The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria

Folashade B. Okeshola

Abimbola K. Adeta

Department of Sociology
Ahmadu Bello University
Zaria, Nigeria.

Abstract

In Nigeria today, numerous internet assisted crimes are committed daily in various forms such as identity theft, desktop counterfeiting, internet chat room, cyber harassment, fraudulent electronic mails ,Automated Teller Machine spoofing, pornography, piracy, hacking, phishing and spamming. Usually these crimes are committed in forms like sending of fraudulent and bogus financial proposals from cyber criminals to innocent internet users. The increasing rates of cyber crime in the society have become a strong threat to Nigeria's e-commerce growth and has led to ill- reputation intentionally and consequently denied some innocent Nigerians certain opportunities abroad. Therefore, innocent internet users should inculcate the habit of continuously updating their knowledge about the ever changing nature of ICTs, through this, they can not only be well informed about the current trends in cyber crimes, but they will also have the knowledge about different forms of the said crimes and how the cyber criminals carry out their heinous activities. Thus, they can devise means of protecting their information from cyber criminals. Internet users should be security conscious. On the whole, this paper examines the nature, causes, types and consequences of cyber crime in tertiary institutions in Zaria, Kaduna State.

Key Words: Crime, Cyber crime, Cyber criminal, internet, Fraud, Perpetrator

Introduction

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 (which also includes eavesdroppers and criminals), false pretence finds a fertile ground in this situation.

However, information technology revolution associated with the internet has brought about two edge functions: that is on one hand, it has contributed positive values to the world. While on the other hand, it has produced so many maladies that threaten the order of the society and also producing a new wave of crime to the world. The internet online business services, which ordinarily suppose 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.

Shinder (2002), define cyber crime as any criminal offenses committed using the internet or another computer network as a component of the crime. Cyber crimes are offences that are committed against individual or group of individuals with a criminal motive to internationally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly using modern telecommunication networks such as internet and mobile phones. Such crimes may threaten nation's security and financial health (Akogwu, 2012).

Research Problem

The contribution of internet to the development of the nation has been marred by the evolution of new waves of crime. The internet has also become an environment where the most lucrative and safest crime thrives. Cyber crime has become a global threat from Europe to America, Africa to Asia. Cyber crime has come as a surprise and a strange phenomenon that for now lives with us in Nigeria. With each passing day, we witness more and more alarming cases of cyber crimes in Nigeria, with each new case more shocking than the one before.

It has become a stubborn mouth sore which causes us a lot of pain and shame because criminally minded individuals in the country are stealing and committing atrocity through the aid of the internet online business transactions.

The youths in every society is of great importance and concern to that society because they are looked upon as the leaders of tomorrow. Olaide and Adewole (2004), observed that a sizeable number of criminals in Nigeria fall within the youthful age. The youths at present have discovered different ways of using the internet in doing different types of criminal activities and these age brackets are usually found in tertiary institutions in Nigeria.

Nigeria is not the only nation where cyber crimes are being perpetrated. The incident can rightly be said to be on the increase in the country due to lack of security awareness and under reportage respectively. Although some people's level of knowledge of the net is observably just for chatting with their friends and may be get information there from, most of them may not be in the position to protect their data or information and computer from malicious programmers (Akogwu, 2012).

In most Nigeria tertiary institutions, various form of crimes are being witnessed ranging from examination malpractices, falsification of admission, rape, robbery and stealing, sexual abuse, assault, cultism amongst others. But in recent times cyber crime a new form of crime now exists in our tertiary institutions which is denting and drilling holes in the economy of the nation. it is also leading to the erosion of confidence in genuine Nigerian commercial credibility and today many western countries with France taking the lead have moved to deny Nigerian businessmen and women who are legitimate the rewards of e-commerce. France today requires web camera verification for most online business transactions from Nigeria.

Studies that focuses on cyber crime largely concentrates on situations in the western world forgetting that the nature of cyber crime is such that geographical and political boundaries are being rendered irrelevant. A person who has access to computer and connected to the internet might be participating, attempting or planning a criminal act anywhere in the world (Kumar, 2003). Awe (2009), confirmed that computer attacks can be generated by criminals from anywhere in the world, and executed in other areas, irrespective of geographical location. And often these criminal activities can be faster, easier and more damaging with the use of the internet. The above statement shows that it is a global issue and as such, has become an image nightmare for the Nigeria government to identify the remote causes and proffer solution.

In Nigeria, perpetrators of this crime who are usually referred to as "yahoo yahoo boys" are taking advantage of e-commerce system available on the internet to defraud victims who are mostly foreigners in 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 pose to have financial institution where money can be loaned out to prospective investors. In this regard, so many persons have been duped or fallen victims. But this could not only be the techniques used by these cyber criminals.

Attempt to address cyber crime by various governments and international organizations have not been successful owing to the fact that the identities remain inadequate. A study by Zero Tolerance (2006) indicates that cyber criminals are usually within the age of 18 and 30 years and they indulge in the crime in order to survive and have a taste of good life. Noting these observations, there is need to identify more attributes these cyber criminals possess and identify other motivating factors since it have been acknowledged that a good taste of life is a major factor.

The questions that readily come to mind are: What are the socio-economic attributes of those involved in cyber crime? What are the factors that are responsible for youth involvement in cyber crime? What are the various cyber techniques used by cyber criminals to perpetrate the act? What are the control measures put in place by law enforcement agencies for operators of cyber cafe to curb cyber crime? What are the negative impacts the menace poses to the society?

Literature Review

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

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

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

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

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

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

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

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

Theoretical Perspective

In sociological analysis, theories are indispensable. They form an integral part of sociological research as it is a general principle that explains or predict facts, observation or events. The theory of differential association was adopted for this study. This theory was propounded by Edwin Sutherland an American Sociologist. Differential association theory proposed that through interaction with others, individuals learn the values, attitudes, techniques and motives for criminal behaviour. According to this theory, the environment plays a major role in deciding which norms people learn to violate (Sutherland, 1939).

The principle of differential association asserts that a person becomes delinquents because of an "excess" of definitions favourable to violation of law over definitions unfavourable to violation of law. What this means is that an individual will become a criminal because they are exposed to more favourable criminal behaviour. That is when one is exposed to more criminal influences rather than more favourable legal influences. In other word, criminal behaviour emerges when one is exposed to more social message favouring misconduct than pro – social messages. This can be seen in environments with poor socio-economic conditions which may encourage negative views towards the law and authority.

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

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

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

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

Methodology

Study Location

Zaria is a city in Northern Nigeria and it is located in Kaduna State. Zaria which used to be known as Zazzau at an earlier time is located within latitude $11^{o}3'$N and $11^{o}15'$N and longitude 7^{o} 42'E and $8^{o}45'$E of the Greenwich Meridian. Zaria is 80km north of Kaduna along the federal high way leading to Kano. The study was conducted in three (3) tertiary institutions in Zaria. These institutions are Ahmadu Bello University Zaria, Federal College of Education Zaria and Nuhu Bamali Polytechnic Zaria. These three tertiary institutions were selected because they represent all the types of tertiary education that an individual may attend to acquire knowledge and also because of the large presence of students.

Population and Sample Size

Considering the nature of the study, the population for the study was divided into four (4) categories. The population for the first category was drawn from students within the selected tertiary institutions. The population for the second category was drawn from operators of cyber cafe, while population of the third category was drawn from the lecturers of computer science Department of the selected tertiary institutions. The population for the last was drawn from cyber criminals within the study area.

For the purpose of this study both probability and non-probability sampling techniques were used to select the respondents. The probability sampling method that was used is the simple random sampling while the non-probability sampling methods were the purposive and snow ball sampling.

Questionnaires were distributed to the three (3) institutions in the following order based on their population.

Institutions	Population	No of Questionnaire Distributed
Ahmadu Bello University, Zaria	30081	242
Federal College of Education, Zaria	8645	70
Nuhu Bamali Polytechnic, Zaria	10994	88

For in-depth interview, four (4) respondents were purposively selected from the second category of respondents which are the operators of cyber cafe within Zaria. In addition, six (6) respondents that is two (2) respondents each from the selected tertiary institutions were purposely drawn from the third category. Finally, two (2) respondents were selected from the fourth category of the population using snowball sampling method. The first cyber criminal that participated in the research was identified with the assistance of an operator of cyber cafe. Thereafter, the second cyber-criminal was identified with the assistance of the first cyber-criminal.

Findings

The study adopted the use of triangulation method in the analysis and interpretation of data. The triangulation method involves the combination of both quantitative and qualitative method in the interpretation of the findings collected from the field. This method increases the validity of the study as findings from the various methods of data collection complement each other. In all, a total of 400 questionnaires were administered and 12 key informants were interviewed.

Socio-demographic Attributes of Respondents

This section presents the socio- demographic attributes of the respondents. The attributes are sex, age, religion and marital status of respondents.

Table 1: Socio-demographic Attributes of Respondents

Sex of Respondents	**Frequency**	**Percentage**
Male	300	75.0
Female	100	25.0
Total	400	100.0
Age	**Frequency**	**Percentage**
18 -24	232	58.0
25 -30	128	32.0
31 -35	20	5.0
36 and above	20	5.0
Total	400	100.0
Religion	**Frequency**	**Percentage**
Muslim	224	56.0
Christian	164	41.0
Traditional	12	3.0
Total	400	100.0
Marital Status	**Frequency**	**Percentage**
Single	328	82.0
Married	68	17.0
Divorced	4	1.0
Total	400	100.0

From the above table, it was found that 75% of the respondents are males while 25% are females. The number of male respondents who participated in the study outweighs the female respondents because most of the females felt it was a male issue. Most of the respondents are young and majority of the respondents are single. This is not surprising bearing in mind that the study was conducted in three tertiary institutions in Zaria. Also, majority of the respondents are Muslim followed by respondents who practice Christianity.

Nature of Cyber Crime by Respondents

This section examines the nature of cyber crime. It identified those involved in the crime, time of perpetration, perpetration point, frequency of occurrence and techniques used to perpetrate the act.

Views of respondents were sought on their access or use of internet. Findings reveal that 99% (396) said they access or use the internet. Only 1% (4) of the respondents stated not to access or use internet. We can conclude that virtually all the respondents use the internet for one activity or the other.

Table 2: Views of Respondents on the Activity they Access while on the Internet

Activity individual Access	Yes	No	Total
Google search	353 (88.3%)	47 (11.7%)	400 (100%)
Social media	315 (78.8%)	85 (21.2%)	400 (100%)
Academic research	308 (77.0%)	92 (23.0%)	400 (100%)
E-mail	296 (74.0%)	104 (26.0%)	400 (100%)
media/entertainment& news	267 (66.8%)	133 (33.2%)	400 (100%)
Sport	204 (51.0%)	196 (49.0%)	400 (100%)
Games	144 (36.0%)	256 (64.0%)	400 (100%)
Internet phoning	69 (17.3%)	331 (82.7%)	400 (100%)
Pornography	33 (8.3%)	367 (91.7%)	400 (100%)
Spamming	17 (4.3%)	383 (95.7%)	400 (100%)
Piracy	14 (3.5%)	386 (96.5%)	400 (100%)

From the table above, it shows that majority of the respondents access google search (88%), social media (79%) and academic research (77%). While only few respondents use the internet for pornography (8%), spamming (4%) and piracy (4%). It was found that respondents who access pornography are also involved in piracy and spamming while on the internet. The low response of the respondents was as a result of the sensitivity of the topic under study.

An in-depth interview conducted with a cyber criminal supported both social media and piracy.

> *According to him, basically there are many things I do on the internet but what I spend most of my time doing is on facebook, yahoo mail, chat room and piracy, I get cool money from downloading software and selling it.*

In a bid to know what he uses the social network for, he stated that "I use it to send fraudulent mail to my target".

Table 3: Views of Respondents as to whether they have heard of Cyber Crime

Heard of cyber crime	Frequency	Percentage
Yes	375	93.7
No	25	6.3
Total	400	100.0

The above table indicates that majority of the respondents (94%) have heard of cyber crime. This means that a very high percentage of the respondents are aware of the crime and are capable of filling, providing adequate and useful information to the questions in the questionnaire. Also, the results from the in-depth interview conducted shows that all the respondents interviewed were aware of the term cyber crime as they were able to define it.
One of the lecturers interviewed defined cyber crime as follows:

> *Cyber crime is derived from two words "cyber" and "crime". Cyber refer to any activities either sales or transaction of services in the cyber space while crime are unacceptable activities. When join together, it means all fraudulent, illicit and unacceptable activities related to cyber.*

All operators of cyber cafe agreed with the above definition and gave the definition of cyber crime as thus:

> *Cyber crime is committing crime through the internet, it does not necessarily mean it have to happen inside the cyber cafe, you can have your laptop, you have your modern in your house and you commit crime; hack people's mail. That is cyber crime.*

In addition, a cyber criminal when asked during the in-depth interview how long he has been involved in cyber crime, he stated that "*I have been doing it for a while let say 4 to 5 years now*".
From the findings, it can be deduced that virtually all the respondents are aware of the existence of cyber crime in the society.

Table 4: Views of Respondents on the Frequency of Cyber Crime Occurrences in Zaria

Frequency of Occurrence	Frequency	Percentage
Frequent	197	49.3
Not frequent	173	43.2
Undecided	30	7.5
Total	400	100.0

As regards frequency of cyber crime in Zaria, it was found that majority of respondents about (50%) agreed that they hear reports of cyber crime frequently in Zaria.
The in-depth interview with key informants agreed that cyber crime is frequent in Zaria. For instance an operator of cyber cafe states that:

> *When my cafe was newly open in 2010, customers that come to browse try to beat our timing system until measures were put in place to curtail them from stealing our time. But people still come to send fraudulent mail and as you can see, we don't allow flash drive into our system.*

A cyber criminal aired his view on the frequency of cyber crime in Zaria as follows:

> *Cyber crime is frequent in Zaria but an ordinary person won't know except when you have fallen victim and this is due to the high level of poverty and many graduates are unemployed. Some have computer skill, so they will use what they have to survive.*

In addition a lecturer stated that:

> *Cyber crime is any crime committed via the internet, so people watching pornography is committing crime, those people sending fraudulent e-mail that is phishing is also committing crime. And those trying to download academic material, text books or soft ware from the internet without paying for it are also committing crime. So you can see that everybody is involved in this crime.*

Table 5: Views of Respondents on Persons Usually Involved in Cyber Crime

Person involved in cyber crime	Frequency	Percentage
Youth	346	86.5
Adult	45	11.3
Aged	9	2.2
Total	400	100.0

As for people involved in cyber crime, findings show that majority (87%) of those who are usually involved in cyber crime are youths. This view is in agreement with the responses from the qualitative data. For instance, an operator of cyber cafe aired his view that "young people are mostly involved in one kind of cyber crime or the other".

As to the time of perpetration of cyber crime, it was found that about 50% (197) of the respondents agreed that cyber crime is perpetrated any time of the day. While 43% (173) said it was perpetrated in the night, with 7% (30) of the respondents who said cyber crime is perpetrated in the day time.

Findings from the in-depth interview also agree with the fact that it can be committed at anytime of the day. For instance a cyber criminal stated that:

> *Cyber criminal have mastered the use of time while committing/carrying out their criminal activities. For example in ATM fraud, when cyber criminals discovered an account, they carry out their attacks mostly on weekends and mostly outside the state where the account is domiciled and at any time of the day.*

Table 6: Views of Respondents on Places where Cyber Crime is Perpetrated

Place	Yes	No	Total
Cyber cafe	323 (80.8%)	77 (19.2%)	400 (100%)
At home	317 (79.3%)	83 (20.7%)	400 (100%)
Private organisation	206 (51.5%)	194 (48.5%)	400 (100%)
Tertiary institution	168 (42.0%)	232 (58.0%)	400 (100%)
Government office	94 (23.5%)	306 (76.5%)	400 (100%)

The table above shows the perpetration points of cyber crime. Findings reveal that 81% of the respondents agreed that cyber crime is usually perpetrated at cyber cafe and 80% said at home. This is to confirm the earlier statement made by operators of cyber cafe that with the introduction of internet modems, blackberry and smart phones cyber crime could be committed at homes.

In line with the above statement, the qualitative data obtained from a cyber criminal has this to say when interviewed on what he used to browse or how he accessed the internet:

> *I have my private modem and laptop that I use to browse at home. Let me tell you, nowadays cyber criminals don't use the cafe any more, they now use wireless and blackberry to access the internet and operate comfortably from their homes.*

A lecturer during the in-depth interview stated that:

> *My view on the perpetrated point of crime is the home. This is due to the fact that even ordinary Nokia C3 can browse and with the reduction in the price of MB, anybody who is interested in criminality can afford it.*

The above indicates that cyber criminals commit crime without leaving their homes.

Table 7: Views of Respondents on the Nomenclatures given to Perpetrators of Cyber Crime

Nomenclatures	Yes	No	Total
Yahoo yahoo boys	386(96.5%)	14(3.5%)	400(100%)
Yahoo millionaire	202(50.5%)	198(49.5%)	400(100%)
Yahoo zee	161(40.3%)	239(59.7%)	400(100%)
Forex trade	148(37.0%)	252(63.0%)	400(400%)

Findings reveal the nomenclatures that most cyber criminals are known as or usually nicknamed. Virtually all the respondents said that cyber criminals are nicknamed yahoo yahoo boyz. This implies that a large percentage of the people have heard of yahoo yahoo boyz and they equally know what they engaged in.

In support of the above statement, a lecturer in an in-depth interview stated that:

> *The name yahoo yahoo boy has become a household name. It simply refers to criminals who indulge in advance fee fraud schemes or involve in internet crime. These yahoo boys enjoy status of big boys in the society and are socially recognized among their friends and everywhere you see yahoo boys, other boys not involved in the crime will want to associate with them due to their flamboyant life style.*

Table 8: Views of Respondents on Techniques/Tools Cyber Criminals Usually Use to Perpetrate Cyber Crime

Techniques/Tools used	Yes	No	Total
Password cracker	349(87.3%)	51 (12.7%)	400 (100%)
Key loggers	213 (53.3%)	187 (46.7%)	400 (100%)
Network sniffer	212 (53.0%)	188 (47.0%)	400 (100%)
Exploit	187 (46.7%)	213 (53.3%)	400 (100%)
Port scanner	125 (31.3%)	275 (68.7%)	400 (100%)
Vulnerability scanner	88 (22.0%)	312 (78.0%)	400 (100%)

Findings show that a reasonable number of respondents 87% are aware of password cracker as a technique that cyber criminals use to carry out their illegal act. Also, 53% of the respondents are aware of key loggers as another technique cyber criminals use to perpetrate cyber crime. However, 31% and 22% of the respondents are aware of port scanner and vulnerability scanner as tools used by cyber criminals to perpetrate their act.
In addition, efforts were made using the in-depth interview to find out more techniques/ tools used by cyber criminals. Aside the aforementioned tools, a lecturer said that:

> *There are various techniques/ tools cyber criminal use to perpetrate their act. They can use mathematical model. A mathematical model is a process where cyber criminals sit down to design a program using Tree diagram, a statistical tools. This is then link with their victim account and the tree diagram keeps checking and checking until it gets the combination of that victim Pin number.*

> *Then there is also the phone techniques where the cyber criminal calls his/her victim to inform him/her that he/she has won a lottery and he/she direct his/her victim to a particular ATM. He ask his/her victim to check the ATM that there is something called phone charge it is suppose to be a cash transfer button but it is not written like that and he dictate a number to his/her victim. This number been dictated is his own personnel number and ask his/her victim type any amount of money and once the amount is typed, it is been deducted from the victim account number.*

Another lecturer in the interview stated that:

> *Cyber criminals use kernel level root kits to perpetrate their criminal act. They use this software to give themselves a backdoor and also to assist them cover their presence in your computer whenever your system is on. With this, they can see what you do but you can't notice their presence.*

To corroborate the aforementioned, a cyber criminal has this to say:

> *There are several types of techniques I know cyber criminal use to get their victim, it all depend on individual skills and talent. For example, some of us create websites that appear legitimate but in reality are scam designed to defraud or obtain information that can be used to commit further economic crimes.*

Similarly, another cyber criminal gave his own view on the techniques used by cyber criminals.

> *In credit card or ATM fraud, I know some of us have powerful software which could assist to access all the account numbers of people that have come to a particular ATM to withdraw. Once they scrutinize the account number and see the one that has big money in it, they then use another type of software to transferring the money into their own account instantly. Sometimes we use social network such as facebook and other chatting network to deceive people to give out their personal data or information.*

When further probe on the type of technique he use for software piracy, he stated as follows:

> *I use SQL injection to download software. Since most of the license key to the software are usually kept in a data base. I usually write series of code that usually go to the data base to fetch the keys and I download it to my system and I use the key instantly on the software. I also use key recorder and password reviler to get the key to software too.*

Concerning how they get their proceeds from their illicit act, a lecturer stated that cyber criminals get their proceeds either from any of the following means; domiciliary account, money gram or western union. From the above it implies that cyber criminals use the following techniques, password crackers, key loggers, mathematical model, SQL injection, man in the middle, creating of illegal websites, Honey pot and kernel level root kits to get their victims and they usually get their proceeds from the above mentioned means.

Types of Cyber Crime

This section examines the types of cyber crime that commonly exist in Zaria.

Table 9: Views of Respondents on the Common Types of Cyber Crime in Zaria

Types of cyber crime	Yes	No	Total
Hacking	339 (84.7%)	61 (51.3%)	400 (100%)
Credit card fraud	313 (78.3%)	87 (21.7%)	400 (100%)
Software piracy	252 (63.0%)	148 (37.0%)	400 (100%)
Cyber identity theft	242 (60.5%)	158 (39.5%)	400 (100%)
Cloning of website/Phishing	185 (46.3%)	215 (53.7%)	400 (100%)
Pornography	171 (42.7%)	229 (57.3%)	400 (100%)
Sweet heart swindle (Social network)	166 (41.5%)	234 (58.5%)	400 (100%)
Cyber defamation	153 (38.3%)	247 (61.7%)	400 (100%)
Malicious program/ Virus dissemination	128 (32.0%)	272 (68.0%)	400 (100%)
Cyber stalking	109 (27.3%)	291 (72.7%)	400 (100%)

The table above shows the common types of cyber crime that are in Zaria. Findings reveal that majority of the respondents are of the view that hacking (85%) and credit card frauds (78%) are the common type of cyber crime in Zaria. However, malicious program/virus dissemination (32%) and cyber stalking (27%) which are other types of cyber crime got low response from the respondents.

Other types of cyber crimes aside the listed ones that are common in Zaria according to respondents includes alteration or disclosure of data, trafficking in passwords and credit card number, lottery, educational scam where students only pay half the tuition fees and stealing of direct TV signals by modifying the card that goes into the satellite receivers.

Findings from the in-depth interview with key informants also identified other types of cyber crime common in the study area. A lecturer states that the common cyber crimes in Zaria are pin fraud, cheque fraud, theft of identity, phishing and economic fraud.

Similarly, a cyber criminal in the interview identified the type of cyber crime he usually indulges in. He stated that:

> *I am into phishing and the use of social network to get my maga. What I do mainly is to pretend as an imposter via online dating. I looked for the profile of people that is male and female that lives outside the country. I always posed to them as a single female looking for a male partner or as big man who needed a wife or tell them stories on how my wife disappointed me and took away my property and children or as a widower. All this is polished in a pitiable way with some pictures to even convince them whenever I'm chatting with them. From there I begin to play my pranks.*

Another cyber criminal when asked on the type of cyber crime he indulges in states that basically, am into software piracy and hacking.

> *We can therefore conclude that credit card fraud, hacking, software piracy, phishing and the use of social network are the major types of cyber crime that are common and being perpetrated in Zaria.*

Social Attributes of Cyber Criminals

In this section, attributes of cyber criminals such as age, sex, religion, educational status, marital status etc. will be discussed.

Table10: Views of Respondents on the Social Attributes of Cyber Criminals

Views	Frequency	Percentage
Age		
18 – 30	351	87.7
31 – 40	44	11.0
41 and above	5	1.3
Total	400	100.0
Sex		
Male	355	88.7
Female	19	4.7
Both	26	6.5
Total	400	100.0
Religion		
Islam	65	16.3
Christianity	117	29.3
Traditional	40	10.0
Any Religion	178	44.4
Total	400	100.0
Educational Qualification		
Primary education	13	3.3
NCE	17	4.3
Polytechnic	49	12.3
University	239	59.7
Others (computer education, masterdegree)	82	20.5
Total	400	100.0
Marital status of parent		
Married	242	60.5
Divorced	79	19.7
Widowed	22	5.5
Undecided	57	14.3
Total	400	100.0

The data in table 10 shows respondents' perception on the social attributes of cyber criminal. It was found that majority (88%) of the respondents were of the view that those individuals who are involved in cyber-crime are within the ages of 18-30 years.

Findings from the qualitative data corroborated with the above result on the age of cyber criminals as all key informants interviewed agreed that cyber criminals are mostly teenagers. For example, a lecturer said that:

> *Cyber criminal are mostly youths between the ages of 20-35 years. This may be due to the early exposure of the young ones to the activities on the internet without proper guidance. I think that is the reason why cyber crime is more among that age bracket.*

As regards sex of cyber criminals, it was discovered that male youths (89%) are more involved in cyber crime. Findings from in-depth interview also agreed to the data from the table. For instance, an operator of cyber cafe had this to say:

> *I will say 99% of cyber criminal are guys. A lot of guys are involved in this act. Though I once came across a very powerful computer programmer and she was a lady. If she decides to use her knowledge negatively, she will be a good cyber criminal.*

The table also revealed the educational background of cyber criminals. It was found that majority (60%) of the youths who engage in cyber crime are university students. However, key informants in in-depth interview did not agree to the statistics obtained regarding the educational qualification of cyber criminals.

For instance, an operator of cyber cafe states that:

> *You don't need to have a university degree before you can commit cyber crime. In fact cyber crime is not committed by dull people. You must be intelligent and smart and most youths that are involve in this are found in any kind of tertiary institution we have in Nigeria.*

Similarly, a lecturer corroborated the above statement that:

> *Cyber criminals can be in any tertiary institution, they could as well be in secondary school depending on the individual exposure to the technology. What I believe is that cyber criminals are not only smart people who have the skill to manipulate and alter technology to fit their needs; they are also smart enough to understand the human element and manipulate human nature to fit their needs.*

From both quantitative and qualitative data, it can be deduced that cyber criminals can be in any of the tertiary institutions listed above. And must possess additional attributes such as smartness and intelligent in order to cheat and defraud innocent individuals. It can also be deduced that it is not easy for low level young individuals with low intelligence quotient to be involved in cyber crimes.

The data in table 10 shows respondents' perception on the social attributes of cyber criminal. It was found that majority (88%) of the respondents were of the view that those individuals who are involved in cyber-crime are within the ages of 18-30 years.

Findings from the qualitative data corroborated with the above result on the age of cyber criminals as all key informants interviewed agreed that cyber criminals are mostly teenagers. For example, a lecturer said that:

> *Cyber criminal are mostly youths between the ages of 20-35 years. This may be due to the early exposure of the young ones to the activities on the internet without proper guidance. I think that is the reason why cyber crime is more among that age bracket.*

From the table as regards sex of cyber criminals, it was discovered that the male youths (89%) are more involved in cyber crime. Findings from in-depth interview also agreed to the data from the table. For instance, an operator of cyber cafe had this to say:

> *I will say 99% of cyber criminal are guys. A lot of guys are involved in this act. Though I once came across a very powerful computer programmer and she was a lady. If she decides to use her knowledge negatively, she will be a good cyber criminal.*

The table also revealed the educational background of cyber criminals. It was found that majority (60%) of the youths who engage in cyber crime are university students. However, key informants in in-depth interview did not agree to the statistics obtained regarding the educational qualification of cyber criminals. For instance, an operator of cyber cafe states that:

> *You don't need to have a university degree before you can commit cyber crime. In fact cyber crime is not committed by dull people. You must be intelligent and smart and most youths that are involve in this are found in any kind of tertiary institution we have in Nigeria.*

Similarly, a lecturer corroborated the above statement that:

> *Cyber criminals can be in any tertiary institution, they could as well be in secondary school depending on the individual exposure to the technology. What I believe is that cyber criminals are not only smart people who have the skill to manipulate and alter technology to fit their needs; they are also smart enough to understand the human element and manipulate human nature to fit their needs.*

From both quantitative and qualitative data, it can be deduced that cyber criminals can be in any of the tertiary institutions listed above. And must possess additional attributes such as smartness and intelligent in order to cheat and defraud innocent individuals. It can also be deduced that it is not easy for low level young individuals with low intelligence quotient to be involved in cyber crimes.

Table 11: Views of Respondents on the Life Style of Cyber Criminals

Life Style	Yes	No	Total
Always on the net	373 (93.3%)	27 (6.7%)	400 (100%)
Spend money lavishly	344 (86.0%)	56 (14.0%)	400 (100%)
Riding the best automobiles	326(81.5%)	74 (18.5%)	400 (100%)
Mainly clubbers	276 (69.0%)	124 (31.0%)	400 (100%)
Date the most beautiful ladies	269 (67.3%)	131 (32.7%)	400 (100%)
Live like kings in the society	252 (63.0%)	148 (37.0%)	400 (100%)
Hang out in upscale pubs	211 (52.7%)	189 (47.3%)	400 (100%)
Indulged in ritual activities	168 (42.0%)	232 (58.0%)	400 (100%)

The result shows that majority of the respondents are of the view that cyber criminals are always on the net (93%) and spend money lavishly (86%), while (53%) and (42%) of the respondents were of the view that cyber criminals hang out in upscale pubs and indulged in ritual activities respectively.

In support of the above life style of cyber criminals, a lecturer stated that:

> *Some of them when they hit big, they do good thing for themselves and their parent. They ride good cars, dress flashy, always attending clubs. Those I knew then in the university were using good cars. Then Toyota Camry and this baby boy were expensive not now that it is pure water.*

In addition, a cyber criminal when asked what he does with the proceeds of the money he receives from the criminal act stated that:

> *What I do mainly with the money I get from the sales of the software I get from the internet is to assist myself in school, have more money to subscribe for airtime and I also spend for my siblings and girlfriends.*

When further asked if he indulge in ritual activities, he states that:

> *I don't do such, however, I know that some of us do such by consulting spiritualists and herbalists in order to continue to be successful and also to assist them charm their victims in order to dance to their tune.*

From the above, it can be inferred that cyber criminals have a flamboyant life style that is quite different from other individuals in the study.

Causes of Cyber Crime

In this section, an attempt was made to identify the causes and motivating factors that are responsible for the involvement of individuals in cyber crime. Respondents were asked to state the motivating factors while the causes of cyber crime was broadly given and respondents were asked to rate them based on a scale given.

The motivating factors that encourages or drive individuals into cyber crime according to respondents varies and it is determined based on a number of different factors such as money/ financial gain, recognition/fame, low rate of conviction or even being caught, easy to perpetrate, intellectual pursuit, frustration, revenge, display of wealth by corrupt politicians and yahoo yahoo boys, laziness, un satisfaction from what they earn, lack of good moral upbringing from parents and guardians.

The qualitative data gave an explicit explanation of the motivating factors.

A lecturer stated that:

> *Someone may have grudges with an organization. A new organization can come and take away his market and you don't feel happy about it and you try to create something that will render that service that organization is producing ineffective. Take for example there are people that design program and anti virus to make money e.g. AVG and Avast. One of these companies could develop virus that the other company anti-virus software won't be capable of handling and tend to make that antivirus ineffective. Then another motivating factor is the tremendous success rate of the Yahoo Boys from their illegal act and not been caught by the law enforcement agencies, this will only serves to encourage others. Other motivating factors include excitement to succeed, get-rich syndrome, vengeance and sometimes sabotage.*

Furthermore, an operator of cyber cafe said that:

> *The motivating factors varies, but I think that inadequate legislation, financial benefits, low costs of executing the crime, low probability of being caught and prosecuted (due to weak laws and enforcement mechanisms) and the level of stigmatization of cyber criminals has not been so great.*

One of the cyber criminal when asked what motivated him into such criminal act states that:

> *You have seen our Nigerian politicians, you see the way they celebrate wealth, and this serves as a motivator for my involvement and other youths in cyber crime. The Nigerian society celebrates wealth without questioning the source of the money. Politicians caught defrauding the state become members of committees of the state and are given national awards like what we just experienced recently. In churches and mosques, corrupt individuals are invited to launch building projects and hold esteemed positions so why won't I find a way to survive from the economic hardship so that they can also call my name.*

Another cyber criminal aired his view on why he indulged in cyber crime as follows:

> *The main reason is those software which I love to use are mostly expensive and I do not have the resources to cope with buying the original software. Instead I attempt to hack the software so that I can use it at my own discretion and even sell it too to make some money. Then in our peer group, we use it as a form of getting reputation for example, if one successfully cracks software you gain some respect from our friends.*

From the above, it can be deduced that the quest for quick luxurious comfort, easy to perpetrate, low chance of cyber criminals being caught and even lower chances of been convicted by law enforcement agencies, vengeance, sabotage, reinforcement of criminal behaviour by family members, lack of resources to purchase original software, gain reputation among peer groups, pleasure and inadequate legislation are the motivating factors for the engagement of individuals in cyber crime.

Table 12: Views of Respondents on the Causes of Cyber Crime

Views	Agreed	Undecided	Disagreed	Total
Unemployment	375 (93.7%)	15 (3.7%)	10 (2.5%)	400 (100%)
Poverty	346 (86.5%)	20 (5.0%)	34 (8.5%)	400 (100%)
Peer group influence	345 (86.2%)	41 (10.2%)	14 (3.5%)	400 (100%)
Defective socialization	265 (66.2%)	89 (22.2%)	46 (11.5%)	400 (100%)
Weak laws	297 (74.2%)	38 (9.5%)	65 (16.2%)	400 (100%)
Corruption	364 (91.0%)	23 (5.7%)	13(3.2%)	400 (100%)
Easy accessibility to internet	302(75.5%)	30 (7.5%)	68 (17.0%)	400 (100%)

The table showed that virtually all respondents (94%) agreed that unemployment is a causal factor of cyber crime in Zaria. Also, 87%were of the view that poverty is a major cause while 86% of the respondents opined that peer group is the cause of cyber crime in Zaria. This view is in agreement with responses from the in-depth interview conducted.

Consequences of Cyber Crime

This section delved into the consequences of cyber crime. This includes loss of life, tarnishing the country's image internationally, loss of revenue etc.

Respondents were asked about the consequences of cyber crime.

Table 13: Views of Respondents on the Consequences of Cyber Crime

Views	Yes	No	Total
Tarnishing the country reputation	368(92.0%)	32 (8.0%)	400(100%)
Lack of trust and confidence hinders profitable transaction	360(90.0%)	40 (10.0%)	400(100%)
Denial of innocent Nigerians opportunity abroad	342(85.5%)	58 (14.5%)	400(100%)
Inimical to the progress &development in the country	275(68.7%)	125 (31.3%)	400(100%)
Loss of employment	231(57.7%)	169 (42.3%)	400(100%)
Loss of life	230(57.5%)	170 (42.5%)	400(100%)
Loss of revenue	221(55.3%)	179 (44.7%)	400(100%)

The above table shows the negative consequences of cyber crime to the society. It was found that 92% of the respondents are of the view that cyber crime will tarnish the country's reputation internationally. Lack of trust and confidence which is currently hindering profitable transaction was also examined as 90% of the respondents agreed to this.

The in-depth interview conducted reveals other negative consequences of cyber crime. A lecturer stated that:

> *Cyber crime creates a bad image for Nigeria and this have earned Nigeria her present ranking/rating in Transparency International where Nigeria is been listed as one of the most corrupt nation in the world. Another consequence of cyber crime is that it will drive away investors because due to the fact that most things are done electronically and if someone can attack your data base, then he has everything about you at his disposal.*

One of the operators of cyber cafe interviewed also states that:

> *Cyber crime has negative consequence. Take for instance, if a white man comes to Nigeria to survey in order to invest and discovered or he is receiving fraudulent mail from different people, he won't invest in the country again.*

Nevertheless, a cyber criminal interviewed had this to say on the consequences of cyber crime.

> *For sure cyber crime has negative consequence. What bad thing that does not have negative effect on the country? Cyber crime threatens foreign investment as well as misrepresents the country among other nations as corrupt. It will also lead to stigmatization of business men and women and they will face certain barriers when carrying out legitimate businesses.*

However, a cyber criminal was of the view that cyber crime plays a dual role in the society when asked about the consequences of the crime. He state as follows:

> *Yes it has negative consequences and among it is that it drive away investors. But not minding the negative consequences it has on the country, it is a way of getting connected and being rated well in the family, school and society, that is if you succeed. It is also a way for survival due to the high rate of youth unemployment and high poverty rate in the country. Take for example now, the money I get from the sales of soft ware I downloaded free from the net. I use it to take care of my needs. These days, when you graduate, you will not find a job even after you had spent so much to obtain a good certificate.*

Conclusion

Taking cognisance of the nature and effects of cyber crime, there will always be new and unexpected challenges to stay ahead of cyber criminals and cyber terrorists, but we can only do this successfully through partnership and collaboration of both individuals and government. There is much we can do to ensure a safe, secure and trust worth computing environment. It is crucial not only to our national sense of wellbeing, but also, to our national security and economic. The remarkable development in human history through computer technology has no doubt brought transformation in all aspects of life, especially in communication and information technology. Nevertheless, the embracement of the internet has come with a lot of mixed feelings despite its numerous advantages to the people of Zaria. In Nigeria, people are valued in terms of what they possess and command economically. Conversely, those without economic success are undervalued and the pressure to achieve success is intensified despite the harsh economic condition such as unemployment amongst others. This necessitated the ability of individuals to devise survival strategies and attain economic success by indulging in cyber crime. The perpetrators of cyber crime are not far- fetched, they are our brothers, friends, colleague, distant relatives and neighbours who can be tamed under appropriate circumstances with the right and positive communication, orientation, education and empowerment.

Recommendations

Education is the most vital weapon for literacy, as such seminars and workshops should be organized from time to time with emphasis on cyber safety so that the individuals will learn to keep their personal information safe and youth will flee cybercrime.

The findings from the study shows that youths involved in cyber crime are either in tertiary institutions or have graduated from tertiary institution. The study therefore, recommends that curriculum which will include courses on cyber crime, cyber management and its prevention should be introduced to both tertiary and secondary schools to take care of the present social changes.

The study discovered that there is no legislation on cyber crime. It is recommended that the government should immediately enact a comprehensive law on cyber crime. In order for legislation on cyber crime to be effective and efficient when enacted, there is need for government to empower graduates by providing employment.

Government should make provision for intensive training of law enforcement agencies on ICT so that they can track down the cyber criminals no matter how intelligent and cunning they may be.

For government agencies, law enforcement agencies, intelligence agencies and security agencies to fight curb cyber crime, it is recommended that there is need for them to understand both the technology and the individuals who engaged in this criminal act.

The findings showed that cyber criminals lives in the society, as such, prevention of cyber crime requires the co-operation of all the citizens and not the law enforcement agencies alone. It is therefore, recommended that everyone should watch and report to law enforcement agencies, anyone who indulge in cyber crime.

Cyber criminals caught are been prosecuted by government. It is recommended that cyber criminals' assets should also be confisticated by the government and the imposition of longer prison terms for cyber criminals. This will serve as deterrence to those youths who want to indulge in such crime.

The innocent internet users should inculcate the habit of continuously updating their knowledge about the ever changing nature of ICTs, through this, they can not only be well informed about the current trends in cyber crimes, but they will also have the knowledge about different forms of the said crimes and how the cyber criminals carry out their heinous activities, thus they can devise means of protecting their information from cyber criminals. Internet users should be security conscious.

Similarly, internet users should not provide personal or financial information to others unless there is a legitimate and assumed reason for that. They should not for instance, throw out papers works like cheques, bank and brokerage statements, old credit cards, drivers license, passports, receipts from ATM among other numerous documents which usually have personal data.

The internet services providers should not just provide broadband connection to their subscribers especially the home users, but they should also monitor effectively what the subscribers are doing on the net, at what time and where. They should provide their customers, especially financial institutions and cyber cafes with well-guided security codes and packages in order to protect their information and soft ware from hackers and publishers.

References

Agba,P.C. (2002), International Communication Principles, Concepts and Issues. In Okunna,C.S. (ed) Techniques of Mass Communication: A Multi-dimentional Approach. Enugu: New Generation Books.

Akogwu, S. (2012),An Assessment of the Level of Awareness on Cyber Crime among Internet Users in Ahmadu Bello University, Zaria (Unpublished B.Sc project). Department of Sociology, Ahmadu Bello University, Zaria.

Awe, J. (2009), Fighting Cyber Crime in Nigeria. http://www.jidaw.com/itsolutions/security3.html.

Ayantokun, O. (2006), Fighting Cyber crime in Nigeria: Information-system.www.tribune.com

Ehimen, O.R. and Bola, A,(2010), Cybercrime in Nigeria. *Business Intelligence Journal, January 2010, Vol.3.No.1*.

Federal College of Education Zaria Students Handbook (Revised 1999).

History of Ahmadu Bello University, Zaria. www.abu.edu.ng/about/history.php-cached.

History of Kaduna State. http://en.wikipedia.org/wiki/kaduna_state

History of Nuhu Bamalli Polythechnic. www.nuba.ng.org

History of Zaria.http://en.wikipedia.org/wiki/zaria

Imhof (2010), Cybercrime and Telecommunication Law. Rochester Institute Of Technology USA.

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

Global Information. www.mcconnellinformation.com. mcconnellinternational L.L.C

Mc Connell (2000), Cyber crime and Punishment. Archaic Law Threaten.

Olaide and Adewole (2004), Cyber Crime Embarrassing for Victims. Retrieved September 2011 from http//www.heraldsun.com.au

Olugbodi, K. (2010), Fighting Cyber Crime in Nigeria. Retrieved September 10, 2011 from http//www.guide2nigeria,com/news_articles_About_ Nigeria

Oyewole and Obeta (2002), An Introduction to Cyber Crime. Retrieved September 2011 from http//www.crime-research.org/articules/cyber-crime.

Ribadu, E. (2007), Cyber Crime and Commercial Fraud; A Nigerian Perspective. A paper presented at the Modern Law for Global Commerce, Vienna 9^{th} – 12^{th} July.

Sesan, G. (2010), The New Security War. http://www.pcworld.com/article/122492/the_new_security_war.htm#tk.mod-rel.

Shinder, D.L.(2002), Scene of the Cyber crime: Computer Forensics Handbook. Syngress Publishing Inc. 88 Hingham Street, USA.

Sutherland, E.(1939), Principles of Criminology. Fourth edition.

Vladimir, G.(2005), International Cooperation in Fighting Cyber Crime.www.crimeresearch.org

Zero Tolerance (2006), Retiree in Trouble over Internet Fraud. *Economic andFinancial Crime Commission, Vol. 1, No. 2*