EXPLORATION OF THE TYPES AND SOCIO-DEMOGRAPHIC FACTORS INFLUENCING THE SCOURGE OF CYBERCRIME AMONG YOUTHS IN WUSE, ABUJA FCT, NIGERIA

[1]Oluwafemi Amos IDOWU, [2]Francis, UROKO & [3]Mzungwega, AGBIR
[1, 2] Department of Sociology, Nigeria Police Academy, Wudil Kano State, Nigeria
[3]Office of the Registrar, Nigeria Police Academy, Wudil Kano State, Nigeria
Correspondence Email: idowuoluwafemiamos@yahoo.com

ABSTRACT

Cybercrime is a technological crime and global phenomenon prevalent among the youth, and with a lot of adverse implications. It is on this premise that this study explores the types and socio-demographic factors influencing the scourge of cybercrime among the youths in Wuse in Abuja (FCT), Nigeria. Several literatures pertinent to the study were reviewed. This explanatory study employed quantitative (survey with the use of questionnaire) method to source for raw data from 150 respondents from Wuse, Abuja FCT, Nigeria. The study revealed that major perpetrators of cybercrime are young male, unemployed people and students, with the use of laptops and advanced android/hi-phones. The study concluded that there are multi-faceted factors causing cybercrime in Nigeria. These are unemployment, quest for quick wealth, corrupt society and criminal minded of the youths. The study recommended that the Nigeria government should ensure adequate public sensitization against the menace of cybercrime in Nigeria; and that government and private sectors should provide job opportunities for the youths. The government should enact an effective law that gives comprehensive punishment for the culprits of cybercrime. Individual, parents and government should ensure personal security and safety on their cyber activities.

Keywords: Causes, Control, Cybercrime, Internet Crime, Youths.

INTRODUCTION

It is no longer news that Information and Communication Technology (ICT) systems are useful in all facets of human's daily activities as it is utilized virtually by everybody in the society including the government. ICT has become part and parcel of human's daily routine activities, and it is not only good for ease, efficiency and pleasure. Also, it is a necessity for innovation and economic growth. The world at large is becoming an information and global society in this the tech-driven age with exchange of information with speed. The world is currently experiencing a lot of social changes which are occasioned by technology. Technology has made communication very easy and fast through telephone (GSM), computer, internet, fax, e-mail and so on. These developments have their attendant problems: cybercrime. Thus, while advancement in technology provides opportunities and benefits, it has also increased vulnerability to crime.

Cybercrime happens in the world of computer and internet. It involves action(s) directed against the confidentiality and integrity of computer systems' networks and data among others. The 21st century hi-tech world and the use of computer networks have given rise to the crime rate in Nigeria and beyond. Cybercrimes are global in nature and the nations of the world cannot easily close their borders to incoming cyber threats. Time and geography, as well as the location of the victims, are no longer barriers to where and when these attacks are launched by the cyber criminals. Hence, Paranjape (2010) posits that cybercrime differs from most terrestrial crimes because of the ease with which one can learn how to commit cybercrime: it requires little resources and it can be committed in a jurisdiction without one being physically present there (Abdulkarim, 2012; Uroko, 2020). Cybercrime can be against persons or property and/or against government – society. The nature of cybercrime prevalence in Nigeria are numerous and it includes: hacking, software piracy, credit card or ATM fraud, identity theft, service attack, virus dissemination, phishing, cyber plagiarism, cyber stalking, cyber terrorism, virus attacks, cyber stalking, marriage scam, cyber-contraband, spam, telecoms fraud, cyber trespass, cracking of satellite or TV decoding devices, selling of fake security software via the net (scare ware), using of web to spread lies (hate speech), hoaxes and urban myths and so on. The Federal Capital Territory (FCT) Abuja in particular and Nigeria in general is not isolated from the negative influence of the modern technology. FCT is an urban centre due to its population size and infrastructure and these attract many outlets because of modern technology. These outlets include: cybercafés, internet service outlets, telecom service outlet and so on.

The phenomenon of cybercrime is a contemporary global problem and it cannot be comprehended without exploring its prevalence and causes among the youths, particularly in Nigeria. The incidence of the phenomenon of cybercrime is not only high, but also increasing at an alarming rate, with its consequent adverse effects. It threatens the national sustainable development, tarnishes the image of the country, and creates a lot of mistrust and mutual suspicion to the citizenry. Despite that, there is a dearth of information on this looming problem. Hence, this study took a broad and eagle view on the phenomenon of cybercrime among youths in Nigeria. It is hoped that the findings of the study would help to give pro-active strategies and recommendations to control cybercrime in Nigeria. Therefore, it is on this premise that this study was designed to explore the types and socio-demographic factors influencing the scourge of cybercrime among the youths in

Wuse, Abuja Nigeria, as the core of Nigeria in term of Federal Capital Territory.

Objectives of the Study

The aim of this study is to explore the phenomenon of cybercrime among youths in Wuse, Abuja Nigeria; while the specific objectives include to:

i. examine the prevalence of cybercrime among youths in Nigeria; and,
ii. explore the types and socio-demographic factors influencing cybercrime among youths in Nigeria.

Cybercrime and Modern Technology

Cybercrime has been defined differently by various scholars, depending on their perspectives. The definition of cybercrime is contextual in nature. However, cybercrime can be defined as breaking into computers to steal or destroy information, or vandalize a computer source code, hacking, illegal publication of electronic information, breach of confidentiality online, publishing of false digital signatures, or illegal interference (system/data), illegal access, and the misuse of device for fraudulence act digitally. Thus, cybercrime involves the intrusions to private and company's online information, network and integrity violations, industrial digital espionage, pirating computer software and other nature of crimes in the cyber where computer is a major factor in committing the offence. However, cybercrime is the act of breaching information security illegally. Paranjape (2010) conceives cybercrime as any criminal activities where computer and/or networks are the main source, tool, or place of perpetrating such crime. This encompasses the network such as phones, telephone networks, fax networks, Very Small Aperture Transmission (VSAT) networks and other ICT equipment. Thus, cybercrime is information and communication related crime.

Cybercrime according to Adesina (2017) can be defined as the crimes committed on the internet using the computer as either as tool or a targeted victim. It encourages illegal activities being perpetrated by one or more people referred to as scammers, hackers, internet fraudsters, cyber citizens or 419ners, yahoo-yahoo guys, yahoo-plus and so on. Azeez and Osunade (2009) posit that cybercrime is any harmful act committed from or against a computer and/or network. Cybercrime is not the same with the most common crimes in the following ways:

i. Cybercrime is easy to learn how and to commit.
ii. It requires few resources compare to the potential damages it can cause.
iii. Cybercrime can be committed in a jurisdiction without being physically present.
iv. The acts are often not clearly illegal, but the end result is illegal.
v. It can be committed by anybody above certain reasonable age (Paranjape, 2010).

Azeez and Osunade (2009) posit that cybercrime (computer crime) is any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them. Cybercrime deals with shattering of computer data or networks through interception, interference or destruction of such systems. It involves committing crime against computer systems or the use of the computer in committing crimes (Uroko, 2020). Just as technology helps in the investigation of crime, it also breeds crime. The frequent cases of advance free fraud, counterfeiting, money laundering, cyber-terriorism and so on involve taking advantage of modern technology particularly "Information and Communication Technology" (Dambazau, 2007; Abdulkarim, 2012).

Abdulkarim (2012) stressed that the subsequent use of technology by Nigerian banks and others in conducting business and transaction exposes people to new ways of crime i.e. "cybercrime". Furthermore, the use of modern technology has removed geographical barriers to crime, maximized anonymity, enhanced the ability of offenders to avoid detection. With modern technology, digital thieves now operate outside the traditional parameters and now take advantage of the technology in launching themselves into new geographic areas. The idea of geographical impediment which is no longer a threat to cybercriminals poses other emerging problems such as the threat of national boundaries, challenges to national government, law enforcement agents, and the need for harmonized cyber laws. James (1993) believes that cybercrimes has been around since the invention of abacus when people use the device for wrong purpose while Tittel (2002) asserts that it is safe to associate the origin of the crime with the emergence of the first computer network.

Cybercrime is contemporarily posing serious threats to society even when organizations engage robust security technology like firewall, antivirus software, intrusion detection tools, authentication services and others, cybercrime keeps spreading. The crime is no longer confined to traditional juvenile hackers (novices or script kiddies as they are sometime called), as professional criminals are now exploiting the network for profit. Computers or communication systems are not immune to cybercrimes as any and every system in the world can be hacked by cybercriminals (Babu & Parishat, 2004; Siebel and House, 1999 and Wall, 2007). For Siegel (2004), "the cybercrime is a new breed of white-collar offences". According to Wall (2007) cited in Uroko (2020), based on victim perspective, cybercrimes are broadly categorized into three, namely: crime against individual person, against property, and against the government.

There are several forms of cybercrimes which sectorally grouped as: banking sector, e-commerce sector, educational sector, telecommunication sector, socio-media sector, and others. However, cybercrime can be generally typified as: Bank Verification Number (BVN) scam, cyber-theft/banking fraud, unauthorized access to hosts (hacking), online-identity theft (phishing), theft of bank cards, credit card fraud, Automated Teller Machine (ATM) scam, cyber plagiarism, software piracy (intellectual property theft), sales fraud and forgery, Data and Airtime Time (DAT) theft from service providers, password sniffing, malware, cyber-stalking, spam, scam mails, wire-tapping/illegal interception of telecommunication, mobile phone virus and cybercrime, delivering victors of mobile virus, copycat website, charity funds scam, social-hi-jacking, cyber terrorism, logic bombs, marriage scam, cyber-contraband, pedophiles, cyber trespass, cracking of satellite or TV decoding devices, selling of fake security software via the net (scare ware), using of web to spread lies (hate speech), hoaxes and urban myths, and so on.

Causes of Cybercrime among Youths in Nigeria

Several factors can be adduced to the causes of cybercrime amongst youths in Nigeria according scholars, which include the followings:

Radda (2005), in his position paper entitled "the role of corruption in the emergence of cybercrime", links the preponderance of cybercrime to high level prevalence of corruption. In expanding this idea further, Ayantokun (2006) opines that cybercrime cannot be divorced from the prevalence of high level of corruption cum wide spread of poverty and unemployment. Ribadu (2007) observed that the perpetrators are majorly the youths and thousands of them are unemployed, but highly knowledgeable in computer. Furthermore in West Africa, three main factors account for and aid the spread cybercrime, viz:

* The free ECOWAS travel protocol.
* The development of information and communications technology infrastructure and,
* Non-liable cybercrime laws coupled with poor attitudes towards cyber fraud, because it is apparently preyed on foreign victims.

Other factors responsible for the prevalence of cybercrime among Nigerian youths include: dearth of trained workforce to control the menace, urbanization, quest for quick wealth syndrome, poor socialization system, poor implementation of cybercrime laws, incompetent security on personal computer/devices, unemployment, global economic realities, peer group pressure, neuroticism traits among the youths, adventure to experimentation, among others. However, Nigerian governments have made several attempts/efforts to curb the menace of cybercrime in Nigeria by enacting cybercrime laws and other criminal laws, such as: creation of Nigeria Cybercrime Working Group (2004), Economic and Financial Crimes Commission Act (2004), Advanced Fee Fraud and other related Offences Act (2006), establishment of Directorate of Cyber-security (DFC) in (2007), Cybercrime Act (2015), and so on. These and others reviewed some issues and techniques involved in security network activities in Nigeria. Despite all the efforts, there are challenges militating against the control of cybercrime in Nigeria. This include biased cybercrime laws, lack of legal framework, problem of legal validity of electronic data and admissibility of electronic documents in the law court, extradition problem (interpol), lack of investigative power and mechanism, lack of synergy between individuals, corporate organizations and government, lack of international cooperation, non-proactive response to cybercrime and so on.

THEORETICAL EXPLANATIONS

There are a lot of theories that explain cybercrime. In this study, Social structure and Anomie theory as well as Routine Activities Theory were employed as the bases of explanation of the factors influencing cybercrime among the youths in Nigeria.

Social Structure and Anomie Theory

Social structure and anomie theory was propounded by Merton (1951) with its root in the theory of anomie by Emile Durkheim (1933) and the theoretical tradition of functionalism. The term anomie as used by Durkheim has its origin in the Greek word “anomos” meaning (normlessness). According to Durkheim (1933) cited in Siegel (2004), an anomie society is the one in which rules of behaviour (norm) are being broken down due to rapid social change, social crisis, or a transition from pre-industrial social system to industrial or urbanized social system (Dambazau, 1999; Abdulkarim, 2012).

Durkheim further argues that deviant behaviour, and by implication cybercrime tendencies, is a product of social structure. He further establishes how socio-cultural structure of society puts pressure on people in committing crime. In line with the above inspiration, Merton (1957) posits that anomie occurs in a situation when the social structure of a society is over-emphasized upon its cultural goals at the expense of institutional means thereby creating an anomie tendencies and by extension the proliferation of various crimes. Thus, cybercrime occurs as people try to adapt to various means in achieving societal cultural goals. Merton (1957) cited in Siegel (2004) though using an American society as his point of departure, argues that society shares cultural values such as success measured by wealth and material possession. However, some societies have institutionalized means of achieving success through educational qualification, talents, hard work and so on. Merton (1957) further posits that, in a balanced society, there is equal emphasis both cultural goals and institutional means (Abdulkarim, 2012).

In an anomic society, great importance is given to success with little or scarce means of achieving the success. According to Merton, in this kind of society, there is tendency for people to reject the rules of the game and strive for success by any available means. Merton asserted that people respond to forgone situation in the following five adaptation modes, which explain crime in general and by implication cybercrime:

- ❖ The *conformist:* These are people who conform to the cultural goals of success and the institutional means. These people follow the legitimate means to success in life.
- ❖ *Innovation*: These people are those who reject normative means of achieving success hence their ways are blocked as a result of scarce legitimate means to success. Thus, they innovate by turning to deviance such as cybercrime, unemployed graduates who turn to armed robbery which promises greater and quick reward.
- ❖ *Ritualism*: In Merton sense, these are people who accept societal means, but did not strive to achieve the cultural goals of success as demanded by the society. Thus, a typical low-grade civil servant or school teacher is an example in this category.
- ❖ *Retreatism*: These are people who reject the cultural goals and also reject the institutional means of society, even when they internalized the duo. According to Merton, the retreatists resolve their conflict situation by given to drugs, alcohol and so on, and these category of people are mostly outcast, psychotics, vagrants and so on.
- ❖ *Rebellion*: These are the people who reject both cultural goals of success and institutional means of success, and seek to replace them with different alternatives. Those that fall under this category are protesters, cyber terrorists and revolutionaries.

According to social structure theory, most criminals are found within the innovation, retreatism, and rebellion adaption modes. Thus by implication, cybercriminals in line with this theory can safely be located in the innovative adaption mode (Abdulkarim, 2012).

Routine Activities Theory (RAT)

The routine activities theory is one of the victimization theories. The theory looks at the role of victims in crime process and the causes of victimization. Routine activities theory explained that cybercrime occurs because there is availability of suitable targets, absence of capable guardians, and there is presence of motivated offenders. The theory according to Siegel (2004) shows how a victim’s behaviour can influence criminal opportunity and victimization risk can be mitigated against by increasing guardianship and reduction of the target vulnerability. Cohen and Felon (1979) in Siegel (2004) conclude that, the volume and distribution of crime are closely related to interaction of the three variables viz:

i. Availability of *suitable targets*, like a home stalked with fast-sales goods, careless person, house without a door, computer without security PIN and so on.
ii. *Absence of capable guardians* as: police, home owners, neighbours, friends and relative.
iii. *Presence of motivated offenders*, for example a large number of unemployed youths, teenagers, males, drug users, provocative behaviour and so on.

The presence of these components increases the propensity of a cybercrime to occur. The theory also holds that crime targets are more likely to be victimized, if they engage in risky behaviour or are poorly guarded and/or are exposed to a large group of motivated offenders, such as delinquents, unemployed youths and drug addict population. The theory believes that if the above set of people congregates in a particular neighbourhood, the place becomes a “hot spot” for crime and violence target. Hence, young guys in many Nigerian tertiary institutions appear to congregate in school as a hub to perpetuate cybercrimes. Likewise, some young guys graduates who are not adequately economically engaged have the tendency to engage in criminal activities particularly cybercrime as it requires knowledge in computer and others.

In referring to guardianship as factor in crime, routine activity theory posits that guardianship is more effective as deterrence, if it comes particularly from conventional peers who are well socialized. The theory according to Siegel (2004) further stresses that peer reaction and condemnation may be a form of moral guardianship that can deter any motivated offenders from engaging in criminal behaviour. The theory also maintains that crimes and by implication cybercrime occurs due to the presence of motivated offenders, availability of suitable targets and absence of capable guardian. It further reiterates that cybercrime victimization risks can be reduced by increasing guardianship and/or reducing target’s vulnerability. The theory according to Schaefer (2005) is of the opinion that cybercrimes are more likely to occur whenever offenders or cybercriminals meet vulnerable targets such as unsecure systems or networks, systems that are not passworded, email message or chat forum that are not encrypted and so on.

In summary, routine activities theory potentially assumes that often cybercrime occurs, if an offender thinks that a target is suitable and there is a capable guidance to be absent. It is the absence of a capable guidance that determines whether a crime will occur or not. In addition, the theory is bounded up that a person’s living arrangement could affects his/her victim’s risk. Likewise, the people who are living in unguarded areas are at the mercy of motivated offenders. Life style of people on the other hand, affects the opportunity for crime, because of his/her exposure to cyber-criminals, and attractiveness as a target of crime to the potential offender.

METHODS

This study employed mixed method of research by triangulating both descriptive (survey) and explanatory research design methods. This method is engaged due to the nature of the study and the designs serve as complementary to each other in order to explore the factors influencing cybercrime among the youths in Nigeria. It helps to get comprehensive, valid and reliable data from the respondents. The study employed questionnaires (survey) for data collection. The primary target population for this study comprised the youths and the public in Wuse Abuja (FCT) Nigeria, both male and female. Wuse Abuja (FCT) is a place with heterogeneous population since it is the hub capital city of Federal Republic of Nigeria. Most of the cyber criminals (youths) usually want to live expensive lifestyles in Abuja and to be in a more secured place like Abuja.

The target populations were chosen because they met the purpose of the study as they have the needed information about the issues of cybercrime among youths and its causes in Nigeria. Multi-stage sampling techniques were employed to select the sample in stages for this study. Wuse district in Abuja FCT is made up of eight (8) zones. Thus, Wuse is geographically stratified into 8 zones. Systematic sampling technique, random sampling and purposive sampling techniques were employed to select the respondents. The study employed quantitative method of data collection with the aid of questionnaire. 150 respondents were involved in the study in the administration of the questionnaires.

The secondary data were sourced through ancillary instruments like literature searches and other available records and documents. The data collected from the field were analyzed with quantitative methods of data analysis. Descriptive statistics was employed to summarize and interpret the data. In addition, univariate statistical tool was used for the data analysis. The univariate technique employed frequency distribution tables and percentages for descriptive purposes.

RESULTS

The data collected from the field were analyzed, interpreted and presented as follows:

Table 1: Socio-Demographic Characteristics of the Respondents

Characteristics	**Recidivists**	
Age	**Frequency**	**Percentage**
Below 16 Years	3	2.0
16 - 25 Years	27	18.0
26 - 35 Years	48	32.0
36 - 45 Years	57	38.0
46 - 55 Years	15	10.0
Total	**150**	**100%**
Sex		
Male	120	80.0
Female	30	20.0
Total	**150**	**100%**
Nationality		
Nigerian	148	98.7
Non-Nigerian	2	1.3
Total	**150**	**100%**
Educational Status		
Primary	9	6.0
Secondary	6	4.0
Undergraduate and Graduate	71	47.3
Postgraduate	64	42.7
Total	**150**	**100%**
Computer Education Status		
None	21	14.0
Certificate in computer	60	40.0
Diploma in computer	54	36.0
Degree(s) in computer science	6	4.0
P.G in Computer studies	9	6.0
Total	**150**	**100.0**
Occupation of Respondents		
Unemployed	62	41.3
Student	29	19.3

Public/Civil-servant	17	11.3
Private employment	16	10.7
Self-employed	13	8.7
No response	13	8.7
Total	**150**	**100.0**
Cybercrime Experience		
Yes	97	64.7
No	53	35.3
Total	**150**	**100.0**

Table 1 reveals that majority of the respondents in the study are between 16 – 45 years old. From the distribution, it can be gleaned that majority of the respondents fall within the youthful age. The male proportion of the respondents as represented were 80% while the females were represented by 20%. As indicated in Table 1, the male respondents are at the modal frequency. Also, the respondents' nationality indicated that a significant 98.7% were Nigerians; while 1.3% were non-Nigerians. This is logical because the study was conducted in Nigeria where majority are Nigerian citizens. In addition, the numbers of respondents who have undergraduate degrees were the majority with 47.3% of the total population. This is closely followed by 42.7% of the respondents who had postgraduate education; while those with primary education constituted 6%. The least among the respondents were those with SSCE having the total population of 4% of the respondents.

Furthermore, 40% of the respondents have certification in computer education, 36% have diploma in computer science, 14% have no computer education, 6% have postgraduate knowledge in computer studies; while 6% has degree in computer science. Apparent from the above distribution is that majority of the respondents have advanced education in computer studies which constituted 86% of the total population. This means that majority of the respondents are computer savvy and are therefore likely to be familiar with computer crimes and provide relevant data needed for this study. The table also reveals that unemployed people constitute the majority of the respondents with 41.3%, followed by students with 19.3%. Public/civil-servants constitute 11.3% of the total respondents. On the hierarchy, private employed staffs were 10.7%; while self-employed people were 8.7%. A significant number of the respondents (60%) have ever experienced cybercrime, while 40% have never experienced cybercrime. This reflects the prevalence of cybercrime in Nigeria, as observed by local and international reports.

Table 2: Types of Cybercrime experienced by Respondents

Types of Cybercrime Experienced	**Frequency & Percentage**		**Total (%)**
	Yes (%)	**No (%)**	
Denial of Service/Malware (Virus attack)	48 (32.0)	102 (68.0)	**150 (100)**
ATM Fraud	51 (34.0)	99 (66.0)	**150 (100)**
Hacking of account/e-mail/social medial	87 (58.0)	63 (42.0)	**150 (100)**
Receiving scam mails	96 (64.0)	54 (36.0)	**150 (100)**
Receiving of Unsolicited e-mails (Spam)	84 (56.0)	66 (44.0)	**150 (100)**
BVN scam	45 (30.0)	105 (70.0)	**150 (100)**
Phishing (Identity theft)	12 (8.0)	138 (92.0)	**150 (100)**

Theft of Bank Card(s)	35 (23.3)	115 (76.7)	**150 (100)**
Copy right theft/Software piracy (cyber plagiarism)	36 (24.0)	114 (76.0)	**150 (100)**
Password sniffing (Cracking)	36 (24.0)	114 (76.0)	**150 (100)**
Cyber stalking (Cyber harassment)	30 (20.0)	120 (80.0)	**150 (100)**
Pornography (Illegal display of sexual acts)	51 (34.0)	99 (66.0)	**150 (100)**
Charity funds scam (Fake charity accounts)	57 (38.0)	93 (62.0)	**150 (100)**
Data and Airtime theft	69 (46.0)	81 (54.0)	**150 (100)**
Sales promotion scam	58 (38.7)	92 (61.3)	**150 (100)**
Cyber-theft/Banking fraud	39 (26.0)	111 (74.0)	**150 (100)**
Cyber terrorism	15 (10.0)	135 (90.0)	**150 (100)**

Table 2 presents the types of crime experienced by respondents. The table reveals that receiving scam mails, hacking of account/e-mail/social medial and receiving of unsolicited e-mails (spam) are the top types of cybercrime experienced by respondents with 64%, 58% and 56% respectively. Other types of cybercrime commonly experienced include data and airtime theft, sales promotion scam, charity funds scam (fake charity accounts), and pornography (Illegal display of sexual acts) among others, but below average of the total population of the respondents.

Table 3: Major Perpetrators of Cybercrime

Major Perpetrators of Cybercrime	**Yes (%)**	**No (%)**	**Total (%)**
Male	141 (94)	9 (6)	150 (100)
Female	48 (32)	102 (68)	150 (100)
Young people	141 (94)	9 (6)	150 (100)
Old people	15 (10)	135 (90)	150 (100)
Students	99 (66)	51 (34)	150 (100)
Unemployed people	141 (94)	9 (6)	150 (100)
Government workers	33 (22)	117 (78)	150 (100)
Self-employed people	36 (24)	114 (76)	150 (100)

Table 3 shows the major perpetrators of cybercrime. Apparent from the above table is that majority agrees that people who fall under the category of young male, unemployed people and students are the major perpetrators of cybercrime with 94% each and 66% respectively. However, majority disagrees that old people, government workers, self-employee and females usually perpetrate cybercrime in Nigeria with 90%, 78%, 76%, 68% respectively. Literature has shown that males and young people are most likely to engage in cybercrime than the other categories because they possess certain traits that encourage cyber criminality. Unemployment, however, has been said to be a major cause of crime in the society.

Table 4: Major Facilities used for Cybercrime

Facility for cybercrime	**Yes (%)**	**No (%)**	**Total (%)**
Networked computers	99 (66)	51 (34)	**150 (100)**
Laptops	138 (92)	12 (8)	**150 (100)**
Cyber Café	84 (56)	66 (44)	**150 (100)**
Tablet Phones (Hi-Pads)	96 (64)	54 (36)	**150 (100)**
Telephones (Mobile)	114 (76)	36 (24)	**150 (100)**

Table 4 presents major facilities used for cybercrime where 92% of the total respondents agree that laptops are mainly used for cyber criminality, while 8% disagrees. 76% of the respondents agree that telephones (mobile) are majorly used, while the remaining 24% disagrees. Furthermore, 66% of the total respondents agree that networked computers are used, while 34% disagrees. Among the total respondents, 64% agrees that tablet/smart phones (hi-pads) can be are usually used, while 36% disagrees; and 56% of the respondents agree that cybercafé are used for committing the cybercrimes and 44% disagrees. This shows that respondents agree that all the facilities in the distribution can be used in perpetrating cybercrime in Nigeria. The advancement in technology has brought about advanced facilities which cyber offenders used in perpetrating different forms of crime. However, an important discovery from the distribution is that all the facilities are networked devices that can be used to reach people from different location.

Table 5: Major Causes of Cybercrime in Nigeria

Cause of Cybercrime in Nigeria	**Yes (%)**	**No (%)**	**Total (%)**
Corrupt society	122 (81.3)	28 (18.7)	**150 (100)**
Unemployment	141 (94.0)	9 (6.0)	**150 (100)**
High level of computer intelligence	54 (36.0)	96 (64.0)	**150 (100)**
Introduction of ICT.	63 (42.0)	87 (58.0)	**150 (100)**
Criminal minded of the youths	96 (64.0)	54 (36.0)	**150 (100)**
Youthful exuberance (Experimentation)	87 (58.0)	63 (42.0)	**150 (100)**
Urbanization	57 (38.0)	93 (62.0)	**150 (100)**
Quest for quick wealth syndrome.	132 (88.0)	18 (12.0)	**150 (100)**
Inadequate Equipped Cybercrime law	66 (44.0)	84 (56.0)	**150 (100)**
Weak implementation of cybercrime law	87 (58.0)	63 (42.0)	**150 (100)**
Incompetent Security on Personal Computers	81 (54.0)	69 (46.0)	**150 (100)**
Poor Cyber Security System in the country	93 (62.0)	57 (38.0)	**150 (100)**

Table 5 above reveals the main causes of cybercrime in Nigeria. 94% of the respondents agree that unemployment is one of the major causes of cybercrime in Nigeria, while 6% disagrees. 88% of the total respondents agree that quest for quick wealth syndrome causes cybercrime, while 12% disagrees. 81.3% agree that corrupt society causes cybercrime in Nigeria, while 18.7% of the respondents disagree. 64% of them agree that criminal mind in youth causes cybercrime, while 36% disagrees. However, majority of the respondents with 64% disagrees that high level of computer intelligence causes cybercrime, while 36% agrees. Furthermore, 62% of the total respondents in the study disagrees that urbanization causes cybercrime, while 38% disagrees. Also, 58% of them disagrees that introduction of ICT causes cybercrime, while 42% of the total respondents agree. 56% of the respondents in the study disagrees that inadequate equipped cybercrime law causes cybercrime in Nigeria, while 44% agrees among the respondents in the study.

DISCUSSION

This study identified that majority of the respondents in the study are within the ages of 16 – 45 years old, male, Nigerians, with above secondary school certificate holders, computer literate who are either students, unemployed, private or self-employed persons and who have experienced cybercrime and the types of cybercrime experienced mostly include: receiving scam mails, hacking of account/e-mail/social medial, receiving of unsolicited e-mails (spam), data and airtime theft, sales promotion scam, charity funds scam (fake charity accounts), and pornography (illegal display of sexual acts) among others. It was further discovered that the major perpetrators of cybercrime are male, unemployed, young people and students. Similarly, the facilities involved in the perpetration of cybercrime are laptops, telephones (mobile), networked computer, tablet phones (hi-pads), and cybercafé. On the causes of cybercrime, it was found out that unemployment among youths, quest for quick wealth syndrome, corrupt society and high proportion of criminally minded youths cause cybercrime among youths in Nigeria.

Conclusion

The study concluded that majority of the male secondary school leavers who are either undergraduates or drop-outs ranging from the ages of 16 to 45 years old appear to be the major perpetrators of cybercrimes. They are mostly computer literate, but unemployed youths or self-employed Nigerians who reside in Abuja hustling for their daily survival. They engage in series of cyber criminalities with the aid of laptops, mobile phones, networked computers, tablet phones (hi-pads or androids) and cyber cafes. This nefarious act appears to be caused by unemployment amongst the youths, culture and quest of quick money syndrome, corrupt society, high proportion of criminal minded youths in Nigeria. However, further studies should look into the ineffectiveness of the Nigeria cybercrime laws and the control of unemployment among the youths in order to control cybercrime in Nigeria.

Recommendations

Based on the findings above, recommendations were made such as:

i. Nigeria government need to pursue serious public sensitization against cybercrime through mass media and incorporation of personal cyber space security should be integrated in Nigeria education curriculum.

ii. Nigeria government needs to adequately equip the Economic and Financial Crime Commission (EFCC) personnel on intelligence, infrastructure and requisite technological knowledge needed. Education and human capacity development on cybercrime control should be strategically launched.

iii. Individuals need to observe personal safety rules such as not disclosing to strangers bank details such as credit card pins numbers, bank account numbers, bank verification number (BVN), e-mail address password, and use of antivirus on their systems against malware etcetera.

iv. There should be provision of jobs for young graduates, vocational skills and entrepreneurial development programmes. This will reduce the number of youths getting involved in cybercrime.

v. Government needs to enact comprehensive laws to punish offenders. The existing laws (Acts) and new laws (Acts) should be adequately implemented in Nigeria to reduce the incidence of cybercrime.

vi. Nigeria government need to train special cyber security experts; and aid the existing law enforcement agencies, intelligence agencies and cyber-security agencies to understand the modus operandi of the cybercrime offenders.

vii. Parents should use content filtering software on computers to protect children from cybercrime. This will reduce the cause of cyber criminality in Nigeria among the teenagers and youths.

viii. Computer networks should be well-protected; and the legal-political will should ensure the adequate enforcement of law in Nigeria.

REFERENCES

Abdulkarim, U. S. (2012). A study of cybercrime in Kano Metropolis. (unpublished M.Sc dissertation). Department of Sociology, Bayero University, Kano State, Nigeria.

Adesina, O. S. (2017). Cybercrime and poverty in Nigeria. *Canadian Social Science, 13*(4), 19 – 29.

Ayantokun, O. (2006). Fighting cybercrime in Nigeria. Information system. Retrieved September 10th 2011, from www.tribune.com.

Azeez, N. A., & Osunade, O. (2009). Towards ameliorating cybercrime and cyber security. *International Journal of Computer Science and Information Security, 3*(1), 1 – 11.

Babu, M., & Parishat, M. G. (2004). What is cybercrime? Retrieved August 27th 2013. http://www.crimeresearch.org/analytic/702/

Cohen, L. E., & Felon, M. (1979). Social crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588 – 608.

Dambazau, A. B. (1999). *Criminology and criminal justice*. Kaduna: Nigeria Defense Academy Press.

Dambazau, A. B. (2007). *Criminology and criminal justice*. Ibadan: Spectrum.

Ibrahim, M. (2017). Regulation of cybercrime in Nigeria: The youth saga. (unpublished M.Sc dissertation). Department of Sociology, Bayero University, Kano State, Nigeria.

James, A. (1993). *Introduction to information system*. 8th Edition. New York: Irwin McGraw Hill Publishing Company.

McConnel, B. W. (2000). *Cybercrime ... and punishment*? Archaic Laws Threaten Global Information. McConnel International LLC. December. www.mcconnellinternational.com

Merton, R. K. (1957). *Social theory and social structure*. New York: Free Press.

Neumann, P. (2004). *Computer related risks*. New York: ACM Press.

Paranjape, N. V. (2010). *Criminology and penology*. 14 Edition. Allahabad: Central Law Publications.

Radda, S. I. (2005). The role of corruption in the emergence of cybercrimes. *Bayero Journal of Accounting Research*, 1(2), May, 131 – 145.

Ribadu, E. (2007). Cybercrime and commercial fraud: A Nigerian perspective. A paper presented at the modern law for global commerce, Vienna 9th – 12th July.

Schaefer, R. T. (2005). *Sociology*. 9th Edition. USA: McGraw Hill Company.

Siebel, T. M., & House, P. (1999). *Cyber rules, strategies for excelling at e-business*. New York: Double Day Publishers.

Siegel, L. (2004). *Criminology: Theories, patterns and typologies*. California: Wadsworth.

Tittel, E. (2002). *From scene of the cybercrime: Computer forensics handbook*. USA: Syngrees.

Uroko, F. (2020). The scourge of cybercrime among youths in Wuse and its implications in Abuja, FCT Nigeria. (unpublished B.Sc project). Department of Sociology, Nigeria Police Academy, Wudil Kano State, Nigeria.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. London: Cambridge Polity Press.