more of male respondent than female.

Table 2: Respondents distribution by age

		Frequency	Percent
Valid	18-24	42	28.0
	25-30	2	1.3
	below 18	106	70.7
	Total	150	100.0

Source: *field survey 2015*

Interpretation

The above table shows that 28% of the respondents are”18-24” age range, while 1.3% are “25-30” age range and 70.7% are “below 18” age range. This denotes that “below 18” age range responded more to the question than the others.

Table 3: Respondents distribution by marital status

		Frequency	Percent
Valid	married	1	.7
	single	149	99.3
	Total	150	100.0

Source: field survey (2015)

Interpretation

The above table shows that .7% of the respondents are married, and 99.3% are single. This depicts that most of the respondents are single.

Table 4: Respondents distribution by religion

	Frequency	Percent
christianity	103	68.6
islam	34	22.7
traditional	13	8.7
Total	150	100.0

Source: field survey (2015)

Interpretation

The above table shows that 68.6% of the respondents are Christians, while 22.7% are Muslims and 8.7% are traditional worshippers. This shows that more Christian responded to the questionnaire than the others.

SECTION B

4.3 FINDINGS

Table 5: Distribution of respondents on 'Do you know anything about cyber-crime?'

		Frequency	Percent
Valid	no	52	34.7
	not sure	9	6.0
	yes	89	59.3
	Total	150	100.0

Source: *field survey 2015*

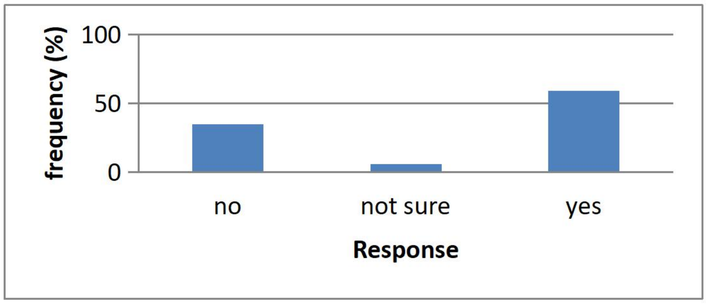

Chart representation of data

Interpretation

Table 6 above shows the distribution of respondents on 'do you know anything about cyber-crime?' It shows that 34.7% of the respondents do not know anything about cyber-crime, 6% are not sure and 59.3% do know what cyber-crime is. This means that most of the respondents know what cyber-crime is.

Table 6: Respondents distribution on 'Have you ever been a victim of cyber crime?'

		Frequency	Percent
Valid	no	135	90.0
	not sure	4	2.7
	yes	11	7.3
	Total	150	100.0

Source: *field survey 2015*

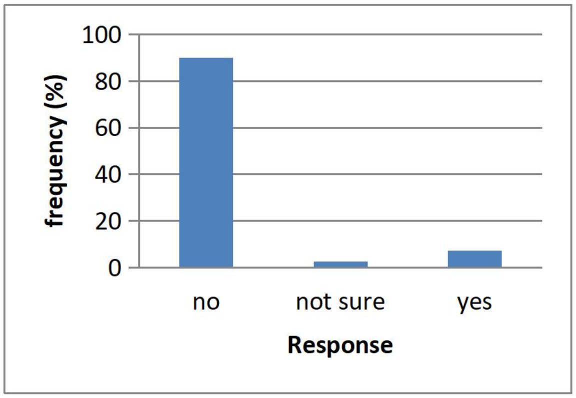

Chart representation of data

Interpretation:

Table 6 above, shows the distribution of respondents on 'Have you ever been a victim of cyber-crime?' it shows that 90% of the respondents have never been a victim of cyber-crime, 2.7% are not sure and 7.3% have been a victim of cyber-crime. This means that most of respondents have not been a victim of cyber-crime.

Table 7: Distribution of respondents on 'Is the level of cyber-crime in Nigeria high?'

	Frequency	Percent
no	24	16.0
not sure	36	24.0
yes	90	60.0
Total	150	100.0

Source: *field survey 2015*

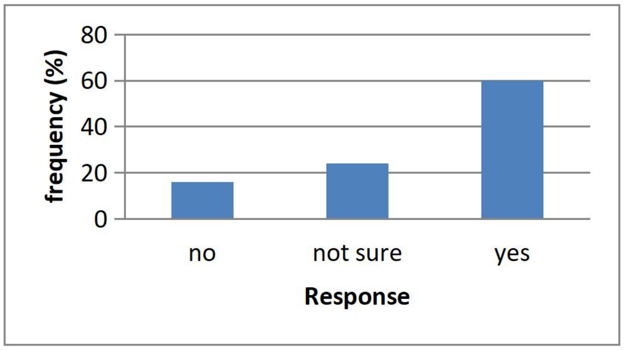

Chart representation of data

Interpretation:

Table 7 above, shows the distribution of respondents on 'Is the level of cyber-crime in Nigeria high?' It shows that 16% of the respondents belief it is not high, 24% are not sure, and 60% belief the rate is high. This means that most of the respondent belief the rate of cyber-crime in Nigeria is high.

Table 8: Distribution of respondents on 'Has the Nigerian Government being able to reduce or combat cyber-crime?'

	Frequency	Percent
no	75	50.0
not sure	51	34.0
yes	24	16.0
Total	150	100.0

Source: *field survey 2015*

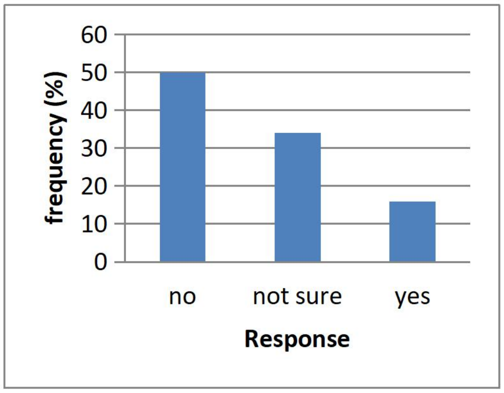

Chart representation of data

Interpretation:

Table 8 above, shows the distribution of respondents on 'Has the Nigerian government being able to combat cyber-crime?' It shows that 50% of the respondents belief Nigeria government has not being able to combat cyber-crime, 34% are not sure and 16% belief Nigeria government have being able to combat cyber-crime. This means that most of the respondent belief Nigeria government have not being able to combat cyber-crime.

Table 9: Distribution of respondents on 'Is cyber-crime perpetuated mostly in the cyber café?'

	Frequency	Percent
no	50	33.3
not sure	38	25.3
yes	62	41.4
Total	150	100.0

Source: *field survey 2015*

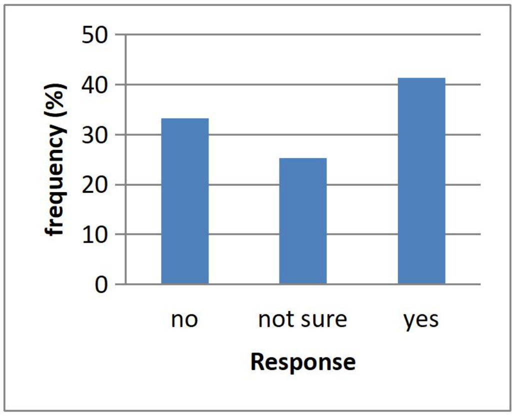

Chart representation of data

Interpretation:

Table 9 above, shows the distribution of respondents on 'Is cyber-crime perpetuated mostly in the cyber-café?' It shows that 33.3% of the respondent belief cyber-crime is not perpetuated in the cyber café, 25.3% are not sure and 41.4% belief cyber-crime is perpetuated mostly in the cyber café. This means that most of the respondent belief cyber-crime is mostly perpetuated in the cyber café.

Table 10: Distribution of respondents on the occurrence of online identity theft (including phishing and online trafficking in false identity information)

	Frequency	Percent
has not occurred	15	10.0
occur frequently	96	64.0
occur infrequently	38	25.3
Total	150	100.0

Source: *field survey 2015*

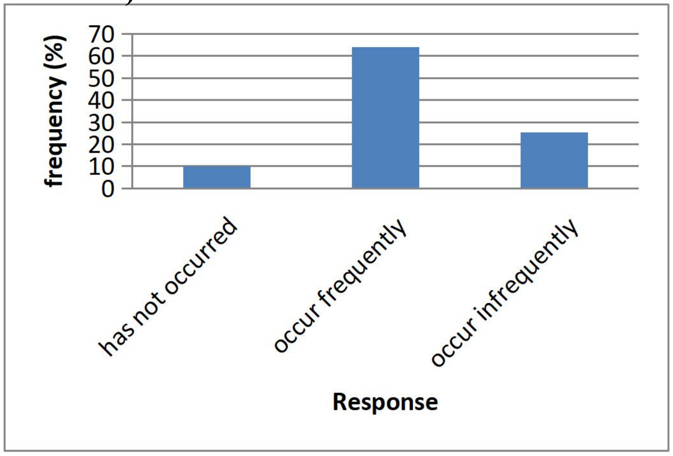

Chart representation of data

Interpretation:

Table 10 above, shows the distribution of respondents on the occurrence of online identity theft. It shows that 10% of the respondent belief online identity theft has not occurred, 64% belief it occurs frequently and 25.3% belief it occurs infrequently. This means that most of the respondent belief that online identity theft (including phishing and online trafficking in false identity information) occurs frequently.

Table 11: Distribution of respondents on occurrence of hacking as a forms and means of cyber-crime

	Frequency	Percent
has not occurred	10	6.7
occur frequently	117	78.0
occur infrequently	23	15.3
Total	150	100.0

Source: *field survey 2015*

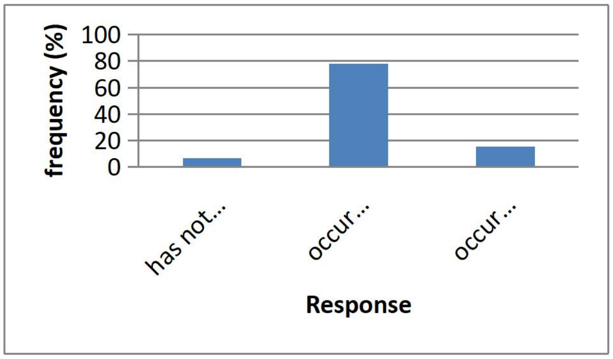

Chart representation of data

Interpretation:

Table 11 above, shows the distribution of respondents on the occurrence of hacking as a forms and means of cyber-crime. It shows that 6.7% of the respondents belief hacking has not occurred, 78% beliefs hacking occurs frequently and 15.3% belief it occur infrequently. This means that most of the respondents belief hacking (illegal intrusion into computer system; theft of information from computer systems) as a forms and means of cyber-crime occurs frequently.

Table 12: Distribution of respondents on the occurrence of malicious code as a means and forms of cyber-crime

	Frequency	Percent
has not occurred	15	10.0
occur frequently	83	55.3
occur infrequently	52	34.7
Total	150	100.0

Source: *field survey 2015*

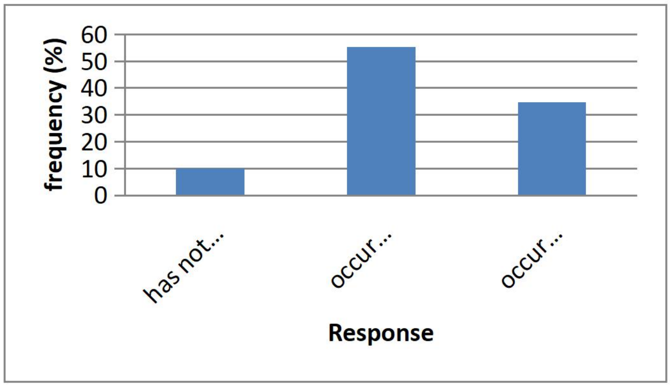

Chart representation of data

Interpretation:

Table 12 above, shows the distribution of respondents on the occurrence of malicious code as a means of cyber-crime. It shows that 10% of the respondent belief malicious code has not occurred, 55.3% belief it occurs frequently and 34.75% belief it occurs infrequently. This means that most of the respondent belief that malicious (worms, viruses, malware and spyware) as a means and forms of cyber-crime occurs frequently.

Table 13: Distribution of respondents on the occurrence of illegal interception of computer data

	Frequency	Percent
has not occurred	13	8.7
occur frequently	89	59.3
occur infrequently	48	32.0
Total	150	100.0

Source: *field survey 2015*

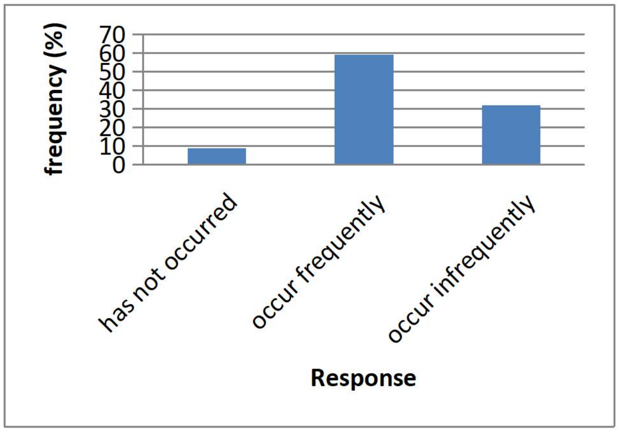

Chart representation of data

Interpretation:

Table 13 above, shows the distribution of respondents on the occurrence of illegal interception of computer data. It shows that 8.7% of the respondent belief illegal interception of computer data has not occurred, 59.3% belief it occurs frequently and 32% belief it occurs infrequently. This means that most of the respondent belief illegal interception of computer data occurs frequently.

Table 14: Distribution of respondent on the occurrence of online commission of intellectual property crimes

	Frequency	Percent
has not occurred	26	17.3
occur frequently	70	46.7
occur infrequently	54	36.0
Total	150	100.0

Source: *field survey 2015*

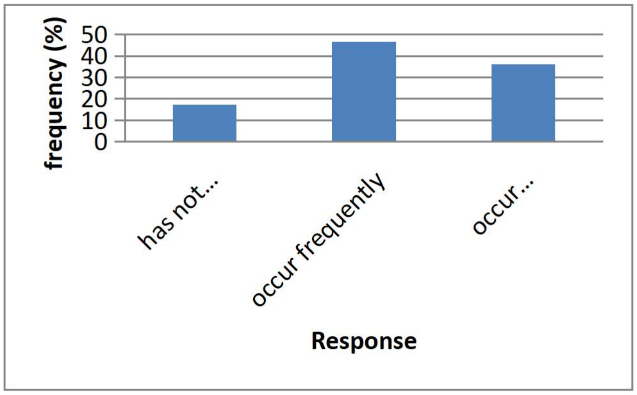

Chart representation of data

Interpretation:

Table 14 above, shows the distribution of respondents on the occurrence of online commission of intellectual property crimes. It shows that 17.3% of the respondent belief online commission of intellectual property crime has not occurred, 46.7% belief it occurs frequently and 36% belief it occurs infrequently. This means that most of the respondent belief that online commission of intellectual property crime occurs frequently.

Table 15: Distribution of respondents on the occurrence of online trafficking in child pornography

	Frequency	Percent
has not occurred	14	9.3
occur frequently	100	66.7
occur infrequently	33	22.0
Total	150	100.0

Source: *field survey 2015*

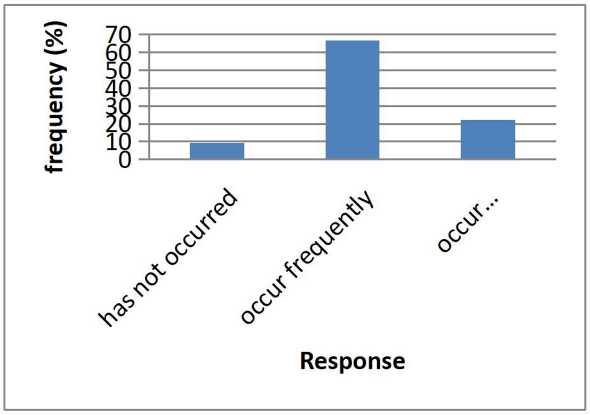

Chart representation of data

Interpretation:

Table 15 above, shows the distribution of respondents on the occurrence of online trafficking in child pornography. It shows that 9.3% of the respondent belief that online trafficking in child pornography has not occurred, 66.7% belief it occurs frequently and 22% belief it occurs in frequently. This means that most of the respondent belief online trafficking in child pornography occurs frequently.

Table 16: Distribution of respondents on the occurrence of intentional damage to computer system or data

	Frequency	Percent
has not occurred	21	14.0
occur frequently	63	42.0
occur infrequently	66	44.0
Total	150	100.0

Source: *field survey 2015*

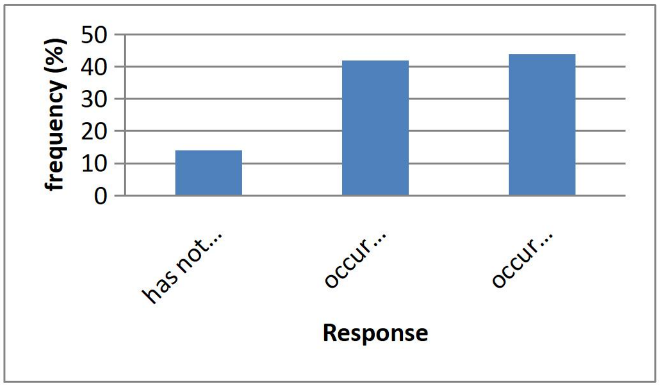

Chart representation of data

Interpretation:

Table 16 above, shows the distribution of respondents on the occurrence of intentional damage to computer system or data. It shows 14% of the respondent belief intentional damage to computer system of data has not occurred, 42% belief it occurs frequently and 44% belief it occurs infrequently. This means that most of the respondent belief intentional damage to computer system or data occurs infrequently.

Table 17: Distribution of respondents on has Nigeria identified, created or established a unit or entity specifically charged with dealing with cyber-crime incidents

	Frequency	Percent
I DONT KNOW	89	60.0
NO	33	22.0
YES	28	18.7
Total	150	100.0

Source: *field survey 2015*

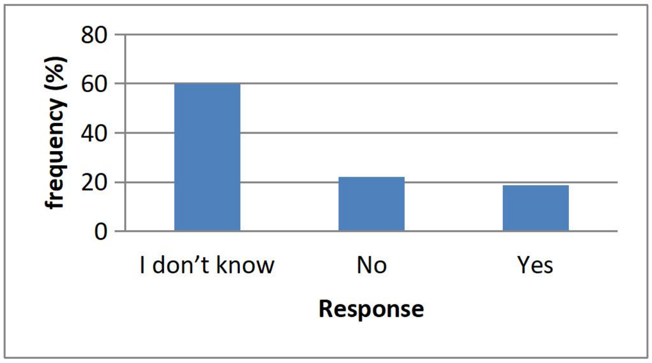

Chart representation of data

Interpretation:

Table 17 above, shows the distribution of respondents on has Nigeria identified, created or established a unit or entity specifically charged with dealing with cyber-crime incidents. It shows that 60% of the respondents don’t know whether Nigeria has created an entity to charge with dealings with cyber-crime, 22% belief Nigeria has not and 18.7% belief Nigeria has done it. This means that most of the respondents don’t know whether Nigeria has created an entity to charge with dealings with cyber-crime.

Table 18: Distribution of respondents on who are the people involved in cyber-crime

		Frequency	Percent
Valid	adults	20	13.3
	children	1	.7
	youths	129	86.0
	Total	150	100.0

Source: *field survey 2015*

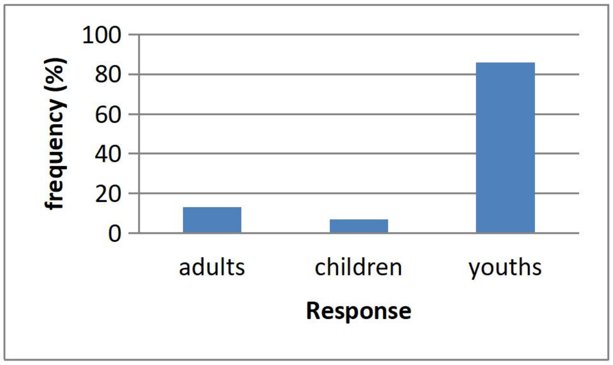

Chart representation of data

Interpretation:

Table 18 above, shows the distribution of respondents on who are the people involved in cyber-crime. It shows that 13.3% of the respondents agree that adults are the one involve in cyber-crime, .7% belief it is the children and 86% belief it is the youth. This means that most of the respondent belief it is the youth that get involve in cyber-crime.

4.4 DISCUSSION OF FINDINGS

Research Question 1: What is the rate of cyber-crime in Nigeria?

Discussion:

During the course of this study the researcher used Table 7 to discuss the above research question. It was discovered that 60% of the respondent belief that the rate of cyber-crime in Nigeria is high. This means the rate of cyber-crime in Nigeria is high.

The researcher used the above findings to draw his conclusion that the rate of cyber-crime in Nigeria is high

Research Question 2: Who are the most perpetuators of cyber-crime in Nigeria?

Discussion:

During the course of this study the researcher used Table 18 to discuss the above research question. It was discovered that 86% of the respondent belief youth are people that are involved in cyber-crime. This means that youth are involved mostly in cyber-crime.

From the above findings the researcher draws his conclusion that the youths are the most perpetuators of cyber-crime.

Research Question 3: What is the level of awareness of cyber laws in Nigeria?

Discussion:

During the course of this study the researcher used Table 14 to discuss the above research question. It was discovered that 60% of the respondents don’t know whether Nigeria government has created, identified, or established a unit or entity specifically charged with dealing with cyber-crime incidents.

The researcher draw his conclusion from the above findings that the level of awareness from Nigeria government on cyber-crime is low and that makes it difficult for the respondents to determine whether they have created or established a unit or entity specifically charged in dealing with cyber-crime.

Research Question 4: What is the level of occurrence of cyber-crime in Nigeria?

<u>Discussion:</u>

During the course of this study the researcher used Table 10-16 to discuss the above research question. It was discovered that 64% of the respondents belief that online identity theft occurs frequently in Nigeria. This means that online identity theft occurs frequently in Nigeria

It was also discovered that 78% of the respondents belief that hacking (illegal intrusion into computer system; theft of information from computer systems) occurs frequently. This means that hacking of computer system occurs frequently.

It was also discovered that 55.3% of the respondents belief that malicious code (worms, viruses, malware and spyware) occurs frequently. This means that malicious code occurs frequently in Nigeria.

It was also discovered that 59.3% of the respondents belief that illegal interception of computer data occurs frequently. This means that illegal interception of computer data occurs frequently in Nigeria.

It was also discovered that 46.7% of the respondent belief that online commission of intellectual property crimes. This means that online commission of intellectual property crimes occurs frequently in Nigeria.

It was also discovered that 66.7% of the respondent belief that online trafficking in child pornography occurs frequently. This means that online trafficking in child pornography occurs frequently in Nigeria.

It was also discovered that 44% of the respondent belief that intentional damage to computer systems or data occurs infrequently. This means that intentional damage to computer system or data occurs infrequently in Nigeria.

The researcher draws his conclusion from the above findings that the level of occurrence of cyber-crime in Nigeria. This because most of the cyber-crimes occurs frequently in Nigeria except that of intentional damage to computer system or data.

CHAPTER FIVE

SUMMARY AND CONCLUSION

5.0 SUMMARY

The objectives of this study were to provide a clear overview of cyber-crime and cyber-security, to provide methods through which cyber security can be improved, to outline the challenges associated with cybercrime in Nigeria, to carry out a research on the view of Nigerian students on cyber-crime, to examine the roles of youths in cyber-crime perpetration in Nigeria and to provide the unemployed Nigerian ICT expert with alternatives to cyber-crime.

The first three objectives (i.e. to provide a clear overview of cyber-crime and cyber-security, to provide methods through which cyber security can be improved, to outline the challenges associated with cybercrime in Nigeria) were properly discussed in the literature review where various terms used in cyber-crime were explained; various forms of cyber-crime were also explained. The concept of cyber security in Nigeria was properly examined; its challenges and ways of improving cyber security were discussed.

In summary terms like hacking, phishing, data espionage, illegal interception, child pornography, religious offences, illegal gamble and online games, data interference etc. are the basic forms of cyber-crime activities. Cyber-crime takes one of these shapes depending on the intention of the perpetrator.

Furthermore, we discussed the cyber-security and its challenges. Some of the stated factors that make Nigeria vulnerable to cyber-crime are: Domestic and international law enforcement, unemployment, poverty rate, corruption, Lack of standards and National Central Control.

Research questions were analyzed using frequency table analysis to draw conclusions on the view of students on cyber-crime and the roles of youths in cyber-crime perpetuation. The researcher administered questionnaire as the source of primary data. The questionnaires were administered to students in Shomolu local government to get unbiased information from secondary school students. A total number of one hundred and fifty (150) questionnaires were administered out of which all were returned and valid. Therefore, one hundred and fifty were used to represent the sample population of the study.

5.1 CONCLUSION

Our result indicated that the rate of cyber-crime in Nigeria is high. This result could be associated with weak security measures and firewalls. There should be introduction of latest cyber security technologies to check this issue. Education of computer users on the issue of cybercrime should also be encouraged in the country.

Cyber-crime rate will not be able to be reduced if computer users are not made to know the various available security measures. The result shows that most people do not know if there are provisions by the government to combat cyber-crime. The government has a role to play in bringing everyone to the understanding of cyber-crime laws in Nigeria and punishment for its violation.

Unemployment in the country made so many people especially youths to seek for other means of employment of which cyber-crime is a major option. Our result also shows that most perpetrators of cyber-crime are youths, most of which are not employed. Provision of employment and encouragement of personal skills will go a long way in bringing cyber-crime to a check in the country.

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.

APPENDIX 1 (QUESTIONAIRE)

YABA COLLEGE OF TECHNOLOGY

DEPARTMENT OF COMPUTER TECHNOLOGY

Dear Respondent,

I am a student of the above named institution currently carrying out a research study on cyber-crime.

The aim of this research is to understand the Nature, causes and consequences of Cyber-crime in Nigeria.

Kindly note that this questionnaire is for academic purposes only; therefore your responses will be treated with utmost confidentiality. As you respond objectively to these items give your candid opinion by providing answers to the questions asked. Your cooperation and participation would be highly appreciated.

SECTION A

PLEASE PUT A TICK (√) IN THE BOX NEXT TO THE ANSWER OF YOUR CHOICE OR WRITE IN THE SPACE PROVIDED AS THE CASE MAY BE.

SEX : □ **MALE** □ **FEMALE**

AGE: □ **18-24** □ **25-30** □ **31-35** □ **OTHERS**

RELIGION: □ **ISLAM** □ **CHRISTIANITY** □ **TRADITIONAL** □ **OTHERS**

MARITAL STATUS: □ **SINGLE** □ **MARRIED**

SECTION B

S/N	STATEMENT / QUESTION	Yes	No	Not sure
1.	Do you know anything about cyber-crime?			
2.	Have you ever been a victim of cyber-crime?			
3.	Is the level of cyber-crime rate in Nigeria high?			
4.	Have the Nigerian Government being able to reduce or combat cyber-crime?			
5.	Is cyber-crime perpetuated mostly in the cyber café?			

Please identify whether the following forms and means occur frequently, occur infrequently or have not occurred by placing a tick (√) as appropriate in the following tables.

S/N	Forms and Means of Cyber-Crime	Occur Frequently	Occur Infrequently	Has not Occurred
6.	Online identity theft (including phishing and online trafficking in false identity information)			
7.	Hacking (illegal intrusion into computer systems; theft of information from computer systems)			
8.	Malicious code (worms, viruses, malware and spyware)			
9.	Illegal interception of computer data			
10.	Online commission of intellectual property crimes			
11.	Online trafficking in child pornography			
12.	Intentional damage to computer systems or data			

13. Has Nigeria identified, created or established a unit or entity specifically charged with dealing with cyber-crime incidents?

□ Yes □ no □ I don't Know

14. Who are the people involved in cyber-crime?

□ Youths □ Adults □ children

REFERENCES

Adebusuyi, A. (2008): The Internet and Emergence of Yahooboys sub-Culture in Nigeria, International Journal Of Cyber-Criminology, 0794-2891, Vol.2(2) 368-381, July-December

BBC News, Tiny Macau overtakes Las Vegas, at: http://news.bbc.co.uk/2/hi/business/6083624.htm

Bloxsome/Kuhn/Pope/Voges, The Pornography and Erotica Industry: Lack of Research and Need for a Research Agenda, Griffith University, Brisbane, Australia: 2007 International Nonprofit and Social Marketing Conference, 27-28 Sep 2007, page 196.

Carr, Child Abuse, Child Pornography and the Internet, 2004, page 8.

Chawki, Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview/;

Child Pornography, CSEC World Congress Yokohama Conference, 2001, page 17; Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007

Conway, Terrorist Uses of the Internet and Fighting Back, Information and Security, 2006, page 16, United States Department of Justice 1997 Report on the availability of bomb-making information, available at: www.usdoj.gov/criminal/cybercrime/bombmakinginfo.html; Sieber, Council of Europe Organised Crime Report 2004, page 141.

Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int.

Council of Europe, Resolution ResAP(2007)2 on good practices for distributing medicines via mail order which protect patient safety and the quality of the delivered medicine, available at: https://wcd.coe.int/ViewDoc.jsp?Ref=ResAP(2007)2&Language=lanEnglish&Ver=original&Site=c &BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75.

Cybercrime, Definition and General Information, Australian Institute for Criminology, available at: www.aic.gov.au/topics/cybercrime/definitions.html;

Cybercrime, Report of the Parliamentary Joint Committee on the Australian Crime Commission, 2004, page 5, available at:www.aph.gov.au/Senate/Committee/acc_ctte/completed_inquiries/2002-04/cybercrime/report/report.pdf;

Dr. Ibikunle Frank, Department of Electrical & Information Engineering, Covenant University, Nigeria E-mail: faibikunle2@yahoo.co.uk

Erickson, Hacking: The Art of Exploitation, 2003.

Eweniyi Odunayo, Department of Electrical & Information Engineering, Covenant University, Nigeria

Explanatory Report to the Council of Europe Convention on Cybercrime, No. 8; Gordon/Ford, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20

Federal Computer Systems Protection Act of 1977. For more information, see: Schjolberg, Computer-related Offences, Council of Europe, 2004, page 2, available at: www.cybercrimelaw.net/documents/Strasbourg.pdf

Goodman/Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf;

Hayden, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3; Hale, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at: www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37; Forst, Cybercrime: Appellate Court Interpretations, 1999, page 1.

Heise News, 23.10.2007, available at: www.heise-security.co.uk/news/97803.

Information Security – Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3, available at: www.globalsecurity.org/security/library/report/gao/d03837.pdf; Sieber, Council of Europe Organised Crime Report 2004

ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at:www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

J.C.R. Licklider & W. Clark, "On-Line Man Computer Communication," August 1962.

Joyner/Lotrionte, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002

Kabay, A Brief History of Computer Crime: An Introduction for Students, 2008, www.mekabay.com/overviews/history.pdf.

Krishna Kumar. 2003. Cyber Laws, International Property and e-commerce Security, Dominant Publishers and Distributors New Delhi.

Kumar, Cyber Law, A view to social security, 2009, page 29.

L. Kleinrock, "Information Flow in Large Communication Nets," RLE Quarterly Progress Report, July 1961.

L. Kleinrock, Communication Nets: Stochastic Message Flow and Delay, Mcgraw-Hill (New York), 1964

L. Roberts & T. Merrill, "Toward a Cooperative Network of Time-Shared Computers," Fall AFIPS Conf., Oct. 1966

L. Roberts, “Multiple Computer Networks and Intercomputer Communication,” ACM Gatlinburg Conf., October 1967. ACM.

Lanning, Child Molesters: A Behavioral Analysis, 2001, page 63.

Longe, O. B, Chiemeke, S. (2008): Cyber Crime and Criminality In Nigeria – What Roles Are Internet Access Points In Playing?, European Journal Of Social Sciences – Volume 6, Number 4

McLaughlin, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2

Mohsin, A. (2006): Cyber Crimes And Solutions, Retrieved from http://ezinearticles.com/?Cyber-Crimes-And-Solutions&id=204167

Nowara/Pierschke, Erzieherische Hilfen fuer jugendliche Sexual(straf)taeter, Katamnesestudie zu den vom Land Nordrhein-Westfalen gefoerterten Modellprojekten, 2008

Okonigene Robert Ehimen, Adekanle Bola Cybercrime in Nigeria, 2009

P. Baran, “On Distributed Communications Networks,” IEEE Trans. Comm. Systems, March 1964.

Paul Taylor (in ENGLISH). November 3, 1999 ed. Hackers: Crime in the Digital Sublime. Routledge; 1 edition. Pg.. 200

Postini, 2007 www.postini.com/stats/

Proceedings of the IEEE, Special Issue on Packet Communication Networks, Volume 66, No. 11, November, 1978. (Guest editor: Robert Kahn, associate guest editors: Keith Uncapher and Harry van Trees)

Prof. Dr. Marco Gercke: Understanding cybercrime: Phenomena, challenges and legal response

Quinn, Computer Crime: A Growing Corporate Dilemma, The Maryland Law Forum, Vol. 8, 1978

Ramjit Singh Hunda, Kawajeet Singh and M. D. Singh. 2004. Aspects to Ensure Admissibility of Digital Evidence, Law Journal Gurn Nanak dev University Amritsar, Vol. 13, Pg. 1

Ropelato, Internet Pornography Statistics, available at: http://internet-filter-review.toptenreviews.com/internetpornography-statistics.html.

Roth, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

Rown/Raysman, Property Rights in Cyberspace Games and other novel legal issues in virtual property, The Indian Journal of Law and Technology, Vol. 2, 2006, page 87 et seq. available at: www.nls.ac.in/students/IJLT/resources/2_Indian_JL&Tech_87.pdf.

S. Crocker, RFC001 Host software, Apr-07-1969.

Schaeffer, B. S., et al. (2009): Cyber Crime And Cyber Security: A White Paper For Franchisors, Licensors, and Others

Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8.

Shun-Yung Kevin Wang and Wilson Huang Internet Journal of Criminology 2011

Sieber, Council of Europe Organised Crime Report 2004, page 65. Regarding the threat of spyware, see Hackworth, Spyware, Cybercrime and Security, IIA-4.

Simon/Slay, Voice over IP: Forensic Computing Implications, 2006.

Slivka/Darrow; Methods and Problems in Computer Security, Journal of Computers and Law, 1975

Sofaer, Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001
Tedford/Herbeck/Haiman, Freedom of Speech in the United States, 2005; Barendt, Freedom of Speech, 2007

Tempelton, Reaction to the DEC Spam of 1978, available at: www.templetons.com/brad/spamreact.html.

The Economic Times. September 11, 2004. 1.

The Guardian Wednesday, July 9, 2008 Pg. 39

The Online-Community HackerWatch publishes reports about hacking attacks. Based on their sources, more than 250 million incidents were reported in the month of August 2007. Source: www.hackerwatch.org.

The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf.

Third Interpol Symposium on International Fraud, France 1979.

Thompson, D. (1989): Police Powers-Where's the Evidence, Proceedings of the The Australian Computer Abuse Inaugural Conference

Thorhallsson, A User Perspective on Spam and Phishing, in Governing the Internet Freedom and Regulation in the OSCE Region, page 208, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

Times Online, 70.000 gather for violent Pakistan cartoons protest, available at: www.timesonline.co.uk/tol/news/world/asia/article731005.ece;

UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication, Sales No. E.94.IV.5), available at: www.uncjin.org/Documents/EighthCongress.html.

V. G. Cerf and R. E. Kahn, "A protocol for packet network interconnection," IEEE Trans. Comm. Tech., vol. COM-22, V 5, pp. 627-641, May 1974.

Velasco San Martin, Jurisdictional Aspects of Cloud Computing, 2009; Gercke, Impact of Cloud Computing on Cybercrime Investigation, published in Taeger/Wiebe, Inside the Cloud, 2009, Walden, Computer Crimes and Digital Investigations, 2006, Chapter 3.250

Walden, Computer Crimes and Digital Investigations, 2006, Chapter 3.192.

Weekes, Cyber-Zoning A Mature Domain: The Solution to Preventing Inadvertent Access to Sexually Explicit Content on the Internet, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue1/v8i1_a04-Weekes.pdf.

Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf

Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007

Wilson, Computer Attacks and Cyber Terrorism, Cybercrime & Security, IIV-3, page 5.

Wortley/Smallbone, Child Pornography on the Internet, Problem-Oriented Guides for Police, USDOJ, 2006, page, 1.