Global Journal of Applied, Management and Social Sciences (GOJAMSS); Vol.22, August 2021; P.254 – 269 (ISSN: 2276 – 9013)

CYBERCRIME IN NIGERIA; A SOCIO LEGAL ANALYSIS WITH FOCUS ON JIGAWA STATE

GARBA ABUBAKAR
+2347062155365
garabalawyer@gmail.com
Jigawa State College of Education and Legal Studies, Ringim, Jigawa State

Abstract

Cybercrime has assumed a new dimension amongst youths in recent time. It was for this reason that the National Assembly had in 2015 enacted an Act known as Cybercrimes (Prohibition and Prevention) Act, 2015 with a view to combating cyber offences in Nigeria. Despite this enactment, cybercrimes are still on the rise in Jigawa State and Nigeria at large, hence, the need to go beyond the law in a quest to find an effective way for the prohibition, prevention and detection of cybercrimes in Jigawa State. Many factors could be adduced as being responsible for the crime in Jigawa State. A sample size of 200 was selected through the use of multi stage sampling procedure. Questionnaire and In-depth interview guide were the main servants, businessmen/women and cyber operators, cyber offenders, private organizations. The specific aim is to investigate the factors responsible for cybercrime, ascertain the consequences of cybercrime, identify the various techniques used in cybercrime and examine the strategic measures that can be put in place towards reducing cybercrime. Findings were made, some of them include that there is a linkage between age and participant in cybercrime. Individuals are aware cybercrime exist. Quest for quick money is a major factor that pushes youth into committing cybercrime. The study recommended among other that the government, Non-governmental Organizations (NGOs) and stakeholders should ensure that they put relevant programmes and campaigns which will make people to be more aware about cybercrime. The governmental, Non-governmental Organizations (NGOs) and stakeholders should ensure that they provide job opportunities for all age categories. Furthermore, families being the primary agent of socialization should be willing to monitor and give their children the required education on crime and also monitor the kind of friends they keep.

Introduction

Technological breakthroughs are hallmark of our contemporary era. One of such breakthroughs could be seen in the use of information systems across the globe. Information and communication technology (ICT) systems are used virtually in all walks of life. They are used at home for personal uses, and at various offices for business and uses. Most organizations, institutions, agencies and governments today, depend on computer networks to carry out both simple and difficult task, engage in technological advances; perform interdependence financial transactions and also disseminate classified information. Furthermore, ICT systems and computer networks enhance electronic commerce, mobile commerce, advances in medicine, research and innovations and social networking. In fact, ICT systems and computer networks are now regarded as basic essential utilities like electricity, water or telephone, without which, organizations and humans would struggle (Aderamola, 2008).

The information and telecommunications revolution is changing the face of crime in fundamental ways. Advances in technologies have provided exciting new opportunities and benefits but they so heighten vulnerability to crime. Computer crimes around the world cost organizations and governments billions of dollars each year (Jaishanker, Pang & Hyde, 2008). Advancements in technology are being used to perpetuate crime and it constitutes a serious problem for organizations and society in general. Cybercrime is one of the words frequently used by individuals in our contemporary society. Saul (2007) explained that to understand the true meaning of cybercrime, there is need to understand the slit waning of cyber and crime. The term “Cyber” is a prefix used to describe an idea as part of the computer and information age and

“Crime” can be described as any activity that contravenes legal procedure mostly performed by individuals with a criminal motive. Cybercrime began with disgruntled employees causing physical damage to the computers they worked with so as to get back at their superiors (Cassaday & Willians, 2001). As the ability to have personal computers at home became more accessible and popular, cybercriminals began to focus their efforts on home users. McAfee (2000) reveal Studies cybercrime which first occurred in the 1960s, when computers were large mainframe systems. Since mainframes were not connected with other ones and only few people can access them, the criminals were always “insiders”.

Actually in the 1970s, cybercrime was called “computer crime” in fact; it was different from the cybercrime which we have today, because availability of internet was restricted within some sections (e.g. US military) in that era. In the following decades, the increasing of computer network and personal computers transformed computer related crimes into cybercrime (Dickson 2008). Since Internet was invented, other new terms, like “cybercrime” and “net crime” became the order of the day as people began to exchange information based on networks of computers, also keep data in computer rather than paper. It is therefore safe to state that cybercrime is an evil having its origin in the growing dependence on computers in modern life. Cybercrimes are illegal behaviours directed by means of electronic operations that target the security of computer systems and the data processed by them.

Cybercrime in a broader sense is computer-related crime or any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network. Cybercrime refers to all activities done with criminal intent in cyberspace.
These fall into three categories:

- Crimes against persons
- Crimes against Business and Non-business organizations
- Crimes against the government

Cybercrimes are offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones.

To effectively fight against the wide spread of cybercrime in Nigeria, the National Assembly had in 2015, enacted a legal framework aimed at Prohibition, Prevention, Detection and Prosecution of cybercrime in Nigeria. This legislation is known as Cybercrime (Prohibition, Prevention, ETC) Act, 2015. It is indeed a comprehensive legislation comprising of 59 sections and schedules aimed at effective fighting cybercrimes in Nigeria. The Act made provisions for offences against critical national information, unlawful access to a computer, registration of cybercafé, system interference, interception of electronic messages, email, electronic money transfers, tempering with critical infrastructure, wilful misdirection of electronic messages, unlawful interceptions, computer related fraud, theft of electronic devices, unauthorised modification of computer systems, network data and system interference etc. Sections 5- 16 of the Act. The Act criminalised these offences on conviction of which carries penalties for imprisonment of period ranging from 3, 7, and 15 years’ imprisonment with fine of N1,000,000.00 up to N7,000.000.00 and or both. This is in addition to refund of the stolen money. With all the above provisions, it appears that cybercrimes are still gaining prominence in the state. There is therefore, a need to examine interaction of the law with the society, hence this research.

Methods Used by Cybercriminals

Cybercrime has increased dramatically in past years, and several recent events appear to be more alarming than ever before which other various techniques has been employed by cybercriminals to perpetrate the act. This includes phishing, spam, cyber terrorism etc. these aforementioned techniques are used to carry out their mission and these depend on what they want from their victims, which could be to defraud the victim of money, information or to cause harm. According to Roger (2008), phishing is simply a high-tech identity theft that does not only steal personal information and identity from unsuspecting consumers, but also an act of fraud against the legitimate businesses and financial institutions that are victimized by phishing. Flushing is usually a social engineering crime pervasive in attacking organizations' or individuals' (customers') information systems (IS) in order to gather private information to be used against organizations to extract some benefit for the perpetrator through the anonymity of identity theft or identity deception acts (Rodger, 2008).

Causes of Cybercrime

According to Stauss (2012) cybercrime is being carried out with some intentions, which are economical, personal, ideological and structural. As is the case with many crimes committed outside the internet, money is a major motivator for many cybercriminals, especially because the dangers of criminality are less apparent when you are hiding behind a network, the perception of low risk and very high financial reward prompts many cybercriminals to engage in malware, phishing, identity theft and fraudulent money request attacks (Richard, 2007). Business-week (2013) estimates that cybercrimes target online banking accounts alone, for example, pull in early 700 million dollars per year globally.

Most Nigerian youths, engage in cybercrime because they feel the rate of return on investment is high and the risk of loss are low and they have concluded it is profitable to continue committing fraud, stealing financial information and hacking into networks worldwide (Igbokwe, 2010). Strauss (2012) stressed on personal reason as a motive why people engage in cybercrime. Cybercriminals are human and what they do is often the cause of personal emotions and vendettas. From the disgruntled employee installing a virus on office computers to a jealous boyfriend hacking into a girlfriend's social media accounts or a teenager taking a school website just to prove that he could do it, many cybercrimes are essentially crimes of passion committed over the internet. Many of these crimes, however, can still have very impacts and cause considerable property damage (Badham, 2008).

Strauss (2009) posited that financial companies like Visa. MasterCard and PayPal refused to let account and card holders make contributions to the controversial non-profit Wikileaks, the "hacktivist" group Anonymous coordinated a series of "bot" attacks on the companies' servers, rendering them unreachable to internet users. These kinds of attacks are conducted for perceived ethical, ideological or moral reasons, damaging or disabling computer equipments and networks to express grievances against individuals, corporations, organizations or even national governments. Beyond the causes that motivate criminals, the environment in which cybercrime is committed also serves to explain the prevalence of the phenomenon while more and more personal and sensitive information is stored online increasing the potential rewards for cybercriminals – neither computer security nor applications like e-mail filters have improved dramatically in terms of coverage. According to the antivirus manufacturer Norton (2012); for sample, as many as 41 percent of computers did not have up-to-date security protection in 2012.

How to Control Cybercrime

Cybercrime cannot be eradicated completely, but can be reduced to a bearable minimum. However, collaborative efforts of individual, corporate organizations and government could go a long way in curbing this menace. Firms should secure their network information. Other measures to be taken include:

The need to educate citizens on how to make use of the internet, the need to continually maintain and update the security on the system. There is also the need to educate corporations' organizations the best practice for effective security management. For example, some large organizations now have a policy that all systems in their purview must meet strict security guidelines. Automated updates are sent to all computers and servers on the internal network, and no new system is allowed online until it conforms to the security policy. There is the need to install firewall security software in all networked systems which can help to protect, detect and block malwares (virus) that is being controlled by cybercriminals.

The internet users have to apply caution in everything they do online, by not clicking on any links in messages from people they do not know. The link will take you a fake website that asks for your private information such as user names and passwords, or it could download malware (virus) on to your computer. Even if the message is from someone you know, be cautious. In addition to your practicing safe shopping, you will also need to be careful as to where you shop online. Be cautious when shopping at a site that you have never visited before and do a little investigation before enter your payment information. Look for a trustmark such as McAfee SECURE^{TM}, to tell you if the site is safe.

Techniques used by cybercriminals

Cybercriminals use different types of techniques or methods to perpetrate cybercrimes. According to a study conducted by Okeshola & Adeta (2013), to determine the type of techniques used by cybercriminals and their findings show that a reasonable number of respondents (87%) are aware of password cracker as a technique that cybercriminals use to carry out their illegal act. Also, 53% of the respondents are aware of the key loggers as rather technique cybercriminals use to perpetrate cybercrime. However, 31% and 22% of the respondents are aware of the port scanner and vulnerability scanner as tools used by cybercriminals to perpetrate their act.

Leukfeldt, Veenstra & Stol (20134) carried out a qualitative survey in Netherland to determine the types of cybercrime or the techniques used by cybercriminals. Their findings reveal that electronic fraud and hacking as the two main techniques used by cybercriminals. Scientific studies of Anat & John (2003); Reid (2003), Easttom (2006), identified spamming, phishing, key logging and denial of service (DoS) as major methods used by cybercriminals to affect small businesses in the United States. Spam (unsolicited e-mail) crowds company inboxes and carries with it the threat of malicious attachments and viruses that can cause further damage (Reid, 2003). Virus detection software can protect against cybercrime, yet computers without the necessary software in susceptible to virus attacks (Cambell, 2004). According to the U.S. (Crime Scene Investigation) CSI/FBI (Federal Bureau of Investigation) Survey (2006) virus attacks constituted the single biggest threat of financial loss to United States (US) businesses. Denial of Service (DoS) attacks' intended to overwhelm the computer networks of a target business (Anat. & John, 2003), for example, cyber extortionists may launch a DoS attack on a network that provides e-mail service to many thousands of small businesses (Lepofsky, 2006).

Consequences/Effects of cybercrimes

To better understand the effect of cybercrimes on a global scale, the researcher decided to introduce the results announced by the last study of Ponemon Institute. The study, titled The 2013 Cost of cybercrime Study, provides an estimation of the economic impact of cybercrimes. It is sponsored by HP for the fourth consecutive year. It reveals that the cost of cybercrimes in 2013 escalated to 78 percent, while the time necessary to resolve problems has increased by nearly 130 percent in four years. Meanwhile, the average cost to resolve a single attack totaled more than $1 million.

According to Ponemon (2013) in his research work, he stressed that "Information is a powerful weapon in an organization's cyber security arsenal. Based on real-world experiences and in-depth interviews with more than 1, 000 security professionals around the globe, the cost of cybercrime research provides valuable insights into the causes and costs of cyberattacks. The research is designed to help organizations make the most cost-effective decisions possible in minimizing risks to their companies". The frequency cost of the cyber-attacks increased in the last 12 months. The average annualized cost of cybercrimes incurred by a benchmark sample US organizations was $11.56 million. This is an increase of 26 percent, financial services and energy and utilities suffered the highest cybercrime costs. Data theft caused major cost, 43 percent of the total external costs, business destruction or lost productivity account for 36 percent of external costs. While the data theft decreased by 2 percent in the last year, business destruction increased by 18 percent. Organizations experienced on average of 122 successful attacks per week, up from 102 attacks per week in 2012. The average time to resolve a cyber-attack was 32 days with an average cost incurred during this period of $1, 035,769, or $32,469 per day – a 55 percent increase over last year's estimated average cost of $591, 780 for a 24-day period. Smaller organizations incurred a significantly higher per-capital cost than larger organizations.

Center for strategic and international studies (CSIS), Titled Threat Landscape Midyear 2013, the organization confirmed the result of the Ponemon Institute. The McAfee security firm estimated that cybercrime and cyber espionage are costing the US economy $100 billion per year, and the global GDP was about $70,000 billion in 2011, the overall impact of cybercrime is 0.04 percent of global income. Another concerning side effect of cybercrime activity is the loss of 508,000 jobs in the US alone. That is mainly caused by theft of intellectual property, which wiped out the technological gap of U.S companies against Asian competitors. The Symantec security firm has just released the 2013 Norton Report, the annual research study which examines the consumers' online behaviours, the dangers and financial cost of cybercrime. Also, their data confirms the concerning results of other analysis. Cybercriminal activities and related profit are in constant growth, the cost per cybercrime victim is up 50 percent, and the global price tag of consumer cybercrime is $113 billion annually. That's a result of the concerns security analysts consider. It also affects the annual global economic scenario and the difficulties faced by enterprises. This data was reported in the Norton Report, a document considered as one of one of the world's "largest consumer cybercrime studies, based on self-reported experiences of more than 13, 000 adults across 24 countries, aimed at understanding how cybercrimes affect consumers, and how the adoption `and evolution of new technologies impact consumers' security". The Norton report also states that the number of online adults who have experienced cybercrimes has decreased, while the average cost per victim has risen.

Sesan, Soremi, & Bankole (2013), carried out a research to examine the economic cost of cybercrime in Nigeria. The survey was administered both online and offline. The offline survey participants were drawn from mainly four locations across the country namely Abuja, (capital city), Abeokuta (South West Nigeria), Minna (Northern Nigeria) and Uyo (South South Nigeria). These locations fairly represent the different parts of the country and relied on the resources of paradigm initiate in those locations to get as many responses as possible. The survey was administered between 2013 with a total two thousand nine hundred and eighty (2,980) respondents participating in the survey, online and offline. The survey was designed to be administered in order to measure respondents' experience in cybercrimes incidents, monetary losses, time losses and other losses that might have been occasioned.

According to Seran, Soremi and Bankole (2013), they found out that 41% of the survey respondents indicated that they had been victims of cybercrime at one time or the other, while 59% indicated that had yet to fall victim. The breakdown of responses by location indicates higher incidence of cybercrime in the western and eastern parts of the country, represented by Abeokuta and Uyo respectively. The northern areas of Abuja and Minna, on the other hand, recorded lower cybercrime occurrences. While 70% of respondents affirmed they were not victims of cybercrime in 2012. This is a probable indicator that awareness of cybercrime is increasing, and is causing people to take preventive measures that reduce their vulnerability to attack. The apparent increase in awareness notwithstanding, 30% of respondents fell prey to the vice of cybercrime in 2012. Despite a higher drop in the event of cybercrime in 2012, Abeokuta and Uyo still recorded higher incidents than other parts of the country. The logical explanation for this would be their relatively higher levels of economic activity compared to other physical areas surveyed. Also the monetary loss sustained by the respondents to cybercrime in 2012 was two hundred and twenty-six million nine hundred and twenty-seven thousand, eight hundred and ten naira, and ten kobo (N226, 927,810.10 or $1,432,172.99). 10% of respondents lost more than one million naira (N1, 000,000). 31% of respondents lost between one hundred thousand naira (N100, 000) and nine hundred and ninety-nine thousand naira (N999, 000). 5% of respondents lost one hundred thousand naira (N100, 000)

Respondents highlighted several other areas of loss they experienced due to cybercrime incidents. The four most common are personal data effects; phones and airtime recharge cards; goods and business. For those who lost goods, this included the loss of opportunities to invest, import and/or export their products. Some respondents who had toured visas for sports events and schools also lost the opportunity to complete their trip. The loss of phones by respondents often meant the loss of private information and data that reside on the devices. Loss of personal data was the most common, with banking information ranking highest in the category, it could also be noted that a number of respondents lost property (asset) to cybercriminal activities in 2012.

According to Seran, Soremi and Bankole (2013), they estimated the economic cost of cybercrime in Nigeria, quantitative research was employed in gathering information around losses (money, time and materials) incurred by citizens through cybercrime. Using Nigeria's minimum wage, lost time was computed, and estimates on Average Revenue Per User (ARPU) – Provided by the telecommunications regulator and others – were used to estimate non-cash, non-time loss. The ratio of internet users that were affected by cybercrime, calculated from survey sample size, was then used to estimate the cost for the larger population. In addition to the monetary losses by respondents, time losses were converted into economic costs using the appropriate fraction of the minimum wage-with each month estimated at 20 working days, and 8 hours per day. The non-cash, non-time loss comprised top-up card used by victims who called to follow up on their losses and few cases of reported real estate loss. Based on applicable ARPU in Nigeria, we computed the economic costs of this loss. The cost estimation conservative estimates to compute the value of real estate losses. The cost estimation focused on 2012, so the percentage of respondents that were affected by cybercrime in 2012 was used to estimate how many of Nigeria's 48.3 internet million internet users experienced the loss. This was used to compute the estimated loss for Nigeria, nothing that though the sample size for the survey provided 2.36% error margin (and 99% confidence level), only the percentage online are affected directly by cybercrime-related losses. This led to the estimated Nigeria consumer loss of N2, 146,666,345,014.75 ($13,547,910,034.80) to cybercrime in 2012. In conclusion, the economic cost of cybercrime in Nigeria was quantified into intangibles like missed trade opportunities, all as a result of the inherent distrust of Nigerians in foreign countries and online occasioned by countless bad experiences. As this report demonstrates, the internal threat is substantial and must be met with concerted deterrent strategy. Else, other new economy initiatives, which are based on electronic interactions such as mobile money, cashless society, e-commerce, and more, will suffer.

Data Presentation and Analysis

The researcher distributed 204 questionnaires with the help of research assistants. However, 200 (98.04%) of the questionnaires were correctly filled when they were returned. The remaining four were not properly filled as a result of this they were excluded for analysis. Consequently, the quantitative analyses for the study were processed with the 200 correctly filled and returned questionnaires.

Analysis of Research Question

This section deals with the analysis of research questions formulated to guide this study.
The researcher asked four (4) research questions to guide this study. They are as follows,
Research Question One: what are the factors responsible for youth involvement in cybercrime? The findings are shown in table 1. respectively.

Table 1: Distribution of respondents, on whether or not they have heard about cybercrimes

Respondent	Frequency	Percentage
YES	192	96.0%
No	8	4.0%
Total	200	100%

Field Survey, 2021

The table clearly indicates that 96.0% of the respondents knew about cybercrimes, only 4.0% of them have no knowledge about cybercrime. This therefore, implies that majority of the respondents know what cybercrime is all about. One of the IDI respondents noted that "Cybercrime is a recent type of crime which is in a widespread in our society. More youths are becoming participants in it" in Jigawa State.

Table 2: Distribution of Respondents on their views about the major cause of cybercrime

Respondent	Frequency	Percentage
Bad Parenting	23	11.5%
Poverty	26	13.0%
Unemployment	64	32.0%
Peer Group Pressure	32	16.0%
All of the above	54	27.0%
No response	1	0.5%
Total	**100**	**100.0%**

Field Survey 2021

It is observed in table 3 that the respondents (11.5%) saw bad parenting as the major cause of cybercrime, 13.0% indicated that poverty is the root cause of cybercrime, 32% maintained that cybercrime is majorly caused by unemployment, 16.0% believed that cybercrime is caused by peered group pressure, 27% indicated that cybercrime is caused by all the above, 0.5% did not respond to the question. This indicates that cybercrime is mainly caused by unemployment.

Table 3: Distribution of Respondents on people who engage in Cybercrime

Respondent	Frequency	Percentage
15-19	2	1.0%
20-25	30	15.0%
31-36	51	25.5%
37years and above	45	22.5%
No response	3	1.5%
Total	**200**	**100%**

Field Survey 2021

Table 3 indicates that individuals between the age bracket of 15-19 have little number of involvement in cybercrime with a percentage 0f of 1.0% , the respondent shows that 20-25years had 15.0% of the general people who involve in cybercrime, majority indicates that people who commit cybercrime are the age category of 26-30 with the number of 34.5%, other respondents maintained that people who fall between the age of 31-36 also engage in cybercrime with a number of 25.5%, 22.5% of them believe that people involve in cybercrime are of that 37years and above, some has the opinion that people who engage in cybercrime has no age bracket, so did not respond to the age category(1.5%), This clearly shows that majority of people who engage in cybercrime are between the age bracket of 26-30 with a percentage of 34.5%. One of the IDI respondents stated that "cybercrime is a crime mostly committed by the youths of various ages"

Table 4: Distribution of Respondents on people who engage in Cybercrime

Respondent	Frequency	Percentage
Greediness	31	15.5%
Poverty	35	17.5%
Peer group pressure	29	14.5%
Quest for quick money	102	51.0%
No response	3	1.5%
Total	**100**	**100%**

Field Survey 2021

Table 4 indicates that 15.0% of people who engage in crime are being lured by greed, while 17.5% of the respondents believe that poverty pushes youths to engage in cybercrime, 14.5% of the respondents indicates that peer group pressure lead youths into cybercrime, 51.0% maintained that cybercrime is mostly caused by quest for quick money, 1.5% did not respond to the questionnaire item. This clearly indicates that majority of the youths who engage in cybercrime in Jigawa State do that in a quest for quick money. These findings are in agreement with the qualitative data.

One of IDI respondents stress that, everybody wants to make money and the society don't care much on how the money is being made, cybercrime is a crime that youths make a lot of money from (male 33 years trader in Jigawa State).

Research Question Two: What are the various cyber techniques used by cybercrimes to perpetrate the act in Jigawa State? The research question is answered by the research questionnaire item 12 and 14. The findings are shown in table 6 and 7 respectively.

Table 5: Distribution of Respondents on techniques used by cybercriminals

Respondent	Frequency	Percentage
Virus attack	4	2.0%
Data theft	31	15.5%
Spam mail	77	38.5%
Fake website	55	27.5%
Debit/Credit card fraud	32	16.0%
All of the above	1	0.5%
Total	**100**	**100%**

Field Survey 2021

Table 5 indicates that 2.0% of the respondents said that virus attack is a technique used by cybercriminals, 15.5% of the respondents indicates that data theft is another technique, but 38.5% believed the spam mails is the major technique used by cybercriminals, 27.5% shows that fake website is another strong technique used by cybercriminals, 16.0% of the respondents indicate that debit and credit card fraud is technique used by cybercriminals but only 0.5% of the respondents that all of the above cyber techniques. These clearly suggest that majority of the respondents believe that spam mails is the major technique used by cybercriminals to carry out their dirty jobs.

One of the IDI respondents (26 years mail cyber offender in Jigawa State) opined that, "spamming is one of the major techniques we use (cyber offenders) to carry out our job because people read their emails daily and reply them".

Another IDI respondent put it this way, "through reading and replying of emails from unknown source people establish contact with cybercriminals". (Male 24-year-old trader).

Table 6: Distribution of Respondents on whether or not they have received messages asking them to disclose some personal information

Respondent	Frequency	Percentage
YES	105	52.5%
No	95	47.5%
Total	**200**	**100%**

Field Survey, 2021

Table 6 indicate that majority of the respondents (52.5%) have received messages from cybercriminals asking them to disclose personal information, 47.5% of the respondents have not received messages from cybercriminals asking them to disclose personal information. The quantitative data above is in agreement with the qualitative data gotten. One of the respondents stressed that “almost every day I receive messages from unknown source telling me that I have won one item or the other in an advertisement which I never registered interest in because I knew that the messages are fraudulent “(male 41 years’ manager in an organization in Hadejia, Jigawa State).

Another IDI respondent 37 years old male civil engineer in Dutse LGA, Jigawa State stated that, “I receive messages on a daily basis from fraudsters claiming to be who they are not”.

Research Question Three: What are the consequences of cybercrime in Jigawa State? The research question is answered by questionnaire 16 and 17.the findings are sown in table 8.

Table 7: Distribution of Respondents on the effects of cybercrime

Respondent	**Frequency**	**Percentage**
YES	133	66.5%
No	66	33.0%
No response	1	0.5%
Total	**200**	**100%**

Field Survey, 2021

Table 7 indicates66.5% of the respondents shows that cybercrime has a major effect on the nation growth and the general well being, 33.0% indicates that cyber has no effect on the Jigawa State status.

One of the IDI respondents explains that, “Nigeria is ranked among the top countries who engage in cybercrime which affects our business transaction with our counterparts abroad. Cybercrime is why they always double check every information we send to them” (female 39 years business in Dutse LGA Jigawa State).

Research Question Four: In what ways can cybercrime be reduced in Jigawa State? The research question is answered by questionnaire items 18, 19, 20, 21 and 22, findings are shown in tables 9, 10, 11, 12 and 13 respectively.

Table 8: Distribution of Respondents on how to eradicate cybercrime

Respondent	**Frequency**	**Percentage**
Through educating people	41	20.5%
Implementing cyber laws	42	21.0%
Creating cyber agency	70	35.0%
All of the above	45	22.5%
No response	2	1.0%
Total	**200**	**100%**

Field Survey 2021

It is shown in table 9 that 20.5% of the respondents stated that cybercrime can be reduced through educating the people, 21.0% of them opined that implementing cybercrime laws can help to eradicate cybercrime, 35.0% of the respondents stated that through creating cybercrime agency, the act will be curbed, 22.5% of the respondents believe that all of the above methods can be used to reduce cybercrime, 1.0% did not respond to the questionnaire item.

One of the IDI respondents opined that, “educating everybody in our society about cybercrime will go a long way in eradicating this mess, it should not be left alone for the government to do, all businesses, agencies, stakeholders, media houses should come to teach people about cybercrime” (male 31 years barrister and solicitor).

Table 9: Distribution of Respondents on how to prevent cybercrime

Respondent	Frequency	Percentage
Installation of antivirus	19	9.5%
Stop using cyber cafe	66	33.0%
Giving cybercriminals long sentence	35	17.5%
Enlighten people about cybercrime	52	26.0%
All of the above	27	13.5%
No responses	1	0.5%
Total	**200**	**100%**

Field Survey 2021

Table 9 indicates that 9.5% of the respondents opined that cybercrime can be reduced through Installation of antivirus programmes into their systems, 33.0% of the majority argued that a way to prevent cybercrime from occurring is that they should avoid using cyber café, 17.5% of them are of the opinion that cybercriminals should be given longer sentence, 26.0% argued that through educating and enlightening people about cybercrime, it can be prevented, 13.5% of the respondents believed that all of the above can be used to prevent cybercrime but 0.5% did not respond to the question. This clearly shows that the majority of the respondents are of the opinion that not using cyber café can bring an end or prevent cybercrime from occurring.

One of the IDI respondents 31 years male barrister and solicitor stressed that, “I still maintain that the easiest and quickest way to prevent ourselves from cybercrime is to enlighten the people through the media and other socialization agent”.

Table 10: Distribution of Respondents on Arrest Carried out by EEFC in Relation to Cybercrime

Respondent	Frequency	Percentage
Very often	30	15.0%
Often	78	39.0%
Hardly	52	26.0%
Never	7	18.5%
No response	3	1.5%
Total	**200**	**100%**

Field Survey, 2021

Table 10 indicates that majority of the respondents (39.0) often witness EFFC arrest people in relation to cybercrime, 15.0% concurred that EFFC do arrest people in relation to cybercrime, 26.0% argued that they hardly see EFFC arrest people on the subject matter, 18.5% are of the opinion that EFFC never arrest people on cybercrime, only 1.5% of the respondents did not respondent to the question. This clearly indicates that EFFC do arrest people in relation to cybercrime in Jigawa State.

Table 11: Distribution of Respondents on whether there are enough laws to combat cybercrimes in Nigeria

Respondent	Frequency	Percentage
YES	101	50.5%
No	92	46.0%
No response	7	3.5%
Total	**200**	**100%**

Field Survey, 2018

Table 11 clearly indicates that 50.5% of the respondents agreed that there are enough laws to combat cybercrimes in Nigeria, 46.0% of them disagreed that that there are enough laws to combat cybercrimes in Nigeria, while 3.5% did not respond to the question. The findings of the quantitative data are in agreement with qualitative data.

"there are lots of laws in Nigerian to guide, protect and persecute cybercriminals" (female legal practitioner in Dutse LGA, Jigawa State).

Table 12: Distribution of Respondents on Stakeholders in Preventing and Controlling Cybercrime in Nigeria

Respondent	Frequency	Percentage
Very Satisfied	33	16.5%
Satisfied	89	44.5%
Dissatisfied	30	15.0%
Very dissatisfied	14	7.0%
Not Sure	33	16.5%
No response	1	0.5%
Total	**200**	**100%**

Field Survey, 2018

Table 12 shows that 16.5% of the respondents are very satisfied of the role played by relevant stakeholders in combating cybercrimes, 44.5% said that they are satisfied, while 15.0% argued that they are dissatisfied, also 7.0% maintained that they are very dissatisfied, 16.5% of the respondents are not sure, 0.5% of the respondents did not respond to the question. This clearly shows that majority of the respondents are satisfied with the role played by relevant stakeholders in combating cybercrimes in Jigawa State.

One of the IDI respondents is of the opinion that, "stakeholders are trying by enlightening the people about cybercrime but they have not shown concrete effort on their part to fight against cybercrime" (male aged 22, student in Dutse LGA).

Test of Hypotheses

The researcher tested the two hypotheses postulated for this study. The hypothesis was re-staled and tested as follows:

Hypothesis One: There is a significant relationship between age and involvement in cybercrime in Jigawa State. Data in table 14 formed the basis for testing hypothesis 1

Table 13: Cross Tabulation between age and crime

What age category do you fall under	Have you written or used a programme that would destroy someone computerized data either knowingly or unknowingly (e.g. a virus, logic bomb, or Trojan horse?)		X2 (4, N = 200 = 11.123 P = .025
	Yes	No	Total
15 – 19	3	10	13
20 – 24	6	18	54
25 – 29	2	50	52
30 – 34	0	34	34
35 and above	2	45	47
Total	13	187	200

Field Survey, 2021

The computed value of chi square is 11.123 while the table value of chi square at 0.05 level of significance with a degree of (df) of 4 is 9.488. Since the computed chi square value is greater than the critical value, the researcher accepted the alternative hypothesis. It follows therefore that there is a significant relationship between age and involvement in cybercrime in Jigawa. This implies that younger people are more likely to involve in cybercrime than the older ones in Jigawa.

Hypothesis Two: male respondents are more likely to involve in cybercrime than their female counterpart in Jigawa State. Data in table 15 formed the basis for testing hypothesis two.

Table 14: Cross Tabulation between age and crime

What is sex	Have you written or used a programme that would destroy someone computerized data either knowingly or unknowingly (e.g. a virus, logic bomb, or Trojan horse?)		X2 (1, N = 200 = 3.598 P = .058
	Yes	No	Total
Male	10	93	103
Female	3	94	97
Total	13	187	200

The computed value of chi square is 5.598 while the table value of chi square at 0.05 level of significance with a degree of (df) of 1 is 3.841. Since the computed chi square value is less than the table value, the researcher rejected the alternative hypothesis. It implies that male respondents are not more likely to involve in cybercrime than their female counterparts in Jigawa State.

Conclusion

From all indications, this has succeeded in highlighting and elaborating on the determinants and consequences of cybercrime in Mushin Jigawa State. Therefore, if these factors are critically examined, tackled and dealt with, the alarming rate of cybercrime in Jigawa in general will drastically reduce hence the need for individual enlightenment towards cybercrime, will discourage youth from engaging in it or falling into victims of same. Despite the fact that this study has contributed immensely in filling a gap in knowledge, it is imperative to note here that it is not above criticism, as there is room for replication and further studies on cybercrime and its associated challenges.

Recommendations

The following recommendations have been adduced for possible implementation:

1. The Government, Non-governmental Organizations (NGOs) and stakeholders should ensure that they put relevant programmes and campaigns which will make people to be more aware about cybercrime.
2. The Government, Non-governmental Organizations (NGOs) and stakeholders should ensure that they provide jobs opportunity for all age categories.
3. The family being the primary agent of socialization should be willing to monitor and give their children the required education on crime and also monitor the kinds of friends they keep.

References

Adebusuyi, (2008). The Internet and Emergence of Yahooboys sub-Culture in Nigeria, *International Journal of Cyber-Criminology*, 2, 368 – 381.

Adesina, A.D.O. & Adeyemi, B.A. (2007(. Teaching to achieve Social Studies Values: *A case of reeducation of Teachers*. Retrieved Oct. 10, 2010.

Anderson, Ross, et al. (2012). Measuring the cost of cybercrime, *11th Workshop on the Economics of Information Security (June 20, 2002*), Retrieved from http://weis2012.econirrfosec.org/papers/Anderson. WEIS2012. pdf

Akogwu, S. (2012). *An Assessment of the level of Awareness of Cybercrime among Internet Users in Zaria* (Unpublished B.Sc. Project/ Department of Sociology, Ahmadu Bello University, Zaria.

Alshalan & Abdullah (2006). Cybercrime fear and victimization: *An analysis of a national survey*. Dissertation, Mississippi State University.

Anat, H. & John, D.A. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review*, 6 (2), 97. CSI/FBI. (2006. *Computer Crime and Security Survey XI Annual*. Retrieved from http://i.cmpnet.com/gocsi/dharea/pdfs/fbi/FB 12006. pdf

Augustine, C., Odinma, & Mieee, (2010). Cybercrime & Cert: *Issues & Probable Policies for Nigeria*, DBI Presentation.

Aggarwal, V. (2009). Lead: *Cybercrimes' rampant, Express Computer*, Retrieved from http://www.expresscomputeronline.com/20090803/markel101.shlml.

Awe, J., (2009). Fighting Cybercrime in Nigeria retrieved from hptt://www.jidaw.com/itsolutions/security3.html.

Ayantokun, O. (2006). *Fighting cybercrime in Nigeria*: Information-system, www.Tribune.Com.

Byongook, M., & John, I., mCcLUSSKEY, Cynthia, P. M., (2010). "Information Technology/Cyber Security Solutions" *Journal of Criminal Justice* 38, 767 – 772.

Boom, Juridische, uitgevers Den H. (2010). Atul Bamrara HNB Garhwal University, India Gajcndra Singh Doon University, India Copyright © 2013 *International Journal of Cyber Criminology* (ˆCC), 7 (1) 4961.

Bohme, Rainer, Tyler M. (2012). *How do consumers react to cybercrime*? 7th APWG eCrime Res. Summit. Las Croahas, 1(2).

Bruce Schneier. Ed., *Economics of Information Security and Privacy III*. Springer, New York.

Cheng, T.C. Edwin, David. Y.C., Lam, Andy, C. L. Yeung. (2006). Adoption of Internet Banking: *An empirical study bin Hong Kong*. Decis.

Chiemeke, C.S. & Longe C. B. (2007). Information and Communication

Penetration in Nigeria: Prospects, Challenges and Metrics. *Asian Journal of Information Technology*. 6 (3), 280 287.

Cybercrime (Prohibition, Prevention, ECT) Act, 2015, Laws of the Federation of Nigeria.

Choo, K.R. (2009). High tech criminal threats to the national information infrastructure. *Information Security Technical Report*, XXX, 1 – 8. Cybercrime. Retrieved from http://www.tcehterms.com/detmitio/cybercrime.

Choo, K.R. (2008). Organized crime groups in Cyberspace: *A typology Springer Science Policing and reducing Crime Unit*: Research, Development and statistic Directorate.

Cohen, L.E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach: *American Sociological Review* (44).

Diller-Haas, A. (2004). Identity theft: it can happen to you. *The CPA Journal*, 74 (4), 42.

Eastlom, C. (2006). *Computer security fundamentals*. Upper Saddle River, N.J: Prentice Hall.

Ehimen, O.R. & Bola, A., (2010). Cybercrime in Nigeria. *Business Intelligence Journal*, 3 (1), 5.

FBI (2005). *FBI Computer Crime Survey*. Retrieved from http://www.fbi.com

Donn B. & Parker, (1998) *Fighting Computer Crime*. New York, USA, John Wiley & Sons, Inc.

D. I. (2001). Scene of Cybercrime: *Computer Forensics Handbook*. Syngress Publishing Inc. 88Hingham Street USA.

Elijah, J., Esquibel M.a. Laurenzano, Jing, X., Ted, Z. (2005). Cybercrime activity: *Methods and Motivations* 2 (2), 290 – 309.

Forencio, Dninei, Cormac, H. (2013). *Sex, Lies and Cybercrime surveys*

Foltz, C.B. (2004). Cyber terrorism, computer crime and reality. *Information Management & Computer Security*, 12 (2), 154.

Fulcher, J. & Scoltt, J. (2007). *Sociology 3rd edition*. Oxford University Press

Hloltfreter, K. Reisig, M.D. & Pratt, T.C. (2008). Low self-control, outline activities and fraud victimization. *Journal of Criminology*. 46, 189 – 220.

Hloltfreter, K. Beaver, K.M. Reisig, M.D. & Pratt, T.C. (2010). Low self control and fraud offending. *Journal of Financial Crime*, 77 (3). 295 – 307.

Hutchings, A. & Hayes, H. (2009). Routine Activity theory and phishing victimization: who got caught in the "net:? *Current issues in Criminal Justice* 20, 432 – 451.

Igbo, E.U.M (1999). Introduction to Criminology. Nsukka Afro-orbis publications.

Independent. (1994). '*Genes linked to violence and crime condemned'*. Retrieved from http://www.independentco.uk/news/genes-liked-to-violence-and crimecondemned-1573089.html

Jaishankar, K. (2008). Space Transition Theory of Cybercrimes. In Schnallangar, F. & Pittaro, M. (Eds.). *Crimes of the Internet* 283 – 301). Upper Saddle River, NJ: Prentice Hall.

Kigerl, A. (2011). Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Computer Review*. 000 (00). 1 – 17.

Koshy, E., Koshy, V, Waterman, H. (2010). Action Research for health care. London: SAGE "Nigeria: Prospects. Challenges and Metrics. *Asian Journal of Information Technology*.

Laura, A. (1995) cybercrime and National Security: "The Role of the Penal and Procedural Law" *Research Fellow, Nigerian Institute of Advanced Legal Studies*, Retrieved from http://nials-nigeria.org/pub/lauraani.pdf.

Longe, O. B. & Chiemeke, S. (2008). Cybercrime and Criminality in nigeria – What Roles Are Internet Access Points In playing? *European Journal of Social Sciences*, 6 (4).

Mc Council (2000). *Cybercrime and Punishment*. Archaic Law Threaten.

Mohsin, A. (2006). *Cybercrimes and solutions*, Retrieved from http://ezinearticles/?cybercrimes and solutions &id=204167.

Okonigene, R.E. & Adekanle, B. (2009). Cybercrime in Nigeria, *Business Intelligence Journal*, retrieved from http://www.saycocorporatiotion.com/saycoUK/BIJ/journal/3(1)/Article7

Olaide & Adewole (2004), *Cybercrime Embarrassing for Victims*. Retrieved September 2011 from http://www.heraldsun.com.au

Oliver E.O. (2010). Being Lecture Delivered at FBI/ George Mason University Conference on Cyber Security holding, *Department of Information Management Technology* Federal University of Technology, Owerri.

Olumide, O. O. & Victor, F. B. (2010). E-crime in Nigeria: Trends, Tricks and Treatments. *The Pacific Journal of Science and Technology*, 11, (1).

Olaide & Adewole (2- -4). *Cybercrime Embarrassing for victims*. Retrieved from http://www.guide2nigeria.com/news-articles_About Nigeria.

Oyewole & Obeta (2002). *An Introduction to Cybercrime*. Retrieved from http://www.crimeresearch.org/articles/cybercrime.

Orin, S. & Kerr (2003). Cybercrime's Scope: *Interpreting Access and Authorization In Computer Misuse Statutes* NYU Law review, 78 (5), 1596 – 1668.

Peter, A. A., Olugbenga, A.,Ige a. a. (2013). WODC, Commissioning Research Division, Ministry of Security and Justice. *Ministry of Security and Justice*.

Ribadu, E. (2007). Cybercrime and Commercial fraud; Nigerian Perspective, *A paper presented at the Modern Law for Global Commerce.*

Roseline, O. & Moses, O. (2012). Cyber capacity without cyber security: A case study of Nigeria's national policy for information technology (NPFIT), *The Journal of Philosophy, Science and Law*, 12, Retrieved from www. Miami.Edu/Ethics/Jpsi

Schaeffer, B. S. et al. (2009): cybercrime and cyber security: *A while paper for Franchisors, Licensors and others.*

Sesan, G. (2010). *The new security war*, retrieved from http://www.pcworld.com/article/122492/the_new_security_war.htmmod-rel.

Shinders Strassmann, P. A. (2009). *Cyber Security for the Department of Defense*,. Retrieved from http://www.strassmann.com/pubs/dod/cybersecurity-dratf-vl.pdf

Stol, W. Ph., Leukfe;dt, E. R & Dommenie, M. M. L. (2011). Internet crime and the police. *Journal of police studies*, 20 (3) 59 – 81.

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

Symantec. (2007). Small and mid-sized business products. *International Journal of cyber criminology* retrieved from http://www.symantec, com/smb/products/index.jsp

The national white collar crime center (2010) *IC3 2009 internet, crime report*. Retrieved from http://www.TC3.state.gov. 1- 29.

The national White collar crime center (2002). *IFCC 2001 Internet Fraud Report*. Retrieved from http://www.IC3.gov. 1 – 27.

Thompson, D. (1989). Police powers – *Where's the Evidence, Proceedings of the Australian Computer Abuse Inaugral Conference*.

Umeozulu, F. (2012). *Perception of Cybercrime Among Nigerian Youths*

Umo,. G. g. (2010). CYBER Threats: *Implication for Nigeria's National Interest*, Retrieved from http://docs.google.com/file/d/QB9sby6n_V503M2FINWIzZjglMDRiosoonJLLltHmjllNmlONzg5NGVINTM2/edith?num=50&sort=name&layout--list&pli=1

Van der Hulst, R. C. & Nweve , R. J. M. (2008). High-tech crime; *inventarisate van literature over soorten criminalities en hun daders*. [High Tech Crime. Literature review about crimes and their offenders] Den Haag: WODC. Gaurav Misra, Permeance of ICT in Crime in India

Vladimir, G. (2005). *International Cooperation in fighting cybercrime* www.crimesearch.org.

Yar, M. (2005). The Novelty of cybercrime: An assessment in light of Routine Activity Theory. *European Journal of Criminology*. 2. 407 – 427.

Zero, T. (2006). Retiree in Trouble over Internet Fraud. *Economic and Financial Crime Commission*, 1, (2) 8 – 12.