Copyright © 2019 International Journal of Cyber Criminology – ISSN: 0974–2891
January – June 2019. Vol. 13(1): 1–20. DOI: 10.5281/zenodo.3366298
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

"Yahoo Boys" Phenomenon in Lagos Metropolis: A Qualitative Investigation

Samuel O. Adejoh[1], Tunde A. Alabi[2], Waziri B. Adisa[3], & Nnenna M. Emezie[4]
University of Lagos, Nigeria

Abstract

This study investigated what law enforcement agents, who are saddled with the responsibility of curbing cyber crime, know about the malaise; how young people are initiated into cyber crime; the roles of peer influence, and parents' approval of cyber crime. The study adopted cross-sectional design and the qualitative method of data collection. The study population comprises four (4) key informants who are law enforcement agents; two (2) "yahoo boys", seven (7) parents, and seven (7) youths in Lagos metropolis. Purposive sampling technique (snowball) was used to select participants, while in-depth interview guide was used to elicit information from participants. The data were analysed using manual content analysis. It was found that law enforcement agents have considerable knowledge of cyber crime and the different methods used by "yahoo boys" to defraud unsuspecting victims. Frequent interaction between "yahoo boys" and young people plays a key role in the initiation of the latter into cyber crime. Peer influence plays some role in cyber crime, but joining the crime is wilful and not by coercion or chicanery. Parents' unwillingness to report the crime, as well as their acceptance of the proceeds, suggests that they do approve of cyber crime, and thereby contribute to its increased rampancy.

Keywords: "Yahoo boys", Parents' approval, Peer influence, Initiation, Law enforcement.

Introduction

Cyber crime is one of the popular forms of deviance among young people in Nigeria (Ojedokun & Eraye, 2012; Tade & Aliyu, 2011). The perpetrators are received by some people and social institutions when they make the illegitimate money; hence, the increasing justification of illegality (Adeniran, 2008; Ninalowo, 2016). This study seeks to investigate the knowledge of law enforcement agents responsible for curtailing cyber crime on the different methods and processes adopted by "yahoo boys" in defrauding

[1] Senior Lecturer, Department of Social Work, University of Lagos, Akoka, Yaba, Lagos, Nigeria. Email: sadejoh@unilag.edu.ng (Corresponding author)

[2] Assistant Lecturer, Department of Sociology, University of Lagos, Akoka, Yaba, Lagos, Nigeria. Email: taalabi@unilag.edu.ng

[3] Senior Lecturer, Department of Sociology, University of Lagos, Akoka, Yaba, Lagos, Nigeria. Email: wadisa@unilag.edu.ng

[4] Postgraduate Candidate, Department of Sociology, University of Lagos, Akoka, Yaba, Lagos, Nigeria. Email: emeziennennamary@yahoo.com

victims; how "yahoo boys" are initiated into the crime, and the possible roles of peer influence and parents' overt or tacit approval of the crime.

For the purpose of clarification, in Nigeria, "yahoo yahoo" refers to the activities which entail the use of computers, phones and the Internet to defraud unsuspecting victims, especially those outside the country. The term "yahoo yahoo" originated from the fact that the use of Yahoo e-mails and Yahoo instant messenger was a dominant medium of communication between perpetrators and victims (Lazarus & Okolorie, 2019). Those who are involved in "yahoo yahoo" are popularly referred to as "yahoo boys". With the popularity of Gmail services and use, "yahoo boys" are now being referred to as *G boys*. With the spread of awareness of "yahoo yahoo" and sensitisation of potential victims, a group of "yahoo boys" have resorted to the inclusion of magic and spiritual powers to aid the defrauding of victims (Melvin & Ayotunde, 2010). This phenomenon is referred to as *yahoo plus*, and perpetrators are referred to as "yahoo boys" *plus*.

The rising popularity of cyber crime may not be unconnected to the fact that the Nigerian state is currently experiencing economic imbalance with attendant high rate of unemployment among able-bodied youths, erosion of traditional values of integrity, and quick-money syndrome. The Economic and Financial Crimes Commission (EFCC) has recorded several arrests and prosecution of cyber crime suspects. Examples of such include the arrest of six "yahoo boys" in Abuja (Daily post, 2018); prosecution of an arrested suspect who attempted to bribe EFCC operatives with 6.9 million Naira (19,140 US dollars), and several other apprehensions and prosecutions in the last one year (EFCC, 2018). It is expected that with the apprehensions and prosecutions, more understanding of the "modus operandi" of culprits will emerge. However, crime may not be static as suspects could adopt new methods when the old ones are known to the people and law enforcement agencies.

The "Yahoo boys" phenomenon in Nigeria falls within the socioeconomic cyber crime (Ibrahim, 2016) as it is done mainly for financial gains. Considering the economic situation in the country, it is unlikely that a complete stop will be put to the menace by using the pain-pleasure approach which states that offenders should be punished. There is a need to understand how young people are initiated into this crime with a view to discouraging the practice. Studies have shown that some people are influenced by their friends (Tade & Aliyu, 2011; Árpád, 2013; Ojedokun & Eraye, 2012; Arimi, 2011; Atwal, 2011). Ige (2008) and Ojedokun and Eraye (2012) suggested that involvement in the crime is not necessarily influenced by socioeconomic status of parents as children of the haves and have not have been equally arrested and prosecuted for involving in the crime. This suggests that if what pushes the poor into committing cyber crime is the monetary gain, children of the rich are being attracted by other factors aside financial gratification. It is on this note that understanding how young people are initiated, and the possible roles of peers and parents become germane.

The traditional African values frown at illegality, especially stealing. The Yoruba adage that goes *kaka ki n ja le, ma kuku seru*, (I will rather become a slave rather than steal), is a pointer to the fact that in older times, stealing of any sort was unacceptable. But in modern times, crimes such as cyber fraud and Internet robbery are pronounced, and proceeds of such crimes are warmly received by our social institutions. The traditional values of integrity and honour have been replaced by the money. With this erosion of values and concomitant political uncertainty, economic turmoil, high rate of youth unemployment and underemployment, it is unlikely that there will be a complete stop in cyber crime in the country.

Cyber crime is not a novel phenomenon in Nigeria, or in the global literature. Studies have investigated the role of peers in cyber crime, but it is not clear how exactly young people are initiated into the act. Understanding the process of initiation can help curb potential "yahoo boys." It is also not clear how and why parents would overtly or covertly support cyber crime. The family-wherein parents are key players- is the primary agent of socialisation. Any form of support given by parents to cyber crime has grave consequences on social order. The understanding of the knowledge of cyber crime processes possessed by law enforcement agents will help to know the areas in which they require further training.

Theoretical Framework

This work revolves around *Ronald Akers' Social Structure and Social Learning Model*. The model generally assumes that individuals learn criminal behaviours the way they learn other behaviours in the society. Learning, Akers noted, is a part of life that is inevitable in as much as people interact with others in the society. Unlike other social learning theorists, such as Albert Bandura and Edwin Sutherland, Ronald Akers' Social learning theory combines and considers both psychological and sociological predictors of learning in arriving at the factors predisposing individuals to the learning of criminal behaviour (Lee, Akers & Borg, 2004; Akers, 2009). For instance, Akers borrowed from B.F. Skinner's Behaviourism, Albert Bandura's Imitation theory, Alfred Schutz's Social phenomenology, Edwin Sutherland's Differential Association theory and Economics' Rational Choice theory, to conclude that the learning of criminal behaviour is a product of operant conditioning, imitation (modelling), bonding, and reinforcement (positive and negative) that go on in our everyday world (Akers, Krohn, Lanza-Kaduce & Radosevich, 1979; Akers, 1990; Holt, Burruss, Bossler & Adam, 2012).

The model states further that learning is a product of social behaviour that requires association with peers, family members and other members of society (Akers et al, 1979; Holt et al., 2012). What is learnt by individuals is however a function of the level of intimacy and differential association maintained with people. People who maintain close contact with criminals are more likely to imitate their behaviour and replicate such behaviour in their day to day interaction with the society. As individuals exchange ideas, the group with which they share intimacy is the one they are more likely to imitate.

Ronald Akers went further to examine the relationships between social structure and social learning in our contemporary world. According to Akers (2009), social structure (which is the assignment of roles, responsibilities, classes, powers and privileges) in the society, plays a significant role in determining how we learn and what we learn. Using his *Social Structure and Social Learning Model (SSSL)*, Akers concluded that individuals' position in the social hierarchies of society will determine the choice of what is learnt, exposure to the criminal world and the extent to which they are deterred from crime.

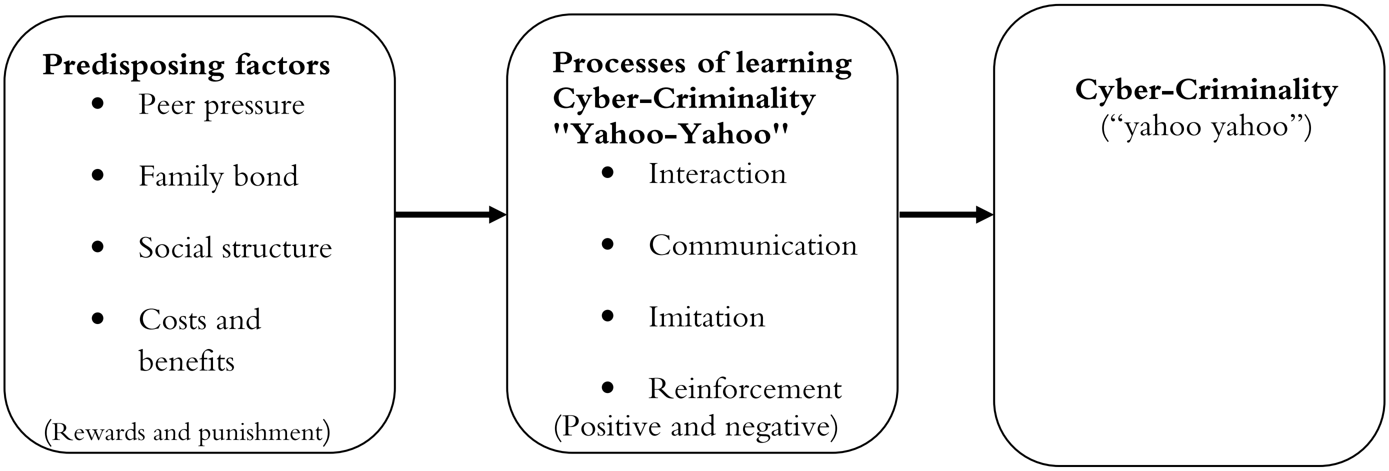
Because the children of the middle and low income class live often live in societies where enforcement of laws is not effective, the rewards to engage in criminal behaviour are usually higher than the punishments. The SSSL model asserts that the higher the rewards for a crime, the higher the probability that individuals will be involved in crime. The model also states that poor bonding with family members and the social environments experienced by young people from poor backgrounds increase their chances of associating with criminals in the society (Akers, 2009; Holt et al., 2012).

The relevance of Akers' social learning model to the explanation of the phenomenon of cyber-criminality in Nigeria can be inferred at three levels. The first level is the fact that the "yahoo yahoo" phenomenon is learned by young people from their routine interaction with cyber criminals in the neighbourhoods, schools, club houses and social gatherings. Given the fact that cyber crime attracts more money for the perpetrators, the conspicuous lifestyles of the "yahoo boys" usually serve as incentives for the recruitment of young people who live in the same society with them but have weak moral bonding and desire to emulate the "yahoo boys".

The second level at which the social learning theory is relevant to this study is its ability to explain the reasons why most young people who join the "yahoo yahoo" business come from low-income class and disorganized environments. Based on the views of Akers, weak family structure, lack of strong social bonds and social disorganization that characterize the low-income environments naturally create a breeding ground for joining cyber-criminality. Given the poor living conditions in most Nigerian cities and high cost of living of the children of the poor (World Bank, 2018), "yahoo yahoo" naturally serves as an alternative to survival.

Figure 1. Relationships between predisposing factors, processes of learning the act and cyber criminality ("yahoo yahoo") in Nigeria

Social learning model of "yahoo boys" phenomenon in Nigeria



The third level at which the SSSL model is relevant in its capacity to account for the costs and benefits of cyber criminality and its implications for the persistence of the problem in Nigeria. From Akers' position, crime will always persist in as much as the rewards for crime are high and punishments for it are mild. The rewards here are the humongous benefits that criminals derived from their criminal actions such as the expensive cars and lavish spending enjoyed by the "yahoo boys". In many cases, these boys may not be arrested or even sentenced when arrested. This is evidenced in the rising cases of cyber-criminality and low level of resistance to pressure to join cyber-thieves despite attempts by government especially the EFCC to effectively control the crime.

The current study, which this model seeks to explain, has brought out three major causes of cyber-criminality in Nigeria; differential association, poor parental background and imitation. They are significant because they determine how the yahoo phenomenon evolves in Nigeria and why suspects have been evading arrest. They are also important in formulating appropriate policies to reduce the incidence of cyber-criminality in the Nigerian society.

Methods

Design, population and location

The study used the cross-sectional survey design and a qualitative method of data collection. The study population comprises four different categories of persons. Those involved in "yahoo yahoo", relevant security agents, parents, and young people who are not necessarily involved in cyber crime but may have friends and relatives who are involved in the act. The participants were selected from different locations in Lagos Island and Lagos Mainland. The rationale for choosing a range of study population is to get diverse responses and in-depth understanding to the research questions.

Sampling and Inclusion

A total of 21 participants who consented to participate were interviewed. The interviews involved 7 parents, 7 youths, 5 law enforcement officers (key informants) and 2 "yahoo boys": 1 male and 1 female. Parents were screened verbally to be sure that they are aware of the phenomenon in question before they were interviewed. In addition, it was confirmed that the parents had adult-children before they were interviewed. The youth selected also had some knowledge of the phenomenon; in fact, some of them had "yahoo boys" as friends and/or former friends. The key informants are officials of law enforcement agencies who specialise in handling cases of fraud and cyber crime. The study adopted purposive sampling in the determination of the study populations. For the "yahoo boys", the study adopted a snowball sampling technique. The male participant did not allow physical contact; the interview was done over the phone. Snowball sampling technique was also used in the selection of officials of the law enforcement agencies. None of the officials allowed recording; they only allowed note taking for security reasons.

Research instrument and data collection

Interview guides, which contained mainly open-ended questions, were used to obtain information from the participants. All the four interview guides contained sections on socio-demographic questions before core issues on cyber crime and the roles of peers and parents in the malaise. We asked police officers to describe their experience in the recent cases of "yahoo boys" they had handled. We also asked police officers questions such as, "what do you understand by yahoo plus?", "how do you perceive the role of friends in luring young people in engaging in '*yahoo yahoo'?* activities" with other probing questions where necessary.

Law enforcement officers were asked to explain how they apprehend "yahoo boys" and incriminating materials they do retrieve from them, and how the case is usually handled. They were also asked about their understanding of the processes and methods adopted by suspects in defrauding victims. A typical question was, "how does the agency operate with respect to the prosecution of 'yahoo boys'?"

"Yahoo boys" were asked questions such as, "since when have you been into this hustle?", "how did you join the hustle?" A probe into how they were initiated was carried afterwards for the two groups. They were asked questions like "what is your area of specialisation?", and "how is it lucrative or better than other areas in this game?" These were asked with the researcher's understanding that there are several kinds of hustling methods (some people deal with ewe or traveller's cheque, others with the Bank of America (BOA), and, "what are the different processes involved before you eventually get paid?" This was asked with the understanding that the hustle is not easy and that it requires several processes and intelligence. They were also asked of the roles their peers played in their joining of the group. The interviews lasted for about 20 to 25 minutes on the average and were conducted in privacy.

Data analysis

The interviews and notes taken were transcribed into the computer, and the data were analysed using the manual content analysis. The analysis was organised around themes and sub themes developed in line with the research questions. Socio-demographic information were first analysed, and it was then followed by the data that addressed the main research questions. Some questions were specific to each study population and some apply to all.

Direct quotes from the participants were presented in the data analysis as has been done elsewhere (Adejoh, Temiola & Adejuwon, 2018). Responses were studied, interpreted and categorised into the research question that they best answer (Silverman, 2013). For research questions that address whether a factor plays a role in influencing cyber crime, two sub-themes were created: one for responses that support a view, and the other for those that oppose it. The data were categorised into preset category and emergent category (Unrau, Gabor & Grinnell, 2006). The preset category allows us to start with themes in advance and then search the data that fits into the theme. We searched for texts in the data that match the theme under consideration. For the emergent category, we read through the texts to find issues recur and are in similar context in the data. This allows the category to emerge from the data.

Ethical issues

All participants were told about the rationale for the study and gave their consents before the commencement of interviews. All the 21 participants agreed to voluntarily participate in the study. No incentive was given to any participant.

Results

1. Socio-demographic characteristics

The youngest participant was a youth of 21 years old; the oldest participant was a parent of 70 years old; the modal age is 49 years. The mean age was 39.5**,** while the standard deviation was 15.5. 61.9% of the participants were males, while 38.1% of them were females. 13 of the participants were married, and seven of them single. Six of the participants were B.Sc degree holders, two were M.Sc degree holders in their respective disciplines, another two participants held Ordinary National Diploma, while one participant held a Diploma certificate.

2. Knowledge of "yahoo boys" phenomenon by law enforcement agents

According to the law of the country, the Economic and Financial Crimes Commission (EFCC), the police and other law enforcement agencies have the mandate to arrest and charge Internet fraudsters to court. A key informant explained the section that gave power to the agency:

> Advance fee fraud act (2006) was established to fight and prosecute all fraud-related crimes. This act gave the EFCC the power to prosecute all financial and economic crimes. Cyber crime is a type of crime that involves the use of computer through the Internet as a means to carry out fraudulent activities in the cyberspace. Because the 2006 act did not cover fraudulent crimes on cyberspace, the cyber crime act 2013 was created to help the EFCC prosecute and fight fraud using the computer and the Internet as a means. Also, this act was made to fight cyber crime locally and globally (Male, law enforcement agent).

Another key informant from the same institution provided more insight:

> Advance fee fraud act, cyber crime act guides the EFCC in the prosecution of offenders. Offences include: obtaining money under false pretence, possession of un-authorized information and access, cyber stalking and terrorism and so on. Also, lavish lifestyle with no legitimate source of income can cause the EFCC to investigate. We also have the money laundering Act which empowers the EFCC to prosecute money launderers which is greatly associated with "yahoo yahoo". The EFCC act empowers us to sue and be sued.

The EFCC had been in the forefront of the arrest and prosecution of "yahoo boys". However, there are other law enforcement agencies such as the police especially those in the special fraud unit. The EFCC does not work in solitude because cyber crime is similar to drug-related crimes which usually involve large networks of criminals. So, officials of the institution work with the police, ICPC, NDLEA, immigration, custom and other international bodies such as the FBI because the USA is the most defrauded country as most of the victims from there are vulnerable (law enforcement agents). It is the belief of some people that the whites are not vulnerable as many think, but they act under the spell of *yahoo plus* --- a practice of fetishism, where rituals are carried out by "yahoo boys" to aid the defrauding of victims.

a. Knowledge of forms of cyber crime and processes used by "yahoo boys"

With respect to knowledge of the activities of "yahoo boys" and some of the processes involved in scamming unsuspecting victims, the key informants demonstrated their awareness and understanding of the phenomenon. A key informant explained different types of hackers:

> There are three types of hackers – the black hackers, the white hackers and the grey hackers. The black hackers perpetrate, penetrate, hack, get information and they will make use of it themselves. The white hackers are for investigation purposes. They are the FBI, the CID and law enforcement agencies. When need be, they can use their professional experience to get information for the purpose

> of investigation. These ones have no criminal intent. The grey hackers have a commercial purpose, they sell, they never use it, and they will just hack to sell. If you doubt them, they give you one to test-run (Male, law enforcement agent).

The key informant emphasised more on the grey hackers. He noted that they often sell e-mail login information of multinational companies to "yahoo boys" who monitor the transaction and interaction between such companies and their clients. He stated further that:

> If I get access to their e-mail, I can read their mails, I can send mails from their mail, I can delete, I can edit and I can see all your transactions through mail. For instance, companies might have somebody that they want to send money to, or those that want to send money to them. Information such as how much they want to send, when and how the money will be sent is contained in the e-mail that "yahoo boys" have access to. Sometimes they ("yahoo boys") might even allow you to send an account, but you wouldn't know that they have sent another e-mail to counteract your e-mail. They may claim that mistake was made in the former e-mail, and that clients should disregard the first account and send it to this particular account details (which they have just sent). It has happened several times and before you know what it going on, money has been transferred. (Male, law enforcement agent)

The point here is that the original owners of the e-mail account will still be able to access it, but the "yahoo boys" can also access the same account. When they send or receive an e-mail that is suspicious, they quickly delete it so that the original owners are not aware someone else is accessing the e-mail account.

Another key informant shared his experience and knowledge of a hardworking IT staff who stole the login of his colleague, then transferred millions of naira:

> So there was a bank intern who was good in computer and other IT stuff. When you enter a banking hall, we have a cashier. Mostly behind the cashier are operational staff. You will find out that if you are using cheque to make withdrawal and the money is large, the cashier will tell you he's coming. He's going to the head of operation to authorize, and the authorization type could be on paper and even through mails, too. They can get authorization so that he can clear the money. So because of this intern's effectiveness and zeal to learn, he assists the head of operations. Most of the time, she assigns her own job to him, So, within that period he was able to get her username and her password. So if you login with her username, you will log in as the head of operation. In that case, you have access to so many things that even the cashier does not have. This guy logged in successfully, went into an account that belongs to the local government, transferred the sum of 27 million naira (75000 US dollars) to other different accounts. The transaction took place on Friday. Between Friday and Monday, they had transferred the whole sum of money to about 29 different accounts, scattered the money everywhere. And as the money was entering the different accounts, they were making withdrawals through the ATM, POS and what have you to make sure that they exhaust the money (Male, law enforcement agent).

This shows that involvement in the act is of different kinds: those who do not have any other job aside the crime and others who are opportunistic/occasional fraudsters. They have legitimate occupation but also involve in the act when they see the opportunity.

Another key informant spoke about contract and "love" scams:

> "yahoo yahoo" could be divided into two broad distinctions: contract and love scams. The love scam involves dating vulnerable and gullible women abroad that are mostly wealthy and single to get financial gains and other benefits. These criminals change their IP addresses to areas of the target location, i.e. someone could be in Nigeria and pose as someone in the US. They also possess international phone numbers that aid their disguise. All information given out to the victim are usually fake including pictures to hide identity, making them hard to trace. The contract scam involves e-mail phishing, identity theft, hacking, defamation, credit card theft and so on. (Male, law enforcement agent)

In addition, the romance scam could be the other way around where the scammer is female and dates male victims. More so, there are some who have several accounts. They hide their identity in some; they show their real self in the other and eventually travel to marry their white lover. In the case of male scammers, they marry white women who are thirty years older or more. Similarly, another key informant mentioned different ways of perpetrating cyber crime and emphasised that it involves networking:

> "yahoo yahoo" is a syndicate that comprises different people that play different roles in aiding the crime. They do not necessarily have to see or know the person. The "yahoo yahoo" game is a wide chain that comprises different people which includes the person who provides an account for a money to be wired so it cannot be easily traced; the money mules who go to the bank to pick up the money; e-mail phishing; love scams; contract scams, credit card frauds, business e-mail compromise (CEO fraud), defamation (impersonation), hackers and so on. (Male, law enforcement agent).

In all, participants from law enforcement agencies have reasonable knowledge and are aware of some of the processes through which "yahoo boys" perpetrate cyber crime. The processes are not fixed as the security participants noted that members of some of the security agencies meet quarterly to share and compares notes on new ways by which "yahoo boys" perpetrate crime., However, once the latter realises that the law enforcement agencies are aware of the latest processes, they initiate another one, thereby suggesting that processes of cyber crime are evolving and dynamic.

b. Knowledge of yahoo plus phenomenon

Yahoo plus is often used to denote the use of fetish items and rituals to aid the defrauding of victims. Surprisingly, law enforcement agents are aware of the phenomenon and none discountenance its existence. One of the key informants noted that:

> Yes, I have heard about yahoo plus. In fact, I even asked from my suspect because I have done a lot of courses in ICT. The plus, according to him, actually means something that has to do with jazz, juju, fetish things, you know, in order to make the perpetrators have authority. They can chew some things so that when

> they talk to victims, they will succumb to their suggestion. They can tell you what to do on the other side and you go ahead to do it without complaining and you might not realize until when the work has been done. That's when you come to realize. (Male, law enforcement agent)

Another key informant noted that *yahoo plus* exists, and there are departments that deal with such cases:

> Yahoo plus means using different forms of spiritual means to enable them carry out this crime. It is a very serious crime. Anti-cultist department handles rituals or ritualism in which this type of crime falls. The herbalist is arraigned to court as well if found as a suspect in the crime. He or she could be arraigned to the court for conspiracy, accessory to the crime. (Male, law enforcement agent)

It is generally believed that the ordinary yahoo is no longer yielding huge sums of money, hence, the need to upgrade or plus it. This is why *yahoo plus* is often regarded as a higher or upgraded version of "*yahoo yahoo*". This is evident in the opinion of a participant that: "Yahoo plus is the upgraded version of "yahoo yahoo". Use of rituals and other fetish means to aid their fraudulent activities."

3. Initiation into cyber crime

Cyber crime, particularly among young people in Lagos, has continued to gain popularity as many young people are becoming attracted to the act. In fact, many youths in Lagos have embraced cyber crime as a way of life and a means of improving their economic condition, especially as unemployment rate continues to soar. Data from this study suggest that many young people get initiated into cyber crime as a result of their interaction with the so-called yahoo-boys and yahoo-girls as well as their own quest to becoming rich and living a flamboyant lifestyle, especially when they compare their standard of living with those of others who are into the fraudulent act. This notion is vividly captured in the opinion of a participant who said:

> When you see people of your level and calibre that are not necessarily doing anything that matches their standard of living, you start feeling intimidated and you start getting inquisitive and you want to be like them. So from your inquisitiveness you ask questions. From there, you get close to those people that are actually involved in this cyber crime or "yahoo yahoo". (Female, 23 years old).

The response above indicates that initiation could begin with upward comparison --- a situation where people compare themselves to those who are of the same age or status but are doing better in standard of living than they. The urge to reach an equal or better standard will push them to question the "yahoo boys" if they have prior cordial relationship, or ask a neutral person who will give them details of real occupation of the gamers, then find a way to introduce the potential "yahoo boy" to those who have been in the game. The introducer must be one the "yahoo boys" trust and have known for some time.

Another participant gave an illustration of how a condition such as hunger can prompt initiation into cyber crime, and that initiation process often begins with interaction between a young person and a cyber crime syndicate as stated below:

> It's rampant, like everybody on the street. You just have people do it. So imagine I say I'm hungry today and I'm talking to someone that is into it about my hunger and the person just says "oh, okay since you don't have anything you are doing, this is what I do." I think that's how people get introduced to it --- by speaking about their situation of unemployment, hunger and so on. (Female, 21 years old).

Similarly, a participant explained how frequent interaction with the syndicate can prompt initiation into cyber crime. Thus, this participant suggests that cyber crime is learned from interaction with other persons in the process of communication. An individual is influenced to participate in cyber crime through watching and interacting with other individuals who are engaging in the criminal act. When asked about process of initiation into cyber crime, the participant said:

> First of all, it's by appearance, when you see something good, and you are like, "ah, I have to step up to this and all." So, it starts with revealing one's disadvantaged status to a syndicate. (Female, 21 years old).

So far, responses suggest that initiation into cyber crime, unlike cultism, is not coerced. People join willingly when they frequently interacted with syndicates who are living posh. As humans, we tend to measure progress by comparing ourselves with people whom we interact frequently and see on a regular basis.

In addition to interaction with those involved in cyber crime, certain environments such as university campuses also aid initiation to cyber crime. Youths, especially undergraduates, have embraced the ICT inventions such that the Internet medium now takes a larger part of their days when compared to their other daily activities. As such, cyber frauds among educated youth are better planned, executed and organized, and it is gradually becoming a sub-culture among them especially as current economic condition crumbles leaving many young people to survive on their own. This notion is evident in the view of a so-called yahoo-girl who holds an M.Sc degree in her academic field of study. When she was interviewed about the initiation process into cyber crime, she said: "Well, I don't like to call it cyber crime, anyways, but it was during my university days." (Female, 28 years old). She made it known that she has been part of the game since her university days and she was influenced by the social environment. Apparently, the proceeds of the crime were used to further her postgraduate studies. Using proceeds of cyber fraud to fund their studies is a common thing among many less privileged young people who join the game.

Similarly, another participant, who is a university graduate and has been involved in cyber crime, explained how distraction of expensive and ostentatious lifestyle seen around school environment can prompt initiation into cyber crime. A participant shared his own personal experience of how he was initiated into the fraudulent act:

> I joined this hustle out of insatiable desires. As a man or a guy, you need a lot of material and financial things. You cannot totally exclude or disregard the things you see especially when you were in a university where there are a whole lot of distractions that make you want to do certain things like driving some certain type of cars at some certain level. (Male, 29 years old)

As noted earlier, people hardly compare themselves with those they cannot see or interact with. The participant emphasised a university which is considered by many to be the plushest university in Nigeria due probably to the location of the institution, and its show of fashion, and conspicuous lifestyle.

4. Role of peers

No human being exists in isolation. At every point in time, people associate themselves with a group of people for various reasons. The influence of this group on youth's decision to indulge in activities that are both positive and negative to conventional expectations cannot be over-emphasized as expressed by some participants.

A participant opined that:

> Peer group is very influential, and most of the people involved in the "yahoo yahoo" fraud are young graduates, some are postgraduates, some are even undergraduates. These are the people that are desperate; these are the people that have seen their friends made it; they have seen people, their friends with flashy car. They too want to feel among, you know, they want to make it, they want to feel happy, they want to feel high ray, they want to join, they also want to go to clubs and spend money, they want to ride in big cars and live a flamboyant lifestyle. So in the process, peer groups play a role. (Male, law enforcement officer)

A participant, who is into cyber crime, agreed with the view expressed above. In his opinion, young people's desire to emulate expensive lifestyle of friends around them can put them under pressure to join cyber syndicates and perpetrate Internet fraud. Thus, his view suggests that youths are more likely to engage in juvenile cyber crimes such as hacking and online bullying if their friends are into it. When the participant was asked whether or not peer influence can influence youth to perpetrate cyber crime, he said:

> Yes, it does. Your friends change cars, wear fine clothes, go to parties with girls, popping champagne. They will always ask you how you are making it. It is the same thing when a runs girl (commercial sex work very common among female university students) wearing good clothes and driving cars, you want to know how they made it as well, what kind of job they do. You join in the process. (Male, 29 years old)

Another participant opined that people of like-minds attract one another. As such, youths involved in cyber crime often form a clique that is bounded by interest in committing cyber crime. She explained that:

> Birds of the same feather flock together. So, the influence is actually very high. If you see people that are into a legal business, you see that their clique of friends is

> actually people in the legal business, too. Likewise, when you see people that are fraudsters, if you check their clique of friends, they all have the same mentality, they all have the same standard of morals and style of living. (Female, 23 years old)

However, the link between peer influence and involvement in cyber crime is often complex as there may be other intervening variables that may come in between. In other words, the relationship between peer influence and cyber crime is not necessarily a direct relationship as suggested by many participants. This notion was vividly captured by a participant (parent) who said that:

> They say, "show me your friend, I will show you who you are." That is just that. They can be influenced, But I have seen a person who follows those ones that are stealing but didn't steal. Instead, he gave them gap. Whatever they gave him, he didn't join them, but they were friends. So you see that this life is what you choose and what your heart desires. The Bible says that it is what you desire to have that will chase you, or that you would desire to do. If you desire to do evil, you will do evil. So all these said, friends can be influenced but what you determine to do within you can be another thing, the environment you are can also teach you what you don't wish to do. So all these is what can trigger people to do what they want to do. (Female, 52 years old)

When asked whether yahoo fraudsters are being influenced by their friends, a participant, who has a similar socio-demographic characteristic as the participant above, explained that apart from peer group influence, the larger society also plays a role in youth indulgence in cyber crime. In her words:

> The society is not really helping the youth in the sense that there is no job. There are lots of graduates out there now and most of them are just like roaming around the street. So because they don't really have something to do, they join such kind of friends and then some of them that are very lazy too, instead of actually thinking of doing something better for themselves, they feel the need to get rich quick, and so they might also go into it. (Parent, female, 52 years old, Civil servant)

The responses above support the earlier assertion that joining the gang is not by coercion but persuasion and attraction. When young people are persuaded by their peers or are intimidated by the conspicuous lifestyle of the "yahoo boys", the final decision lies with the former.

Another participant, who is also a parent, illustrated how peer pressure can combine with the effect of unemployment to prompt young people to commit cyber crime. Unfortunately, many Nigerian youths in their productive years are unemployed. With the current economic situation, unemployed youths are more vulnerable to peer influence, and can easily be lured into cyber crime. The participant had this to say:

> Yes, some are influenced actually in the sense that "an idle mind is the devil's workshop." When they are there, they are doing nothing (jobless) and you know as they grow, they have some needs they have to maintain and when they are not maintaining that, a friend could invite them for a business deal. There, they are

> influenced because of what he wants or the needs they have. (Parent, female, 48 years old, Civil servant)

Meanwhile, a participant downgraded the extent to which peer influence lures youth into cyber crime. The participant is of the view that while peer pressure can indeed lure young people into cyber crime, there is a limit to this influence. He explained that:

> Somebody can be influenced to do what he does not want to do, but these children we talk about are out of kindergarten. They know what they are doing and they do it intentionally. I agree that they are being influenced, but they have their mind already made up to join them. (Parent, Male, 54 Civil Servant)

A participant who is involved in cyber fraud opined that the overall economic condition rather than peer pressure is the major reason why young people commit cyber crime. Many young people in an attempt to escape poverty and improve their standard of living indulge in what is known as "socioeconomic cyber crime." This participant has this to say:

> I think it's the economy in general, because when you're in a country where there's no job security, you come out of the university and there's no hope for the future. So a major factor is the economy, yeah, and peer pressure is added to it in the sense that you see someone who legitimately works for his money being oppressed by an individual that scammed someone to get money. So when you see such a thing happening, you decide to damn the consequences and go into this business so you can make your own money and spend it laulau. But then I think, majorly it's the economy. If the economy was good enough and there was job security, I can bet you that 50% of people that are into this business would not be in it. (Female, 28 years old)

5. Parents' approval

Parents, as agents of socialization, are expected to provide sound moral support, which reflects the societal norms and values, for their young ones. They are expected to guide their young ones through rules and discipline. However, for economic and other reasons, many parents have deviated from their expected role. It has been observed that many parents are indifferent about how their wards make their money. In fact, some participants opined that some parents even support their children in carrying out cyber crime. As some participants explained it, the support may be direct or indirect, tacit or covert. A key informant who has been serving in the enforcement agency for 12 years stated that:

> Parents do not report crimes, most times they do not know exactly what their children do to make money even if they might be aware that it is illegal or through dubious means. They do not support their children directly but indirectly. As a result of the silence to the crime, they support it. Also, environmental factor plays another role in the support of this crime especially areas with high poverty rate where people see "yahoo boys" as 'gods' that will help them alleviate their poverty. They celebrate them in their families and society as people that made it despite all odds. They won't want to bite the hand that feeds them. (Male, law enforcement agent)

Indeed, there are several cases where popular "yahoo boys" are given chieftaincy titles, and are asked to contribute towards community development projects. In fact, some of the gamers are breadwinners of their families; they feed their parents, wives and children, and pay siblings' school fees from the proceeds of cyber crime.

Another participant is of the view that some parents often show negligent attitude concerning how their children make their money. He stated that:

> Some parents lay down, they play low tune when it comes to that. All what they want to celebrate is that their child has finally made it, but they are not too careful in finding out how he makes it. (Male, law enforcement agent)

Another participant opined that:

> Parents play a role indirectly in the support of their children by not questioning them on the means of livelihood. In fact, we have a rare situation where the father encourages the son to learn "yahoo yahoo". (Male, law enforcement agent)

There are indeed cases where parents employ teachers to teach their wards how to become an Internet fraudster. However, no registered IT institute will overtly teach people such things. But the idea is that the basic knowledge such as how to operate the computer, open an e-mail account and use chat messengers taught in computer schools are required to become a yahoo boy.

While some parents are aware of their wards' illegitimate source of income and either act neutral or give them moral support and in prayers, there are some others who do not know what their children do to make money. A female Internet fraudster attested to this fact:

> To be sincere, my parents are not aware because they actually know I have an official job. I go to work in the morning to go and oversee my goods, even if my parents are not exactly sure of where the money came from but I told them I had investors invest in my business and the business is actually doing very well. Do you want to come and calculate my money for me? (Female, 28 years old)

Similarly, another participant, who is also involved in cyber crime perpetration, has this to say about parental support for cyber crime,

> I don't think any parent would support this hustle. My parents don't know what I do. They believe I'm into business. (Male, 29 years old)

Internet fraudsters and the likes are fond of saying that they are into business of clearing and forwarding when asked what they do for a living. Parents are expected to have sufficient idea and knowledge of their children's occupation, the location and knowledge of few co-workers where necessary. It is not sufficient for parents to know that their children work, they should be able to match the lifestyle and expenses of such children to the occupation, and report any perceived discrepancies to law enforcement agency.

Discussion

This study sought to investigate the knowledge of methods and processes adopted by "yahoo boys" in defrauding victims, and also to know how "yahoo boys" are initiated into the crime, and the possible roles of peer influence and parents' approval of the crime.

Regarding knowledge of security agents about the crime, it was found that the law enforcement agents have some knowledge of the various ways by which cyber crime is perpetrated by "yahoo boys" and those of yahoo plus. Some of the common ways known to law enforcement agents include romance scam and wire both of which are intertwined which the "yahoo plus" phenomenon. Romance scam entails that a suspect registers on social media and often times dating websites where they send spam messages to several people requesting to be their friend or lover. Those who respond are followed up on and are frequently communicated with on a regular basis to build the trust. The suspect tries as much as possible to gain the love and trust of the victim. This may include sending nude pictures and gifts. After the trust has been gained, the suspect then begins to extort money from the victims. The reasons given to the victim could be that they are sick and need money for treatment, or that their business is not doing well and needs financial assistance.

Sometimes, the yahoo plus boys use rituals and fetish means to aid the process. One of their approaches is the use of gifts including rings, necklaces and fabrics. These items would have been taken to a herbalist who prepares them with charms (full names of the would-be victims and that of their parents are often chanted or inscribed in the charm) for a number of days before it is sent to the victims in Diaspora. It is believed that once the unsuspecting victims put on the jewellery, or fabric, they will be under the influence of the charms and do whatever the suspect says. Another method involves chewing and licking of fetish items before speaking to a victim on the phone, it is their belief that the victim will not resist their command. Studies should do a forensic investigation of the nature of such conversation, whether it involves command from the suspect, and the time interval between such call and when a victim sends money. Extant studies identified ritualism and fetishism as part of the culture of many African countries and were documented by both colonial and post-colonial writers (Harnischfeger, 2006; Akiwowo, 1983; Nwolise, 2012; Simpson, 1980; McCall, 2004; Payne, 1921; Talbot, 1923; Wolff, 2000; Rubin, 1989; Cohen, 1966).

With respect to the role of initiation, this study found that the process of initiation into cyber crime among youths is heavily dependent on their interaction with others who indulge in cyber crime. This result is also supported by one of the assumptions of Edwin Sutherland's theory of Differential Association, Sutherland (1939). The reason for the claim that youth interaction with cyber criminals contributes to their indulgence in cyber crime is not far-fetched. Since social interaction is an integral part of social group and cyber crime perpetrators do not exist in isolation; they are brothers, sisters, relative, schoolmates or neighbours to young people; therefore, it can be logically deduced that young people will interact with cyber fraudsters and may be initiated in the process.

More so, the role of the university environment in aiding the process of youth initiation into cyber crime cannot be jettisoned. This is particularly true as the environment breeds individuals of different background. Some are from wealthy homes, while some have ventured into cyber crime as a means of survival and living large in school. This also contributes to the attraction, and consequently initiation of young people into cyber crime as they feel intimidated and interact with the fraudsters without minding to go any length to become like the latter. Even though the university is a pro-social institution, its environment has serious impact, both positive and otherwise, on the students and those around it.

Regarding the role of friends, it was found that peer pressure is a complex factor in the explanation of young people's involvement in cyber crime. The young people as a contributory factor corresponds with Esiri (2013) who noted that of one of the goals of peer pressure is concordance, and the result of such is conformity to criminal behaviour in delinquent subculture. It supports the assertion of Nsofor (2013) that peer group is an agent of socialisation where young people internalise behaviours, the kinds of behaviour, whether good or bad, embraced by a child is contingent upon the characters of the peers.

However, the result of this study shows that despite the enormous influence of peers on young people, the relationship between peer influence and cyber crime is complex as other intervening variables and the personality of the young person are very important in determining the kind of peer he or she will attract. This finding is supported by philosophical view that like-minded people attract one another. Reckless (1981) also used the concept of "containment", which he defined as the ability and strength of a person to direct himself or herself and resist deflection from conventional norms and peer influence. Reckless suggested that youth involved in cyber crime have low-self esteem, and practising cyber crime may be an attempt on the part of those who do not feel the emotional security that comes with a positive self-image. Despite this complexity, the role of peer influence cannot be over-emphasized on youth involvement in any criminal act, including cyber crime. In addition, even when friends are suspects of cyber crime, the pro-social behaviours of parents and teachers and the commitment of a person to their relationship with the pro-social entities can deter them from joining *"yahoo boys"* (Hirschi, 1969).

Lastly, the finding of this study suggests that parents' overt or covert support may suggest to suspects and potential suspects that the act is not too bad. Indifferent attitude and lack of concern for activities of young people is common among Nigerian parents, particularly those in poverty-stricken areas of Lagos State. They encourage or at least show indifference to sources that will improve their standard of living. This indifferent attitude encourages young people to perpetuate the act.

The notion that parents can play important roles in curbing cyber crime among youth is highlighted in Hirschi's (1969) Social Bond theory. For Hirschi, the importance of parents in controlling cyber crime among youth is rooted in the bonds that youth form; bond to pro-social values, pro-social people, and pro-social institutions. According to him, it is these bonds that end up controlling young people's behaviour when they are tempted to engage in criminal or deviant acts. Hirschi outlines four types of social bonds: attachment, commitment, involvement and belief.

Attachment with pro-social parents is particularly relevant when examining the role of parents in preventing young people from committing crime. Hirschi held the view that parents and schools are of critical importance in this regard; whereas youth who form close attachments to their parents and schools are less likely to engage in cyber crime given that their parents and schools frown at such act. This is similar to the notion of Vander Ven and Cullen (2004) that low socioeconomic parents may not be able to provide necessary moral and material support for them. Parents' inability to provide basic needs can affect social bonds between they and their children so that even when such parents are pro-social, the child may tilt towards illegitimate means to survival.

Conclusion

The *"Yahoo yahoo"* phenomenon is rampant in the Lagos metropolis. The law enforcement agencies are aware of some of the processes and approaches used by suspects to defraud unsuspecting victims. Uncompromised efforts from the law enforcement agents and institutions, and cooperation of financial institutions and members of society will go a long way in yielding more arrest and prosecution of suspects. *Yahoo plus* phenomenon also exists and is being practised by suspects who are eager to make it big. It is, however, not clear how prosecutors are able to provide and justify evidence of fetishism and ritual practices against the suspect in the court of law. Initiation of young people into cyber crime requires complex interaction and teaching-learning process that is not coerced. Tacit or direct support from parents and members of the society suggests that proceeds of cyber crime are acceptable. Anti-social friends are not enough to lure young people into cyber crime, the role of pro-social parents and institutions, and the personal disposition of the individual can mediate such influence. Future studies should look into the profiles of victims of cyber fraud, and then investigate the frequency of transaction before and after they received gift items from suspect. Future studies should also investigate possible influence of location of universities on pro-social values and cyber crime.

Acknowledgements

We appreciate all our participants who spared their time to be part of the study.

References

Adejoh, S. O., Temilola, O. M., & Adejuwon, F. F. (2018). Rehabilitation of drug abusers: the roles of perceptions, relationships and family supports: *Social Work in Public Health*. doi: 10.1080/19371918.2018.1469063

Adeniran, A. I. (2008). The Internet and emergence of yahoo-boys sub-culture in Nigeria. *International Journal of Cyber Criminology, 2*(2), 368–381.

Akers, R. L. (2009) *Social Learning and Social Structure: A General Theory of Crime and Deviant*. US: Transaction Publishers.

Akers, R. L., Krohn, M. D., Lanza-Kaduce L., & Radosevich, M. (1979). Social Learning and Deviant Behaviour: A Specific Test of a General Theory, *American Sociological Review, 44*, 636-655

Akers, R. L. (1990). Rational Choice, Deterrence and Social Learning Theory in Criminology: The Path Not Taken, *Journal of Criminal Law and Criminology*, *81*(3), 653-676.

Akiwowo, A. A. (1983). *Ajobi and ajogbe: variations on the theme of sociation*. Ife: University of Ife Press.

Arimi, C. N. (2011). *Social-economic factors influencing the crime rate in Meru Municipality, Kenya*. University of Nairobi Research Archive.

Árpád, I. (2013). A greater involvement of education in fight against cyber crime. *Procedia -Social and Behavioural Sciences, 83*, 371 – 377.

Atwal, A. (2011). Youth cyber crime influenced by peers. Retrieved from https://youthtoday.org/2011/06/youth-cyber crime-influenced-by-peers.

Cohen, A. (1966). Politics of the kola trade: some processes of tribal community formation among Migrants in West African towns. Africa. *Journal of the International African Institute, 36*(1), 18-36.

Daily post Newspaper (2018). EFCC arrests six "'yahoo boys"' in Abuja. Retrieved from http://dailypost.ng/2018/05/15/efcc-arrests-six-yahoo-boys-abuja.

Esiri, M. O. (2013). The influence of peer pressure on criminal behaviour. IOSR Journal of *Humanities and Social Science, 21*(1), 8-14.

Harnischfeger, J. (2006). State decline and the return of occult powers: the case of Prophet Eddy in Nigeria. *Magic, Ritual, and Witchcraft (Summer 2006)*. University of Pennsylvania Press.

Hirschi, T. (1969). *Causes of delinquency*. Berkeley: University of California Press.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2012) Social Learning and Cyber-Deviance: Examining The Importance of a full Social Learning Model in Virtual World. *Journal of Crime and Justice*, *33*(2), 31-61.

Ibrahim, S. (2016).Social and contextual taxonomy of cyber crime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice, 47*, 44-57.

Ige, O. A. (2008). *Secondary school students' perceptions of incidences of Internet crimes among school age children in Oyo and Ondo States, Nigeria*. A Masters dissertation in the Department of Teacher Education, University of Ibadan.

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics, 40*, 14–26.

Lee, G., Akers, R., & Bong, M. J. (2004) Social Learning and Structural Factors in Adolescent Substance Use, *Western Criminology Review*, *5*(1), 17-34.

McCall, J. C. (2004). Juju and justice at the movies: vigilantes in Nigerian popular video. *African Studies Review, 47*, 51-67.

Melvin, A. O., Ayotunde, T., (2010). Spirituality in cyber crime ("“yahoo yahoo”") activities among youths in South West Nigeria. In: *Youth Culture and Net Culture*: *Online Social Practices* (pp. 357–376). Hershey, PA, USA: IGI Global.

Ninalowo, A. (2016). *Nexus of state and legitimation crisis*. Lagos: Prime Publications.

Nsofor, J. U. (2013). Causes and effects of campus cults on Nigerian educational system, *Journal of the Nigerian Sociological Society, 2*(1), 139-142.

Nwolise, O. B. C. (2012). *Spiritual dimension of human and national security*. Eighteenth Faculty Lecture Series, Faculty of the Social Sciences, University of Ibadan (April 26, 2012).

Ojedokun, U. A., & Eraye, M. C. (2011). Socioeconomic lifestyles of the yahoo-boys: a study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology*, *6*(2), 1001–1013.

Payne, N. (1992). Towards an emancipatory sociology: abandoning universality for the true indigenization. *International Sociology, 3*, 161-70.

Reckless, W. C. (1981). Containment theory: An attempt to formulate a middle-range theory of crime. In. I. L. Barak-Glantzet.al (Eds.), *Mad, the Bad, and the Different*, (pp. 67-75). New York: Lexington Books.

Rubin, A. (1989). *Art as Technology: the arts of Africa, Oceania, native America, Southern California*. In A. Rubin and Z. Pearlstone (Eds.). *Art as Technology: the arts of Africa, Oceania, native America, Southern California* (pp. 133-38.) Beverley Hills, CA: Hilcrest, Pr.

Silverman, D. (2013). *Doing qualitative research (4th ed.)*. London: Sage Publications.

Simpson, G. E. (1980). *Yoruba religion and medicine in Ibadan*. Ibadan University Press.

Sutherland, E. (1939). *Principles of Criminology*. Chicago: University of Chicago Press.

Tade, O., & Aliyu, I. (2011).Social organization of Internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology*, *5*(2), 860–875.

Talbot, P. A. (1923). *Life in Southern Nigeria*. London: Macmillan.

Unrau, Y. A., Gabor, P. A., & Grinnell, R. M. (2006) *Evaluation in Social Work: the Art and Science of Practice*. Oxford: Oxford University Press.

Vander Ven, T., & Cullen, F. T. (2004). The Impact of maternal employment on serious youth crime: does the quality of working conditions matter? *Crime and Delinquency*, *50*(2), 272-291.

Wolff, N. H. (2000). The use of human images in Yoruba medicines. *Ethnology,* 39(3), 205-224.

World Bank (2018). *Poverty and Shared Prosperity 2018: Piercing Together The Poverty Puzzle*, Washington D.C., The World Bank