Quest Journals
Journal of Research in Humanities and Social Science
Volume 9 ~ Issue 9 (2021)pp: 84-94
ISSN(Online):2321-9467
www.questjournals.org

Research Paper

A Historical Assessment of Cybercrime in Nigeria: Implication for Schools and National Development

Moga, Ezekiel[1], Salihu Abdullahi GALLE (Ph.D)[2], Abdulkarim Rukayyat[3]
[1]*Department of Arts and Social Science Education*
Nasarawa State University, Keffi, Nigeria
[2] *Department of Educational Foundation,*
Educational Research, Measurement & Evaluation Unit,
Nasarawa State University Keffi,
[3]*Department of Computer Science,*
Federal University Lafia, Nasarawa State.

ABSTRACT
A nation would not grow without assessing the previous and present occurrences especially in this era of high globalize society that transform virtually all activities in a technological ways which human beings see advantage. Hence, this study focuses on a historical assessment of cybercrime in Nigeria: Implication for schools and National Development. A mixed research design was employed by the researchers in generating primary and secondary data. Primary data was generated using Focus Group Discussion (FGD) using 200 undergraduate students of the Nasarawa State University, Keffi based on cybercrime and the secondary data was generated based on the existing electronic materials. The data generated from FGD were analysed using descriptive statistics of frequencies and percentages. Findings revealed that 84% of the students agreed that cybercrime exist highly among students such as; hacking of Face-Book Page or WhatsApp Page of someone in disguised using it for devious acts, Manipulating students' school fees and semester results are some of the cybercrimes in the school system. Further results of the secondary sources revealed related cybercrime to include; quest for wealth, Poor implementation of cybercrime laws, and corruption among others. With these alarming results, schools and National development would be at catastrophic in different ramifications of economy activities. The paper suggests that; schools should form personality assessment committee to assess students attitudes toward cybercrimes, Personal Identification Number (PIN) should not be made known to unknown persons, and Government should enact stringent laws and prosecute perpetrators of such act without discrimination among others.

KEYWORDS*: Historical Assessment, Cybercrime, National Development, Nigeria*

Received 25 August, 2021; Revised: 07 September, 2021; Accepted 09September, 2021 © The author(s) 2021. Published with open access at www.questjournals.org

I. INTRODUCTION

In the recent years, the advent of computers and the internet has opened a vast array of possibilities for the young and the old in the international community to have access to the world from their homes, offices, cyber cafes and so on. In recent times, internet or web-enabled phones and other devices like iPods, and Blackberry, have made internet access easier and faster. Not so long ago, computers were large, cumbersome devices utilized primarily by government, research and financial institutions. The ability to commit computer crimes was largely limited to those with access and expertise. Today, the technology is ubiquitous and increasingly easy to use, ensuring its availability to both offenders and victims (Clough, 2010). The proliferation of digital technology, and the convergence of computing and communication devices, has transformed the way in which we socialise and do business. While overwhelmingly positive, there has also been a dark side to these developments. Proving the maxim that crime follows opportunity, virtually every advance has been accompanied by a corresponding niche to be exploited for criminal purposes (Clough, 2010). Thus, one major consequence of this unlimited access to the world has been an increase in the spate of cybercrimes. Numerous crimes of varying dimensions are committed daily on the Internet worldwide.

National development is an economic development. Economic development quantitatively means a higher GDP per capita. Since GDP is a measure of consumption, a higher consumption means that the people of the country eat better food, live in better homes, live in in a better environment with clean and pure air and water. More importantly, they have assurance of leading a better life in the future (Sandeepan, 2018). Zack (2019) sees National development as the change in growth and development, which include social, cultural and economic change. It is the ability of a country to improve the social welfare of the people characterize by the overall development of a collective socio-economic, political as well as religious advancement of a country. Tolu and Abe (2011) describes National development as the overall development or a collective socio-economic, political as well as religious advancement of a country or a Nation. This is best achieved through development planning which can be described as the country's collection of strategies mapped out by the government

Statement of the Problem

The contribution of the internet to the academic development of among Nigerian undergraduate has been marred by the conscious evolution of new waves of crime. The internet has also become an environment where the most productive and safest offence thrives. Cyber-crime has come as a surprise and a strange appearance that for now lives with us in Nigeria. With each passing day, we observe more and more alarming cases of cyber-crimes is perpetrated by Nigerian undergraduate, 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 among students and committing all sorts of atrocities through the aid of the internet online contact and transactions. In most cases, various forms of crimes are being witnessed ranging from exam negligence's, falsification of admission, rape, robbery and stealing, sexual molestation, onslaught, cultism amongst others. With this ugly happening, the face of the department and the institution at large has suffered a lot of setbacks schools and national development. It is against this background that this study investigating a historical assessment of Cybercrime in Nigeria: Implication for schools and National Development. Hence, the following Focus Group Discussion Questions (FGDQ) guided the study: Are you aware of cyber-crime? Do you think scammers are in your school? and Do you think some students used e-fraud to generate school fees and others.

Historical Assessment of Cybercrime in Nigeria

The origin of cyber crime that is the very first instance, in which someone committed a crime across a computer network, is impossible to know. What is possible to know is the first major attack on a digital network which can then be used as a reference point of event in the evolution of cyber based crimes.

In 1971, John Draper, a phone phreak, discovered a whistle which produced the same tones as telephone switching computers of the time. Phone phreak is a term used to describe computer programmers obsessed with phone networks, the basis of modern day computer networking. He built a "blue box" with the whistle that allowed him to make free long distance phone calls, and then published instruction on how to make it. With this development, the instances of wire fraud rose significantly. Again in**1973,** a teller at a local New York bank used a computer to embezzle over $2 million dollars (https://.le-vpn.com/history-cyber-crime-origin-evolution). **It was in 1978** that the first electronic bulletin board system came online and quickly became a preferred method of communication for the cyber world. It allowed fast, free exchange of knowledge including tips and tricks for hacking into computer networks. **In1981,** Ian Murphy, popularly known as Captain Zap to his fans, was the first person convicted of a cyber crime. He was alleged to have hacked into the AT&T network and changed the internal clock to charge off-hours rates at peak times. He received 1,000 hours of community service and 2.5 years of probation, a mere slap on the wrist compared to today's penalties, and was the inspiration for the movie *Sneakers*.

Again in1982 , Elk Cloner, a virus, was written as a joke by a 15 year old kid. The said various is considered as one of the first known viruses to leave its original operating system and spread in the "wild". It attacked Apple II operating systems and spread by floppy disk. Hacking became known in 1983 when movie War Games was released. The movie depicts a teenage boy who hacks into a government computer system through a back door and nearly caused the world to World War III. **Precisely in 1988,** Robert T. Morris who was. a graduate student at Cornell, released a self-replicating worm. The worm was said to have infected more than 600,000 networked computers. The first large-scale case of ransom ware is reported in 1989. The virus once downloaded, held computer data hostage for $500(https://.le-vpn.com/history-cyber-crime-origin-evolution). **In1993,** Kevin Paulson was caught and convicted for the offence of hacking into the phone systems. He took control of all phone lines going into an LA radio station in order to guarantee winning a call-in contest. At one point he was featured on America's Most Wanted, when the phone lines for that show went mysteriously silent. When the FBI began their search he went on the run but was eventually caught. He was sentenced to 5 years in Federal penitentiary and was the first to have a ban on Internet use included in his sentence.

It was in 1994 that the World Wide Web was launched, allowing black hat hackers to move their product info from the old bulletin board systems to their very own websites. A student in the UK used the information to hack into Korea's nuclear program, NASA and other US agencies using only a Commodore Amiga personal computer and a "blue boxing" program found online. Shortly after, sometime in **1995,** Macro-viruses appear. Macro-viruses are viruses written in computer languages embedded within applications. These macros run when the application is opened, such as word processing or spreadsheet documents, and are an easy way for hackers to deliver malware. This is why opening unknown email attachments can be very risky. Macro-viruses are still hard to detect and are a leading cause of computer infection.

In 1996 ,CIA Director John Deutsch testifies to Congress that foreign based organized crime rings were actively trying to hack US government and corporate networks. The US GAO announced that its files had been attacked by hackers at least 650,000 times, and that at least 60% of them were successful. **Worse still, in 1999** a Melissa Virus was released. It became the most virulent computer infection to date and results in one of the first convictions for someone writing malware. The Melissa Virus was a macro-virus with the intention of taking over email accounts and sending out mass-mailings. The virus writer was accused of causing more than $80 million in damages to computer networks.

Cyber crime really began to take off in the early 2,000's when social media came to life. The surge of people putting all the information they could into a profile database created a flood of personal information and the rise of ID theft. Thieves used the information in a number of ways including accessing bank accounts, setting up credit cards or other financial fraud. The number and types of online attacks increase exponentially.The latest wave is the establishment of a global criminal industry totaling nearly a half-trillion dollars annually. These criminals operate in gangs, use well-established methods and target anything and everyone with a presence on the web.

Specifically in 2002, Shadow Crew's website was launched. The website was a message board and forum for black hat hackers. Members could post, share and learn how to commit a multitude of cyber crimes and avoid capture. The site lasted for 2 years before being shut down by the Secret Service. 28 people were arrested in the US and 6 other countries ((https://.le-vpn.com/history-cyber-crime-origin-evolution). The instances of hacking, data theft and malware infections skyrockets became so rampant in 2007. Currently, the number of records stolen, machines infected rise into millions as well as the amount of damages caused into billions. The Chinese government is allegedly most accused of hacking into US and other governmental systems.

Conceptual Clarification

Cybercrime in Nigeria

Cybercrime is a very popular crime in Nigeria. Cybercriminals in Nigeria are notorious for luring people across the planet into fraudulent scams via spam mails, cash-laundering e-mails, and cleverly designed but pretend company partnership offers. Criminals involved in the advance fee fraud schemes (419) known as "yahoo yahoo" are popularly referred to as "yahoo boys" in Nigeria. Yahoo yahoo is the most popular local name for cybercrime in Nigeria. It usually involves the use of email, particularly through a Yahoo address or yahoo messenger to con unsuspecting victims. The nation has therefore carved a niche for herself as the source of what is now generally referred to as "419" mails named after Section 419 of the Nigerian Criminal Code (Capp 777 of 1990) that prohibits advance fee fraud.

The "yahoo boys" use various methods in getting their victims. Many of these fraudsters patronize cyber cafes, browsing the internet all night, sending scam mails to unsuspecting victims. Many foreigners, especially females, who are seeking for spouses via the Internet have fallen victim of the "yahoo boys". They pretend to be ready to go into a lasting relationship with these women and subsequently start to exploit them. Some of them get their victims to help in procuring travel documents to where they reside or even to assist in getting residential permits for them. Once they have been able to achieve their aims, they stop communicating with the victim and move on to another target (Adesina, 2012).

In other instances, the scammers use stories of severe life circumstances, tragedies, family deaths, personal injuries or other hardships to keep their victims concerned and involved in their schemes. They also ask victims to send money to help overcome alleged financial hardships. Many of the victims just lick their wounds and carry on life, but some of the very bitter victims report to the appropriate authorities who often apprehend and prosecute the suspects. The situation is worsened by the fact that several non-Nigerians apprehended for cybercrimes most often claim to be Nigerians before they are thoroughly investigated and their country of origin established. Demonstrating the gravity of the problem of cybercrime in the country, in 2007, a young Nigerian musician, Olumide Adegbolu (also known as Olu Maintain) released a hit song called "Yahooze". The song, which sparked a lot of controversies, speaks of a flashy lifestyle, fancy trips and expensive drinks, if the songster is able to "hammer" (obtain) 1 million dollars and coverts it into Naira (Nigerian currency). Critics argued that the song was a glorification of internet fraud or "Yahoo Yahoo", pointing out that for a young man

to think of living such a life style if he gets such a huge amount of money, he must be a scammer. This has been vehemently denied by Olu Maintain himself claiming that the song was just a reflection of his rise to fame and the change money has made to his life.

The song and the whole controversy that trailed it reflects the current trend of thinking of many Nigerian youth. The quest to possess and ride flashy cars and live frivolous lifestyles have lured many Nigerian youth into the "yahoo yahoo" business. It is not unusual to enter a cybercafé and find that most of the people there are (mainly) boys in their 20's or early 30's who are browsing the internet in search of potential victims. There is even what is called "night browsing" where, for a fee, they stay on the internet all through the night to carry out their businesses. The boys often team up to practice their businesses in other to be able to get ideas from each other. Also, as seen in Figure 1 below, many of them also have laptops that they use to perpetrate this crime.

A Typical Yahoo Yahoo Operation Source:

However, in recent times, because of some stringent measures put in place by many financial institutions and various organizations that do online transactions, the cybercriminals in Nigeria apparently suffered a setback to national development. To this end, the more desperate among them has had to resort to spiritual means to enhance their businesses. This is referred to as "Yahoo Plus". Yahoo plus is an advanced form of yahoo yahoo whereby the "yahoo boys" employs traditional spiritual means like voodoo or juju to hypnotize their victims into doing their bidding and parting with whatever amount of money they request for. The yahoo boys indulge in occultic ritual practices to enhance their potential to defraud people. It involves employing traditional spiritual means like voodoo or juju in ensuring that the cybercriminal hypnotizes his victims and thereby brighten the swindler's chances of getting his victims hypnotised. Once this is successfully done, the victim is guaranteed to keep remitting money from wherever he or she is in the world. There are various strategies deployed in achieving this feat. The yahoo boy approaches a spiritualist or diviner who consults, the "oracle" or the "gods". He is then given diverse options of rituals to perform. These include sleeping in a coffin for certain numbers of days, sleeping in the cemetery, bringing body parts. In other words, he kidnaps a victim, kills him/her and extracts the body part needed. Some are even told to sleep with virgins as part of the rituals. Most often, young girls are kidnapped and raped and sometimes killed by these ambitious people.

Other forms of rituals performed include sleeping with pregnant women or mad women and sometimes, the yahoo boy may be told not to take his bath for days or months as doing so may have terrible repercussions.

Another popular "yahoo" crime in Nigeria is phishing. Phishing is an attack that typically involves sending an email to a victim that looks to the unsuspecting recipient as if it comes from a legitimate source, for instance, a bank. For phishes, an email is sent asking the victim to verify personal information through a link to a fraudulent web page. Once that is provided, the hacker can access the victim's financial information. According to Richards (2016), the year 2015 recorded high number of phishing emails from suspected cyber criminals in Nigeria, peaking when the Central Bank of Nigeria (CBN) announced deadline for Bank Verification Number (BVN). Cyber criminals swamped unwary bank customers with phish emails to warn them that their accounts were about to be blocked and consequently steal their credentials once they supply their details.

Reasons for Cybercrime

When the internet was developed, the founding fathers of internet hardly had any inclination that internet could be misused for criminal activities. Today, there are many disturbing things happening in the cyberspace (Chiemeke, 2012). However, scholars have attributed the causes of cybercrime in the world to the

following: that the causes of cybercrime include unemployment, negative role model, lack of adequate policing facilities and social gratification (Okoro, 2010). According to him, all these reasons serve to facilitate cybercrime in most of the world. The widespread of corruption, harsh economic climate, high underemployment, disregard for the rule of law, lack of transparency and accountability in governance are the main causes of cybercrime in most countries of the world Okoro,2010). Cybercrime could be associated with two causes which are the primary and secondary. The primary causes include the prevalence of poverty and weak educational system (Bolt, 2008). The secondary cause can be trace to greed, corruption and get rich quick syndrome. The high level of corruption and the spread of poverty is seen as the main cause of cybercrime in Nigeria among university undergradua (Ayantokun, 2006)

Cybercrime and its effect on Nigeria National Development

The proliferation of cybercrime has negative impact on Nigeria. According to the National Security Adviser (NSA), Maj-Gen. Babagana Munguno (rtd), the 2014 Annual report of the Nigeria Deposit Insurance Corporation (NDIC), shows that, between year 2013 and 2014, fraud on e-payment platform of the Nigerian banking sector increased by 183%. Also, a report published in 2014 by the Centre for Strategic and International Studies, UK, estimated the annual cost of cybercrime to Nigeria at about 0.08% of our GDP, representing about N127 billion (Iroegbu, 2016). Apart from economic loss, cybercrime has brought disrepute to Nigeria from all over the world. For instance, in India, it was claimed that about 90% of foreign nationals arrested for cybercrimes in Hyderabad city since September 2015 were Nigerians. According to the source, of 67 foreigners arrested for online fraud, 60 were from Nigeria, five from Cameroon, and the other two were South African nationals. There are three basic types of online frauds through which Nigerians perpetrate the crime—lottery, jobs, and matrimonial scams (Lasania, 2016).

Fundamentally, Nigerians are treated with suspicion in business dealings. As pointed out by Ribadu (2007):

Cybercrime is depressing trade and investor confidence in our economy and to that extent it is a present and clear danger to our national security and the prosperity of our citizens. Indeed, of all the grand corruption perpetrated daily in our communities, most are of the nature of cybercrime executed through the agencies of computer and internet fraud, mail scam, credit card fraud, bankruptcy fraud, insurance fraud, government fraud, tax evasion, financial fraud, securities fraud, insider trading, bribery, kickbacks, counterfeiting, laundering, embezzlement, as well as economic and copyright/trade secret theft.

The situation is such that international financial institutions now view paper-based Nigerian financial instruments with scepticism. Nigerian bank drafts and checks are not viable international financial instruments. Nigerian Internet Service Providers (ISPs) and email providers are already being black-listed in e-mail blocking blacklist systems across the Internet. Also, some companies are blocking entire Internet network segments and traffic that originate from Nigeria. Newer and more sophisticated technologies are emerging that will make it easier to discriminate and isolate Nigerian e-mail traffic (Chawki, 2009).

Legislation on Cybercrime in Nigeria

Having good legislation in place is one of the major steps in curbing cybercrime. In 2004, the Nigerian government established the Nigerian Cybercrime Working Group comprising representatives from government and the private sector to develop legislation on cybercrime. Furthermore, in 2007, the government established the Directorate for Cyber Security (DfCS), which is an agency responsible for responding to security issues associated with growing usage of internet and other information and communication technologies (ICTs) in the country. It was provided with a funding of N1.2 billion (approximately USD9.8 million using 2007 exchange rates) to carry out its mission. Apart from these initiatives, there are general laws that are not specifically related to cybercrime but are being enforced to deal with the crime. Some of these laws, which are examined below, are: the Nigeria criminal code (1990), Economic and Financial Crimes Commission (EFCC) (Establishment) Act 2004, and the Advance Fee Fraud and other Related Offences Act 2006.

Nigeria Criminal Code Act 1990

The Criminal Code Act of 1990 (Laws of the Federation of Nigeria, 1990) criminalizes any type of stealing of funds in whatever form, an offence punishable under the Act. Even though cybercrime is not mentioned in the Act, it is a type of stealing punishable under the criminal code. Chapter 38 of the Act deals with "obtaining Property by false pretences—Cheating." The specific provisions relating to cybercrime is section 419, while section 418 gave a definition of what constitutes an offence under the Act. Section 418 states that:

Any representation made by words, writing, or conduct, of a matter of fact, either past or present, which representation is false in fact, and which the person making it knows to be false or does not believe to be true, is a false pretence.

While section 419 states:

Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years.

The Economic and Financial Crime Commission Act, 2004

The Economic and Financial Crime Commission Act (Laws of the Federation of Nigeria, 2004, as amended) provides the legal framework for the establishment of the Commission. This Act repeals the Economic and Financial Crimes Commission (EFCC) (Establishment) Act 2002. Some of the major responsibilities of the Commission, according to part 2 of the Act, include:

1. The investigation of all financial crimes, including advance fee fraud, money laundering, counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, contract scam, etc.;
2. The coordination and enforcement of all laws against economic and financial crimes laws and enforcement functions conferred on any other person or authority;
3. The examination and investigation of al1 reported cases of economic and financial crimes with a view to identifying individuals, corporate bodies, or groups involved;
4. Undertaking research and similar works with a view to determining the manifestation, extent, magnitude, and effects of economic and financial crimes and advising government on appropriate intervention measures for combating same;
5. Taking charge of, supervising, controlling, coordinating all the responsibilities, functions, and activities relating to the current investigation and prosecution of all offences connected with or relating to economic and financial crimes, in consultation with the Attorney- General of the Federation;
6. The coordination of all investigating units for existing economic and financial crimes, in Nigeria;
7. The Commission is further charged with the responsibility of enforcing the provisions of the Money Laundering Act 1995; the Advance Fee Fraud and Other Fraud-Related Offences Act 1995 ; the Failed Banks (Recovery of Debts) and Financial Malpractices in Banks Act 1994, as amended; the Banks and other Financial Institutions Act 1991, as amended; and Miscellaneous Offences Act (EFCC, 2004) .

Advance Fee Fraud and Related Offences Act 2006

According to Section 23 of the advance fee fraud Act (Laws of the Federation of Nigeria, 2006):
False pretence means a representation, whether deliberate or reckless, made by word, in writing or by conduct, of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe to be true.
Section 383 sub-section 1 of the Nigerian Criminal Code states: "A person who fraudulently takes anything capable of being stolen, or fraudulently converts to his own use or to the use of any other person anything capable of being stolen, is said to steal that thing". Advance Fee Fraud and Other Fraud Related Offences Act 2006 deals with internet crime issues, however, it only covers the regulation of internet service providers and cybercafés, it does not deal with the broad spectrum of computer misuse and cybercrimes.

Cybercrimes Act of 2015

All the above legislation has proven ineffective in curbing cybercrime as it is on the increase. In a bid to put in place stronger legal framework to curb cybercrime, a revision of the existing cybercrime legislation was put forward by the Government in September 2008. The bill titled "A Bill for an Act to Provide for the Prohibition of Electronic Fraud in all Electronic Transactions in Nigeria and for other Related Matters," passed second reading in November 2012 at the Senate. In May 2015, the cybercrime bill was signed into law, properly defining the act as unlawful with penalties attached to any disobedience of the law. The Act, known as the Cybercrimes (Prohibition, Prevention etc.) Act 2015 creates a legal, regulatory and institutional framework for the prohibition, prevention, detection, investigation and prosecution of cybercrimes and for other related matters. Particularly, the Act engenders a platform for cyber security and in turn, ensures the protection of computer systems and networks, electronic.

Concept of National Development

For a better understanding of National Development, it is fundamental to briefly explain development. Development is a process that creates growth, progress, positive change or the addition of physical, economic, environmental, social and demographic components. It is a dynamic process in that it involves a change from one state or condition to another. Ideally, such a change is a positive one – an improvement of some sort (for instance, an improvement in maternal health) (www.soas.ac.uk). Gboyegu(2003) captures development as an idea that embodies all attempt to improve the condition of human existence in all ramifications. It implies

improvement in material wellbeing of all citizens not the most powerful and rich alone, in a sustainable way such that today's consumption does not imperil the future. It also demands that poverty and inequality of access to the good things of life be removed or drastically reduced. It seeks to improve personal physical security and livelihood and expansion of life chances.

Development is a process that creates growth, progress, positive change or the addition of physical, economic, environmental, social and demographic components. In this sense, the purpose of development is a rise in the level and quality of life of the population, and the creation or expansion of local regional income and employment opportunities, without damaging the resources of the environment. In brief, development can be seen as a tool enabling people to reach the highest level of their ability, through granting freedom of action, i.e, freedom of economic, social and family actions (sid-israel.org). Having conceptualized development, National development is a comprehensive term which include improvement in living standard of the people, increase in per capita income, providing social amenities like quality education, medical care, potable water, transportation, electricity e.t.c to the citizens of the country. The basic idea of National development is the ability of a country to improve the social welfare of the people through provision of these basic amenities(www.studyrankersonline.com).

National development is an economic development. Economic development quantitatively means a higher GDP per capita. Since GDP is a measure of consumption, a higher consumption means that the people of the country eat better food, live in better homes, live in in a better environment with clean and pure air and water. More importantly, they have assurance of leading a better life in the future (Sandeepan, 2018). Zack (2019) sees National development as the change in growth and development, which include social, cultural and economic change. It is the ability of a country to improve the social welfare of the people characterize by the overall development of a collective socio-economic, political as well as religious advancement of a country.

Tolu and Abe (2011) describes National development as the overall development or a collective socio-economic, political as well as religious advancement of a country or a Nation. This is best achieved through development planning which can be described as the country's collection of strategies mapped out by the government. In spite of series of development strategies put in place by successive government in Nigeria with good intentions to make possible realistic dreams of National development, all attempts to generate meaningful development proved futile due to; lack of good governance, high level of corruption and indiscipline, the mono economic base of the country and other emerging issues in the country notably: kidnapping, Terrorism, Boko Haram and Cybercrime. The aforementioned issues are unfriendly to national development; hence the choice of this topic

Theoretical underpinning of cybercrime

Cybercrime and criminological theory on the role of computers and internet as an interestingly pivoted function in daily life, making it virtually essential to understand the dynamics of cybercrime and those victimised by it (Thomas, 2013). The anthology cybercrime and criminology theory: first readings on hacking, piracy, theft, and harassment explore the predators for participation in various forms of cybercrime and deviance, from common problems like media piracy to more distinct offences such as computer hacking. Most criminological theories were developed to account for street crimes, so it is unclear how these methods may apply to virtual offending. This approach provides critical insight into the utility of multiple theories to account for cybercrime. Cybercrime and criminological theory give direct insights into the rates and prevalence of cybercrime offences using sets of data from population across the globe. It offers readers a basic understanding of, and appreciation for various forms of cybercrime and outlines prospective predator of both offending and victimisation. This theory is relevant to this study because it has revealed that computers and internet are used to commit fraud, which they use to hack to do piracy, theft, and harassment to individual and banks.

It is also necessary to note that students use handsets to commit examination malpractices. This theory can be applied because it will help to address the issue of crimes at various levels ranging from community and socialisation influence theories. Theoretical explanations of a crime are essential for several reasons. Not only do they help society to know how and why crime occurs but they can also be useful in helping to prognosticate future criminal behaviour. Theories of crime are also of help in attempting to prepare successful rehabilitative interventions for offenders as well as developing crime blocking strategies that have the best chance of success in a giving society. Differential association theory was propounded (Folashade, Okeshola & Abimbola, 2013). He coined the phrase (differential association) to address the issue of how people learn deviance. This theory explains deviance regarding the individual social relationships. The theory sees the environment as playing a major role in deciding which norms people learn to violate. Specifically, people within a particular reference group provide norms of conformity and deviance. This theory is significant because it puts an individual social environment into context as a means to explain why some individual engage in criminal behaviour. The theory has the following assumptions, which is related to this study;

1. Criminal behaviour is learned: this means that criminal behaviour is not inherited as such the person who is not already trained in crime does not invent criminal behaviour. This assumption proposes that individuals are inherently good and only turn towards deviant behaviour as a result of learning the behaviour.
2. Criminal behaviour is learned in interaction with other persons in the process of communication. An individual is influenced to participate in criminal behaviour through watching and interacting with other individuals who are engaging in the criminal behaviour (Folashade, Okeshola & Abimbola, 2013).
3. The principal part of the learning of criminal behaviour occurs within intimate personal groups this would be any group that has a significant influence over them such as their family or close friends this factor makes a great deal of sense. Since the process of socialisation and growing up is heavily influenced by the groups of people that an individual is a part of. Most families try to institute a positive influence on a member of their own, however, if a juvenile comes from a family that is broken and develop strong emotional ties with friends engaged in deviant behaviour then this is likely also to drive them into the same deviant behaviour.
4. When criminal behaviour is learnt, the learning includes techniques of committing the crime, which is 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 the actions. For example, an individual from a disadvantaged background may rationalize cybercrime as taking from those who have wealth to make things fair, among others. This theory was propounded to help explain white-collar crime, fits in with those who violate or commit cybercrime.

Review of Empirical Studies

Igba, Elizabeth and Aja (2018) examine cybercrime among university undergraduates: implications on their academic achievement. The results show among others that undergraduates perceive cybercrime as a tool for personal development. It was observed that much needed to be done to ensure, safe, secure, and trustworthy network environment. This implies that undergraduates should be made to imbibe value re-orientation in order to be more useful in life. The result should be an eye opener to both students and lecturers on the more positive ways of benefiting from the globalised world through internet services without necessarily abusing it.

Research Method

Research Design

A mixed design of descriptive survey research was used for this study. Describe survey research as research that involves the collection of data from a sample that has been chosen to represent a population to which the findings of the data analysis can be generalized. Primary data was generated using Focus Group Discussion Questions (FGDQ) using 200 undergraduate students of the Nasarawa State University Keffi based on cybercrime and the secondary data was generated based on the existing electronic materials.

Population and Sample of the study

The population for the survey constituted of all the students of the Nasarawa State University Keffi where 200 students were selected using purposeful sampling technique selected from 5 faculties.

Instrument for the Data Collection

The instrument used for data collection was a FGDQ. They were presented in a modified 2-point rating scale thus: Agree (SA) = 2 points, Disagree (D) = 1 point.

Validation and Reliability of the Instrument

The FGDQ was vetted for face and content validity by two experts which yielded 0.78 validity index. In determining the reliability of the FGDQ, Split-half test method was used, and scores were computed using Cronbach alpha which yielded 0.76 reliability coefficient.

Method of Data Collection and Analysis

Focus Group Discussion Questions (FGDQ) was administered to the respondents by the researcher using FGD method. The primary data collected were analysed using the frequency and percentages and the results are presented in Table below.

Table: Students Responses toward Cybercrime in Schools

Questions Descriptions	**Agree**	**Disagree**	**Decision**
Are you aware of cyber-crime?	**175** (87.5%)	**25**(12.5%)	Accept
Do you think scammers are in your school?	**158**(79.0%)	**42**(21.0 %.)	Accept
Do you think some students used e-fraud to generate school fees and others	**170** (85.0%)	**30**(15.0%)	Accept
Pooled %	**168**(84.0%)	**32**(16.0%)	Accept

Sources: *Field Work: Moga, Galle & Rukayyat (2021)*

Table 1 shows response of students toward cybercrime in Nigerian schools. Out of 200 students represent 100%, 175 represents 87.5% agreed that they are aware of cybercrime while the other 25 students' represents 12.5% disagreed. In the same way, 158 students' represents 79.0% agreed that there were scammers in their school and lastly, 170 students' represents 85.0% agreed that some students are using school portal for e-fraud to generate school fee, results to gain advantage. The pooled percentage of students responses on agreed 168(84%) and disagree 32(16%) are dichotomously presented in bar chart below.

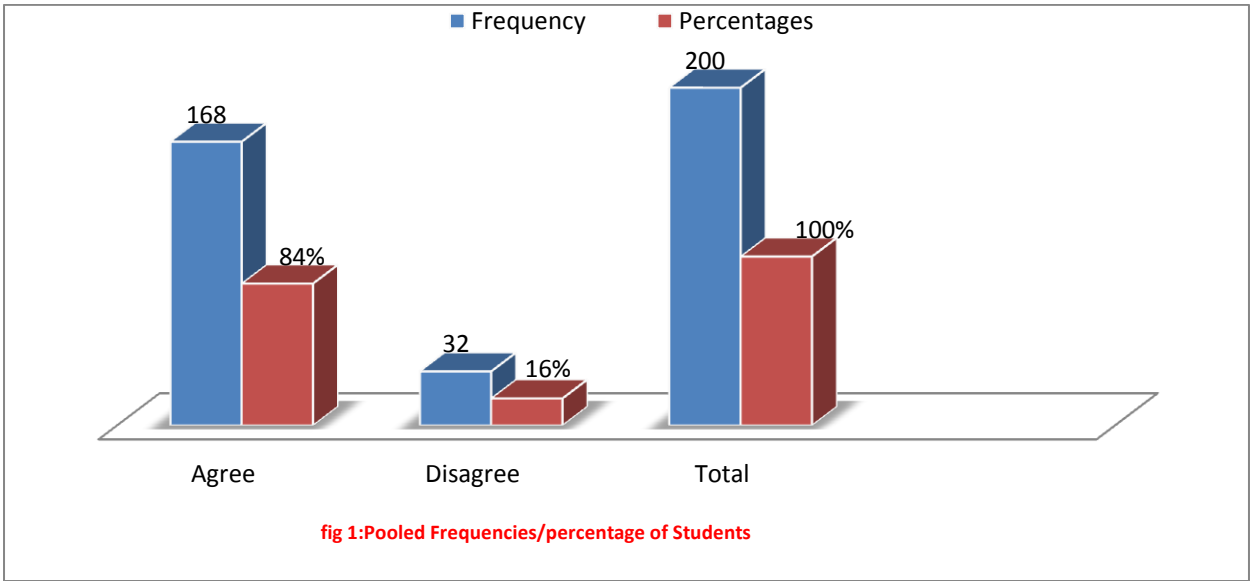

fig 1:Pooled Frequencies/percentage of Students

II. DISCUSSION OF FINDINGS

Table 1 shows response of students toward cybercrime in Nigerian schools. Out of 200 students represent 100%, 175 represents 87.5% agreed that they are aware of cybercrime while the other 25 students' represents 12.5% disagreed. In the same way, 158 students' represents 79.0% agreed that there were scammers in their school and lastly, 170 students' represents 85.0% agreed that some students are using school portal for e-fraud to generate school fee, results to gain advantage. The pooled percentage of students responses on agreed 168(84%) and disagree 32(16%) are dichotomously. This finding is in agreemenIthat of gba, Elizabeth and Aja (2018) results show among others that undergraduates perceive cybercrime as a tool for personal development. It was observed that much needed to be done to ensure, safe, secure, and trustworthy network environment. This implies that undergraduates should be made to imbibe value re-orientation in order to be more useful in life. The result should be an eye opener to both students and lecturers on the more positive ways of benefiting from the globalised world through internet services without necessarily abusing it. Further findings revealed that 84% of the students agreed that cybercrime exist highly among students, such as Hacking of Face-Book Page or WhatsApp Page of someone in disguised using it for devious acts, Manipulating students school fees and semester results are some of the cybercrimes in the school system. Further results of the secondary sources revealed related cybercrime to include; quest for wealth, Poor implementation of cybercrime laws, and corruption among others.

III. CONCLUSION

The paper upholds that cybercrime is an offence that involves using the internet or computer to carry out illegal activities for financial or personal gains. Such illegal activities include identity theft and social engineering. In achieving their aim, cyber criminals use malware or a group of Zombie computers known as '**'botnet''** which often results in network being inaccessible to normal users.

Urbanization, poor implementation of cybercrime laws, unemployment, corruption, poverty, proliferation of cyber cafes and the porous nature of internet, negative role models and greed were identified as causes of cybercrime in Nigeria. The paper notes that the increasing rate of cybercrime in Nigeria affects National development in different ramifications such as; it dents Nigeria's image internationally, Nigerian citizens face reputational risk as they are being perceived internationally as potential scammers, it makes business environment difficult for start-ups and small and medium sized enterprises just as it leads to loss of intellectual property or personal information.

Since cyber criminals persistently look for ways of using the computer illegally for their personal gains, the paper advocated for the proper setting of passwords, safeguarding Personal Identification Number(PIN), the

use of in Encryption, Network account, Biometric Security Techniques as ways of mitigating cybercrime related cases in Nigeria.

Against the backdrop that the youths are the most vulnerable in cybercrime related cases Nigeria due to unemployment, the paper suggests in strong terms that Nigerian government should do more in terms of creating job opportunities or platforms for youths to acquire entrepreneurial skills to build a career for themselves. This is hoped to ultimately reduce the level of cybercrime related cases in Nigeria.

IV. SUGGESTIONS

In order to ensure that Nigeria is free from the shackles of cybercrime, the following suggestions are made.

1. Nigerian Government should enact stringent laws against cybercrime and ensure that violators are punished accordingly without discrimination.
2. Seminars and workshops should be organized regularly to sensitize the public on the need to keep safe their personal information.
3. Nigerian government should borrow a new leaf from the initiative employed by other countries of the world in combating cybercrime such as the Anti-Scam Centre set up by the Singapore Police in collaboration with the three major banks in that country which had successfully disrupted operations of scammers by impeding fund transfers.
4. Financial institutions and individuals should ensure proper and constant use of firewalls to prevent attacks and filter malware or suspicious malicious codes.
5. Personal Identification Number (PIN), Bank account number and e-mail access should never be shared to unknown persons as systems are fraught with security issues.
6. Government should do more in terms of creating job opportunities or platforms where youths can acquire entrepreneurial skills to build a career for themselves as this is hoped to significantly drop cybercrime related cases in the country.

REFERENCES

[1]. Ayantokun, S. G, (2006). The negative impact of globalization on Nigeria. *International Journal of Humanities and Social Science, 2*(15), 193-201.

[2]. Bolt, S. L. (2008) "Security in Computing (3rd) Upper Saddle River: Prentice Hall PTR, 2008.

[3]. Chawki, M. (2009). *Nigeria tackles advance fee fraud*. Retrieved from http://www2.warwick.ac.uk/fac/soc/law/elj/ jilt/2009_1/chawki/chawki.pdf

[4]. Chiemeke, B. S. (2012) "a security beget insecurity? Security and crime prevention awareness and fear of burglary among university students," the East Midlands. Security Journal, 22(1), 3-23. (2012).

[5]. Chiemeke,U (2012) Cyber-crimes and the boundaries of domestic legal responses: Case for an Inclusionary Framework for Africa. *Journal of Information, Law and Technology (JILT), 1*, 1-18.

[6]. Clough, J. (2010). *Principles of cybercrime*. Cambridge: Cambridge University Press.

[7]. Folashade N Okeshol, B & Abimbola, D (2013). Concepts, measurement and causes of poverty. *CBN Economic & Financial Review, 39*(4), 35-45

[8]. Folashade, B. O. & Abimbola K. A. (2013), "The Nature, Causes and consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria," American International Journal of Contemporary Research Vol. 3 No. 9; September 2013.

[9]. Folashade, B., Okeshola, E., & Abimbolam, K. A.(2013), "The Nature, Causes and consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria," American International Journal of Contemporary Research Vol. 3 No. 9; September 2013.

[10]. Igba, D. I.; Elizabeth, C. I.; and Aja, S. N. (2018) examine cybercrime among university undergraduates: implications on their academic achievement. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 2 (2018) pp. 1144-1154 © Research India Publications. http://www.ripublication.com

[11]. Igba, D. I.; Elizabeth, C. I.; and Aja, S. N. (2018) examine cybercrime among university undergraduates: implications on their academic achievement. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 2 (2018) pp. 1144-1154 © Research India Publications. http://www.ripublication.com

[12]. Iroegbu, S. (2016). Nigeria loses over N127bn annually through cybercrime. Retrieved from http://www.thisdaylive.com/ index.php/2016/04/19/nigeria-loses-over-n127bn-annually-through-cybercrime

[13]. Kshetri, N. (2013). *Cybercrime and cybersecurity in the global south*. Hampshire: Palgrave Macmillan

[14]. Lasania, Y. Y. (2016). 90 per cent of foreigners involved in cybercrime are Nigerians. Retrieved from http://www. thehindu.com/news/cities/Hyderabad/90-per-cent-of-foreigners-involved-in-cyber-crime-are-Nigerians/ article14572630.ece

[15]. Okoro, E (2010). *Nigeria comes 3rd in global cybercrimes survey*. Retrieved from http://www.abujacity.com/abuja_ and_beyond/2010/11/nigeria-comes-3rd-in-global-cybercrimes-survey-.html

[16]. Okoro, E. E. (2010). "the Normalcy of Vice: the Public Sector and Corruption in Nigeria, in C.O.T. Ugwu (Ed)) Corruption in Nigeria: Critical Perspectives," Nsukks: Chuka Educational Publishers, 2010

[17]. Ribadu, N. (2007). *Cyber-crime and commercial fraud: A Nigerian perspective*. Presented at the Congress Celebrating the Fortieth Annual Session of the UNCITRAL (United Nations Commission On International Trade Law), Vienna, Austria, 9-12 July. Retrieved from http://www.cnudmi.org/ pdf/english/congress/Ribadu_Ibrahim.pdf

[18]. Rishi, R., & Gupta, V. (2015). *Strategic national measures to combat cybercrime: Perspective and learning for India*. Retrieved from http://www.ey.com/Publication/ vwLUAssets/ey-strategic-national-measures-to-combat-cybercrime/$FILE/ey-strategic-national-measures-to-combat-cybercrime.pdf

[19]. Sandeepan, B. (2018). What is National Development? Retrieved fromwww.quora.com>what-is-national

[20]. Thomas, D., & Loader, B. (2000). Introduction—cybercrime: Law enforcement, security and surveillance in the information age. T

[21]. Thomas, J. H.(2013) "Cybercrime and criminological theory: Fundamental readings on hacking, piracy, theft, and harassment," (first edition) ISBN: 978-1-60927-496-2, P. 228 @ 2013 PMid:23700684

[22]. Tolu, L. & Abe, O.(2011). National Development in Nigeria: Issues, challenges and prospects. *Journal of Public Administration and Policy Research, Vol.3(9).* Retrieved fromhttp://www.academicjournals.org/

[23]. Zach, V.W.(2019). Nigerian Home Videos, Cultural Values and National Development: Select Review. *Benue Journal of Media Arts and Literary Studies, Vol.2.I*SSN:2672-4928