Sapientia Global Journal of Arts, Humanities and Development Studies (SGOJAHDS), Vol.4 No.1 March, 2021; p.g. 257 – 268; ISSN: 2695-2319 (Print); ISSN: 2695-2327 (Online)

CYBERCRIME ORDEAL IN NIGERIA SECURITY FIRMAMENT

AFOLABI MUYIWA B. (PhD)
Department of Intelligence and Security Studies,
College of Social & Management Sciences
Afe Babalola University, Ado – Ekiti
afobam1840@gmail.com +2348166903787

&

ESOSO AGBOR JULIANAH
Department of Sociology,
College of Social & Management Sciences
Afe Babalola University, Ado – Ekiti
julianahumani@gmail.com, +2348061534305

Abstract

Cybercrime involves making use of computers or other Information Communication Technology devices as well as the internet by individuals to commit crimes in cyberspace. This has caused monumental damage to the image of the country in spite of the fight against corruption and unending efforts of the present administration to reposition the country in the committee of nations in its own style. Some of the numerous types of cybercrimes perpetrated in Nigeria include fraud, identity theft, phishing, hacking, and different categories of cyber fraud. This paper concisely examines the nature of cybercrime in Nigeria and how the crime is being committed by a vast majority of Nigerian youths. The causes of cybercrime in the nation such as poverty, peer pressure, unemployment, amongst other factors are examined in the paper. With the growing rates of cybercrime in the country, cyber and human security may be gravely threatened. The paper concluded that, there may be upsurge in cybercrime rate if the menace is not rigorously addressed with the level of unemployment and poverty in the country. There is a need for cybercrime to be minimized if not diligently dealt with by the government, its law enforcement, security agencies and other professional bodies. The paper recommended that government security agencies need to keep up with technological and security advancements. It will always be a losing battle if security professionals are miles behind the cybercriminals. Hence, issues of unemployment, poverty, and re-orientation of the citizenry should be prioritized beyond mere propaganda and politicization.

Keywords: **Cybercrime, Information Communication Technology, cybercriminals.**

Introduction

Cybercrime perhaps has become the most evolving aspect of crime in the 21st century. The internet has made the dimensions of cybercrime diverse. The extent to which this menace has grown is quite devastating. The way cybercrime is perceived varies as it constitutes a variety of issues. Cybercrime has become very rampant in continents all over the world, including

Africa. The rate at which cybercrimes are committed in Africa is quite alarming. Cybercrime issues have become high-profile, especially those that are related to hacking, copyright infringement, child pornography, and child grooming (Pitts, 2017).

Cybercrime is being used interchangeably with other computer-related crime. Thus, one might speak of 'cybercrime', 'high tech crime', 'computer crime', 'technology crime', 'digital crime', and 'IT crime' and be discussing the same and/or different concepts, respectively. Nevertheless, cybercrime has been described as any activity in which computers or networks are a tool, a target, or a place of criminal activity. But the problem with this definition is that it is too broad. For example, if one uses a keyboard to commit battery, it does not mean that a cybercriminal act has been committed. Also, according to the National Crime Prevention Council (2015), cybercrime is any activity involving computers and networks. This definition is not very explicit because 'any activity' could also include a legal activity (Crime Prevention Council, 2015). Cybercrimes are offences that are committed against an individual or group 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 the internet and mobile phones. Such crimes may threaten the nation's security and financial health (Folashade et al, 2015).

Nature of Cybercrime in Nigeria

Cybercrime has been an eluding factor in the cyberspace transactions in Nigeria, where cybercrimes and computer-related crimes are endemic. With the integration of computer technology as a global issue, the economy of most nations in the world is accessible through the use of Information communication and technology (Dillon et al, 2016). Cyber Crime constitutes a major threat to Nigeria. As it stands, cybercrimes affect the economy of Nigeria in various sectors. The lack of confidence in the banking sector as a result of the impact of cybercrime is damming on the economy. The impact of cybercrimes on the Nigerian economy is becoming compelling and manifests to many as computer literacy increases, adding that organizations seem to pay less attention to security in contrast to the more technology that these scammers adopt. In Nigeria, organizations are busy adopting information technologies without commensurate investment in information security. This is a predisposition to cybercrime because the Nigerian society is technologically investing its way to cyber insecurity.

With the opportunity opened to the general public in use for various ICT devices, certain high-level crimes are committed and some of the perpetrators of these crimes are referred to as 'Yahoo boys' in Nigeria. They take advantage of cyberspace transactions available on the internet to defraud the unsuspected victims who are mostly foreign transactions in thousands and millions of dollars. Fraudulently, they represent themselves as having particular goods to sell or that they are involved in shipping or a loan scheme. Most of the perpetrators-criminals'/yahoo boys take advantage of some people looking for a spouse through the internet. These criminally minded individuals will discuss with the victims through the internet and they will pretend to be interested and loving. Before the victim realized, the criminals would have succeeded in luring them to send dollars to enable them to facilitate traveling documents (Ehimen and Bola, 2017).

Email scams and spam is other repulsive phenomena among cybercrime, these are ways used to present false financial investment (This Day, 2015).
Nigeria's image is in question and has been tarnished as a result of her citizens' involvement in cybercrime. The criminals send an email that the victim is the named beneficiary to the will of an estranged relative and stands to benefit the estate or the trust fund. Sometimes they used online charity; the criminals send emails to the victims soliciting funds and assistance to charitable organizations that do not exist (Akano, 2016). However, this discussion is not meant to portray Nigeria as the only people that engaged in these types of crimes. Although electronic scam or spam emails are generally believed to be linked to Nigeria, the scam is now prevalent in many other African countries and the targets are usually innocent individuals who could be anywhere in the world. The shift in the act has now extended to text messages, with the increase of use of cell phones, text messages are sent to mobile users to lure the victim into captivity. During their act, a mobile user will receive a text message congratulating the user for winning a certain amount of money in the promo by directing the user to call a particular number to claim the prizes or a package sent from the US to deliver but someone has to pay doorstep delivery or clearing agent fees. The criminals have developed different strategies aimed at luring their victims (Lawanson and Afolabi, 2020; Akano, 2016).

Cybercrime is undoubtedly a contemporary problem in Nigeria. While it continues to expand in magnitude and dimensions globally, awareness of the dynamics and multi-faceted effects of cybercrime seems to be drastically low in Nigeria. This is dangerous to live with, because cybercrime by its nature is evolving and that cybercriminals are becoming more sophisticated in their operations. Besides, the number of Nigerians that are connected to broadband Internet keeps growing beyond limits and absence of efficient law enforcements and security agencies to checkmate the menace is more worrisome. The expanding rate of cybercrime in Nigeria has the capability of wiping out our developmental gains, retarding growth fortunes by many decades, and most importantly affecting the National Security of the nation at large.

Causes of Cybercrime in Nigeria
It has been an issue of debate that most of the categories of cybercrime that are prevalent today are a reflection of crimes that migrated from the physical space to cyberspace (Phillip cited in Olatunde – Kamali, 2020). The debate, therefore, raises the question: why would criminals choose to migrate from the physical space to cyberspace? It should be noted that not all cybercriminals migrated from the physical space to cyberspace. Some crimes emerged after the development of Internet technology. It is this type of crime that Marcum (2014) described as the true cybercrimes. In the same vein, Ndubueze (2013) argues that cyber-induced modernity has led to the emergence of new forms of crime and criminality in Nigeria. Cyberspace crime and criminality are motivated by several factors in Nigeria.

Youths in Nigeria are influenced and fascinated by the internet and its numerous capabilities. Young people are curious by nature and always want to experiment. This curious mindset may lead some intelligent young people with above-average Internet skills to inadvertently engage in deviant and criminal behavior online. The curiosity of Nigerian youths has pushed them to discover many vices that can be committed in cyberspace and one's comfort. Not only are the youths curious and involve in this menace, but the majority of perpetrators are very young (Lawanson and Afolabi, 2020).

One major factor adduced for the rise in various manmade security threats and crimes in Nigeria, most particularly cybercrime is poverty. Brue (2005) defines poverty as a condition in which a person or a family does not have the means to satisfy basic needs for food, clothing, shelter, and transportation. The poverty and crime synergy has long been argued in criminological discourses. Field (1990) posits that economic conditions exert countervailing effects on criminal motivation and criminal opportunity. Human beings strive to satisfy basic needs and when some cannot access the legitimate means for doing so, they may resort to illegitimate means such as cybercrime. Because there are many unemployed youths in Nigeria, there are by extension many poor people in Nigeria. Some of these poor youths to satisfy their physiological needs may find it convenient to engage in cybercrime.

Criminal Administration System and slow dispensation of justice constitute another cogent reason for different kinds of crime in Nigeria. The prosecution of cybercriminals and dispensation of justice is quite slow and sometimes never occurs. Many cybercrime cases are either forgotten or discarded due to the many loopholes in the Nigerian judicial systems. Cybercrime cases are not treated importantly and many cybercriminals tend to get away with it.

Mischievousness has been identified as one of the root causes of information security incidents in organizations (Safa, Maple, Waston and Solms, 2018). The act of mischief-making is an age-long phenomenon and as such not new. Mischief makers may employ the Internet as a tool to execute their nefarious activities. This is because the internet can grant them relative anonymity. Mischief makers who could be current or former employees of an organization, political opponents, and former friends of the victim may target an organization or an individual for cyber victimization to get even for a perceived wrong. Many young people belong to the category of people that have been referred to as digital natives (Dacosta, et al., 2012). They are born in the era of the Internet and digital technologies which some people refer to as computer age. Youngsters' disposition to computer and any other electronic device is a testimony to this. Youths may want to by-pass the password on a computer system or hack into an email account just to prove that they can break into what was considered secure. They are not motivated by financial gain.

Youths in Nigeria today are mostly influenced and pressured into cybercrime by their allies, friends and mates. Yahoo boys are said to often form social communities with online friends and in the quest for acceptance/recognition with these individuals may demonstrate their ability to hack accounts (Marcum, 2014). Arguably, adolescents feel at home within their circle of friends. Because theirs is a world of adventures, they often want to take a flight of fancy' and their peers provide an enabling environment for this to happen. Thus, research on Internet Sociological insights on the contemporary social problems in Nigeria reveals that people may commit cybercrime damning the consequences just to impress their delinquent peers (Phillip, N. 2020).

It could be observed that employment prevents crime for some people under certain conditions and that a reduced rate of employment could result in a high rate of crimes and vices. Nigeria has an unemployment problem. According to the National Bureau of Statistics (NBS), Nigeria's unemployment rate increased from 14.2% in Q4 2016 to 16.2% in Q2 in 2017 and 18.8% in Q3 2017 (National Bureau of Statistics, 2017). In 2020, Nigeria's unemployment

rate has navigated to 27.1%. According to NBS Labour Force Survey, unemployment rate was 27% in Q2 2020 four percentage points higher than 23% reported in Q3 2018 (www.tradingeconomics.com). It could be deduced from these data that the unemployment rate is one of the factors responsible for youth involvement in cybercrime**.** Many unemployed youth in Nigeria are involved in online advanced fee fraud (yahoo-yahoo). The unavailability of job opportunities for graduates with degrees lures them into seeking other means to survive. And with the growing rate of cybercrime in Nigeria, there is a high chance that in a group of 10 friends, 2 out of them are involved in such notorious activity making it easy for the other friends in the group to turn to cybercrime as a means of survival. The post End SARS have gone farther by employing spiritual intelligence to advance the scope of their crimes and the quest for wealth this period by the youths will be catastrophic in future.

The anonymity that the Internet gives users allows people to live out their second lives. The increasing rate of crime and disorder in modern society may be attributed to the political inspiration to people to live two lives. The first life is the formal life that is governed by imposed order, while the second life exhibits the real character of a person. The Internet Sociological Insights on The Contemporary Social Problems in Nigeria is said to be encouraging people to live a second life. To exemplify, an otherwise respected person in society may be involved in online childgrooming as he/she may feel comfortable doing so, with a pseudo-identity.

More so, many citizens engage in criminal activities online for financial gain. For example, online advance fee fraudsters; popularly referred to as "yahoo-yahoo boys" are primarily motivated by the desire to make fast money from their gullible victims and live an extravagant lifestyle. It has been argued that it is relatively easier, less risky, cost-effective to steal information than to rob a bank (Lawanson & Afolabi, 2020). Thus, criminals are using ransomware (the digital form of blackmail that involves taking a person's computer hostage) to extort money from the person (Mansfield-Devine, 2016). Digital thieves target consumers as digital baits to rip them off from various malware schemes like ransomware and malvertising (Chaudhry, 2017). Some individuals may use the Internet as a medium to seek revenge. For example, a person may use social networking sites to intimidate his or her former partners. Clough (2015) describes the phenomenon of non-consensual pornography also known as 'revenge porn' in which intimate images that were consensually taken are eventually uploaded to the Internet or disseminated through social networking sites or websites created for such materials to cause a former partner emotional distress. Similarly, the cyberattacks may be motivated by a quest for revenge for a wrong done or perceived to be done to the attacker (Marcum, 2014). The attacker in this instance may be a disgruntled employee, an aggrieved or ex-employee, an ex-partner, a political opponent, or a competitor in business. The cyberattack, though extra-judicial may just be their way of getting even with the victim.

It could be observed that organized crime groups that carried out traditional activities are now utilizing the contemporary methods that the internet creates for criminal ends (Lavorgna, 2015). The internet offers an opportunity for decentralized, flexible networks of loosely organized criminal's partner in the distribution of work based on knowledge and skills (Leukfeldt, 2015). There are enough motivations for organized criminal groups to employ the internet architecture for criminal gains. One such reason is that the Internet guarantees them

anonymity and drastically reduces their risk of doing business as their chances of apprehension are relatively low. This fact could also be associated to other crimes such as kidnapping, hostage taking and other heinous insecurity issues

The regular global technological development, proliferation of cybercafés and the porous nature of the internet added up to the reasons for cybercrime in Nigeria. The internet has made it possible to break between boundaries and gain access to things in cyberspace despite distance or proximity. The availability of the internet makes geographical boundaries irrelevant. The internet has also made it possible for one's geographical location to be hidden making it difficult to track cybercriminals. Besides, the increase in the number of android and sophisticated phones and computers as well made it easy for people to access the internet and exploit its many possibilities.

Upshot of Cybercrime in Nigeria

The advent of cybercrime has a vast amount of effect on the nation and its sectors. The involvement of youths in this subculture has introduced risks that have greatly affected the economy. Cybercrime is no doubt creating a dent in the nation's image which remains a crucial source of national embarrassment for the country. The fear of cybercrime has made several persons avoid the use of Information Computer Technology (ICT). This harms the welfare of citizenry and investors. Confidence in a nation's financial institution could be diminished by the activities of cybercriminals. Potential investors and tourists are also scared and this damages the image of the nation internationally.

In the recent time, Nigerian citizens face profiling and rejection in the world due to the narrative that Nigeria is a nation - state made up of scammers. This could affect the nation's citizens socially outside the country as every citizen is perceived as a potential scammer. The presence of cybercrime in Nigeria has resulted in the loss of money as well as intellectual property, low productivity, etc. Cybercrime has an enormous negative impact on the global economy. The former President of the Nigerian Senate, Dr. Bukola Saraki during the Nigerian First Legislative Stakeholders Conference on Information and Communication Technology ICT and Cyber Security held on Monday 6th November 2017 disclosed that Nigeria lost about N127 billion to cybercrime (The Punch, 2017). Also, huge revenue is lost to the cyber underground economy where cybercriminals and their patrons buy and sell stolen digital materials.

The rate at which cybercrime is evolving in its many dimensions will require a multifaceted approach. However, the nation seems to be behind in its efforts to curb cybercrime even though the menace is eating into the little developmental gains of the nation. Cybercrime is becoming normalized in society; it has been accepted as a way and means of life by many youths and citizenry despite the fact that security operatives have apprehended many perpetrators while some are on trial. This is also damaging the nation's financial capabilities and security of its banking sectors.

Theoretical Underpinning

There are different theories which can be employed to explain the menace of cybercrime, but for the purpose of this paper, Albert Bandura's Social Learning Theory (SLT) will be used to explain the basis of cybercrime in the context of this paper. Social Learning theory explains

human behaviour in terms of continuous reciprocal interaction between cognitive, behavioural and environmental influences. In other words, this theory is based on the idea that we learn from our interactions with others in a social context. Separately, by observing the behaviors of others, people develop similar behaviors. After observing the behavior of others, people assimilate and imitate that behavior, especially if their observational experiences are positive ones or include rewards related to the observed behavior (Bandura, 1977).

This theory is relevant to this paper because, people engage in crime because of their association with others who engage in crime. Their criminal behavior is reinforced and they learn beliefs that are favorable to crime. They essentially have criminal models that they associate with. As a consequence, these individuals come to view crime as something that is desirable, or at least justifiable in certain situations. Learning criminal or deviant behaviour is the same as learning to engage in conforming behavior: it is done through association with or exposure to others. In fact, association with delinquent friends is the best predictor of delinquent behavior other than prior delinquency. Thus, the main idea behind social learning theory is that we become who we are based on our surroundings and this explanation can be used to explain cybercrime. Youths are the major perpetrators of cybercrimes and they learn faster from their peers and friends. This accounts for why many undergraduates of our public universities are the objects of EFCC operations against cybercrime.

Social learning theory is a general theory of crime and has been used to explain a diverse array of criminal behaviors (Burruss et al., 2016). In regards to cybercrime in Nigeria, research had found that social learning theory can explain the development and ongoing issue of software piracy. In their study of software piracy, Burruss et al, found that individuals who associate with software piracy peers learn and subsequently accept the deviant conduct. Software piracy requires a certain degree of skills and knowledge to access and deviant peers to originally learn these skills from. Furthermore, the deviant individuals rationalize their criminal behavior and help in the fostering of a network that connects and teaches other individuals these rationalizations and behavior. The study also suggested that individuals are more likely to engage in software piracy when they see others experiences positive reinforcement for their participation (Burruss et al., 2016).

Not only does social learning theory explain for software piracy, elements of this theory can be attributed in other cybercrimes. For example, in any crime, the rationalizations and skills must be learned and behavior is reinforced through the association and observation of others. While social learning theory emphasizes the importance of external factors that influence criminal involvement, low self-control theory posits that low self-control is a key factor underlying criminality. This theory was originally developed by criminologists Michael Gottfredson and Travis Hirschi. They proposed that their self-control theory can explain all types of crimes, all the time (Burruss et al., 2016). Individuals with low self-control were characterized with being risk taking, short-sighted, impulsive and prefer simple and easy tasks. These characteristics inhibit an individual's ability to accurately calculate the consequences of deviance. According to this theory, cybercrime can be seen as a means by which cybercriminals in Nigeria obtain immediate gratification, and the ability to delay such short-term desires is linked to self-control. As such, those with a propensity for criminal involvement are thought to lack sufficient self-control. Also, people with low self-control act

impulsively- without much thought and based on what they are feeling at the moment. This makes them risk takers as they do not consider the consequences of their actions. Finally, low self-control people are focused on themselves and lack empathy towards others (Burruss et al., 2016).

Low self-control originates in early socialization when parents are ineffective in their parenting skills. Parental upbringing matters a lot in Nigeria. When you bring up your child with a high moral standard, there is every tendency that such a child will not go astray. Theoretically, if parents have a high moral standard, there is every tendency that the children will not have bad characters, because such parents will always question their children whenever they notice foreign character in them. For example, if you don't question children in Nigeria, that means you encourage them to get into what could be termed, 'an apprenticeship in 419 business' or cybercrime in later life.

Therefore, neglecting and uncaring parents are likely to fail to socialize their child to properly delay gratification, care about the feelings of others, and restrain their impulses. As a result, children with low levels of self-control end up being more prone to crime such as cybercrime and other forms of crime, and their criminal propensity continues into later life. The characteristics of low self-control can be applied to some simple forms of cybercrime, including software piracy. In their study, Burruss et al, stated that levels of low self-control are directly related to the act of software piracy. For instance, an individual is likely to perform software piracy because they are impulsive and unable to wait to purchase a copy of the software. These individuals are not likely to be empathetic to the copyright holder and neglect any responsibility. Further, these individuals are likely to be attracted to the thrill and ease of engaging in software piracy. Low self-control do have an effect on cybercrime and that social learning theory measures (i.e., associating with deviant peers and positive attitudes towards cybercrime) condition this effect. Thus, from the characteristics of low self-control, those with low levels of self-control are likely to participate in deviant behavior both on and offline, within and outside the cyberspace because of their desire of immediate gratification.

Measures of Curbing Cybercrime in Nigeria

Cybercrime has grown rapidly in Nigeria as a result of the introduction of modern telecommunication and broadband technologies. Nigeria was ranked 16th in cyber-attack vulnerability in Africa in 2016 by Checkpoint. The drastic growth can be attributed to the availability of resources as well as the relative ease with which the perpetrators can acquire the skills for committing such crimes, (Umaru, 2019). The Global Cybersecurity Index [GCI] (2018) has ranked Nigeria 57th out of 175 countries on the campaign against the menace of cybercrime globally. Nigeria was ranked Fifth in Africa (www.precioustimesng.com). Therefore here are some ways in which cybercrime in Nigeria could be curbed, the Economic and Financial Crimes Commission has stipulated some measures to be taken to curb cybercrime among which include:

i. Undertaking international awareness programs to inform the world of Nigeria's strict policy on cybercrime and to draw global attention to the steps taken by the government to rid the country of internet 419 and all other forms of cybercrimes
ii. That each sector of the telecom industry, namely the global system for mobile

iii. communications operators, private telecom operators, and cybercafés should come up with a due care document that would be the standard guide and proffer measures for effective policing of cybercrime in Nigeria;
iv. That all cybercafés must be registered with the Cooperate Affairs Commission, NCC, and the EFCC;
v. All cybercafés must install acceptable hardware surveillance;
vi. Each cybercafé is expected to be a watchdog to others, as they have detailed to have direct access to EFCC (Adomi, 2017).

Cybercrime and Regulations in Nigeria

One of the major anti-cybercrime laws in Nigeria is the Cybercrime Prohibition Act 2015. The Act made provision for an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of Cybercrimes in Nigeria.

The Nigeria Data Protection Regulation 2019 is also another regulation that is targeted at protecting both data in motion and at rest. Moreover, there are general laws that deal with financial crimes such as the Economic and Financial Crimes Commission (EFCC) Act 2004. The Economic and Financial Crimes Commission Act was adopted in June 2004. It repealed the Financial Crimes Commission Act of 2002 and establishes a Commission for Economic and Financial Crimes. Under this act, the commission has the power to investigate all financial crimes relating to terrorism, money laundering, drug trafficking, etc. sections 14-18 stipulates offences within the remit of the Act (Kamali, 2020)

Other initiatives directed at protecting the interests of Nigerians in cyberspace may include; the National Information Technology Development Agency (NITDA), Nigerian Communication Commission (NCC), Economic and Financial Crimes Commission (EFCC), and the National Cybercrime Working Group (NCWG). The upgrade of the Nigeria Financial Intelligence Unit (NFIU) to a full-fledged Agency (NFIA) is also a great leap to strengthen the fight against cybercrime in the country (Olatunde-Kamali, 2020).

Conclusion and Recommendations

The paper has confirmed that cybercrime is one of the serious crimes within the Nigeria security firmament because, the general populace becomes increasingly refined in their understanding and use of computers and the technologies associated with it. There is a strong indication that cyber-crimes will become more rife. Nigeria is rated as one of the countries with the highest levels of e-crime activities. Cyber security must be addressed seriously as it is affecting the image of the country in the outside world. A combination of sound technical measures tailored to the origin of Spam (the sending ends) in conjunction with legal deterrents will be a good start in the war against cybercriminals. Information attacks can be launched by anyone, from anywhere. The attackers can operate without detection for years and can remain hidden from any countermeasures. It will always be a losing battle if security professionals are miles behind the cybercriminals. Fighting cybercrime requires a holistic approach to combat this menace in all ramifications.

More so, the Nigeria-nation needs to rebrand its image. A rebranded nation attracts more investment, promotes tourism, and ensures speedily development. It involves commitment

and hard work in the social-cultural, economic and political advancements of the nation's sector. In essence, Nigeria has to take steps to rebrand its image which has been deteriorated by the menace of cybercrime. Analytical and technical or technological capabilities to curb cybercrime in order to detect and analyze cyber-attacks must be put in place.

It is also recommended that appropriate legislation be put in place to ensure that special courts be set up with all the appurtenance of law to ensure that justice is speedily and quickly dispensed, and judgments rendered swiftly, thus removing all unnecessary legal technicalities that prolong unnecessary trial of accused persons in corruption cases. In an attempt to enhance prosecution of offenders, some aspects of the nations enabling Acts and laws need to be amended and reviewed especially in areas that border on abuses of preliminary objections, interlocutory application, and deliberate delay of the judicial process.

Also, media houses and strategic communication agencies should regularly embark on adequate public awareness on the activities of fraudsters and consumer education on the usage of critical computer applications. Education is seen as the most vital weapon for literacy. There is a need for regular seminars and workshops to be organized from time to time with the emphasis on cyber safety so that individuals will learn to keep their personal information safe. There is a need for proper consumer education on the need to; observe simple rules such as ensuring the installation and usage of dedicated anti-malware protection on individual computer systems, and avoid pirated computer software. Personal Identification Number (PIN), bank account, and email access should never be shared with unknown persons as systems are full of security issues. Irrespective of how sophisticated they are. Confidential information should never be shared or disclosed to anybody, as no network can 100% guarantee security from malicious hacking. Ignore any unsolicited e-mail or SMS requiring any financial information.

Finally, to address varieties of security threats particularly cybercrimes in Nigeria, there is the need to create job opportunities for numerous unemployed youths. Government and Private organizations should put in place measures and mechanisms to address problem of unemployment and poverty beyond party-line, ethnic, religious line or mere propaganda. Law enforcement, intelligence, and security agencies need to be trained and re-trained to keep up with technological and security advancements in order to curb cybercriminal activities.

References

Adeniran, A. I. (2008). The internet and emergence of the yahoo-boys sub-culture in Nigeria.

Adomi, E (2016), 'Overnight Internet Browsing Among Cybercafe Users in Abraka, Nigeria', *Advanced Free Fraud in West Africa*, pp 33-34. Nigeria: EFCC

Akano, D. (2016). Switzerland to return S380m Abacha loot. *Daily Independent*, March, are Younger Internet Users. In K. Jaishankar (Ed.). *Interpersonal Criminology*: *Revisiting Interpersonal Crimes and Victimization*. pp. 203 - 214

Bandura A. (1977). *Social Foundation of Thought and Action*. Englewood Cliffs NJ: Prentice

Bandura A. (1977). *Social Learning Theory*. New York: General Learning Press

Brue, L. (2005). Economics - Principles, Problems, and Policies

Burruss, George W., Bossler A. M. & Holt Thomas J. (2015). Assessing the Model on Low Self-Controls Influence on Software Piracy. *Crime and Delinquency,* 59(5), 1157-1184

Chaudhry, P. E. (2017). The Looming Shadow of Illicit Trade on the Internet. *Business Horizon*, 60(1) 77-89.

Clough, J. (2015). *Principles of Cybercrime.* Cambridge: Cambridge University Press. *Contemporary Research*. Vol. 3, No. 9, pp 98-113.

Council of Europe Convention on Cybercrime, ETS No. 185, 2015. Cybercrime in Tertiary Institutions, *American International Journal of Contemporary*

DaCosta, B., Kinsell, C., and Nasah, A. (2012). Millennials are digital natives? An investigation

Economic and Financial Crimes Commission Act, 2004

Economic and Financial Crimes Commission EFCC (2004): Information Handbook. Abuja: Experience. In N. Ribadu, I. Lamorde, and D. W. Tukura (Eds). *Current Trends in*

Folashade B. Okeshola & Abimbola K.Adeta, (2015) 'Nature, Causes, and Consequences of Fraud Among Nigerian Youths and its Effect on Nigeria's Global Image. *International Journal of Intellectual Discourse (IJID)*, Volume 3(2):409-421.

Hall. *Information Security and Application International Journal of Cyber Criminology*, 2 (2): 368–381. into digital propensity and age. (pp.90-106).

Jexcel Commercial and Securities Printers; EFCC, Pp 1-5. *Journal of Community Informatics*. 3(2)

Kigerl, A. (2012). Routine Activity Theory and the determinants of high cybercrime countries. *Know*. London: Oxford University Press. *Laundering Control*, 18 (2):153-168.

Lavorgna, A. (2015). Organized Crime Go Online: Realities and Challenges. *Journal of Money*

Lawanson J. & Afolabi M. B. (2020). Chasing the Nigerian Dream: The Proliferation of Cyber

Leukfeldt, R. (2015). Organized Crime and Social Opportunity Structures: A Proposal for Future Long Essay

M. B., Asiegbu L. N. & Bodunde D. O. (Eds) *Unending Frontiers in Intelligence* a*nd Security Studies.* Ado-Ekiti: Intelligence and Security Studies Programme, Department of Political Science and International Studies, ABUAD.

Mansfield-Devine, S. (2014). The Dark Side of Advertising. *Computer Fraud and Security*, 2014 (11):5-8.

Marcum, D. (2014) Cybercrime. New York: Wolters Kluwer

Mba N. A. & Afolabi M. B. (2017). Introduction to Cybersecurity and Cybercrime'. In Afolabi

Mbaskei, M. (2018). Cybercrimes: *Effect on Youth Development*, http://www.i- genius.org.

Model to Reduce Information Security Insider Threats in Organizations. *Journal of* National Bureau of Statistis (2017). Unemployment and Underemployment Report

Ndubuzue, P. N. (2015). The Social Media, Moral Panic and Governance in Contemporary

Ndubuzue, P. N. (2017a). Generation Y and online Victimization in Nigeria: How Vulnerable Nigeria. *Nigerian Journal of Social Sciences*. 11(2): 158-174

Obarafor, V. (2019) Cybercrime in Nigeria, Causes, Effects, and Solutions.

Okeshola F. B. & Adeta A. k. (2013): Nature, Causes, and Consequences of Cybercrime in Olatunde – Kamali O. (2020). Economic and Financial Crime Commission Intelligence

Operations and Cybercrime in Nigeria: A Case Study Of Abuja, F.C.T. An Unpublished

Oumarou, M. (2017). Brainstorming Advanced Free Fraud: 'Faymani'- the Camerounian Research Directions. *The European Review of Organized Crime*, 2 (2): 91-102. *Research Vol.3.No 9.*

Safa, N.S., Maple, C., Watson, T. and Sloms, R. V. (2018). Motivation and Opportunity based

Singer, P, and Allen, F. (2017). *Cybersecurity and Cyber Warfare: What Everyone Needs to Social Science Computer Review*, 30 (4): 470 - 486. System. Available at www.ndic.gov.ng

Tade, O. & Aliyu, I. (2015). Social Organization of Cybercrime among University

Tertiary Institutions in Zaria-Kaduna state, Nigeria. *American International Journal of*
The Punch Newspaper (2017) Nigeria Loses N127BN to Cybercrime
Umaru, I. (2020). *The Impact of Cybercrime on the Nigerian Economy and Banking*
Undergraduates in Nigeria. *International Journal of Cyber Criminology* 5, 860-875
Wednesday day, 18th 2015