Tools, Techniques and Underground Networks of Yahoo-Boys in Ibadan City, Nigeria

*Usman Adekunle Ojedokun, Ph.D.**
Lecturer
Department of Sociology
University of Ibadan

Ayomide Augustine Ilori
Ph.D. Candidate
Department of Sociology
University of Ibadan

Abstract

Despite the fact that the online criminal activities of Nigerian cyberfraudsters popularly known as the Yahoo-boys has attracted tremendous scholarly attention, little empirical information exists on their operational tools, techniques and underground networks. Hence, this study was motivated by the need to fill this observed gap. Social learning theory was adopted as theoretical guide while in-depth interview was principally deployed for data collection. Snowball sampling technique was utilized for the selection of 11 Yahoo-boys operating in Ibadan city. The results showed that Yahoo-boys who became wealthy through cyber fraud perpetration were being imitated by their peers who saw them as role models. Two major categories of operational tools were generally deployed by the Yahoo-boys for crime commission and illicit cash flows. Underground online forums, foreign criminal contacts and abroad-based criminal associates constituted the major sources of their operational tools and positively reinforced them towards cyber fraud. Yahoo-boys invested huge capital in the procurement of operational tools because they positively defined cyber fraud as a profitable business. There is the need for global law enforcement agencies and relevant international cybercrime-fighting institutions to constantly review and analyze the latest tools and techniques being employed by cyberfraudsters to effectively curtail their illegal activities.

Keywords

Cyberfraudsters, Cybercrime, Cyber fraud, Tools, Techniques, Underground Networks, Yahoo-boys, Nigeria

* Direct correspondence to Usman Adekunle Ojedokun, Ph.D., Lecturer, Department of Sociology, University of Ibadan; uaojedokun@gmail.com.
* http://dx.doi.org/10.36889/IJCJ.2021.003.
* Received 8 March 2021; Revised 19 May 2021; Accepted 20 May 2021; Available online 2 June 2021.
INTERNATIONAL JOURNAL OF CRIMINAL JUSTICE, Vol. 3 Issue 1, June 2021, 99-122

INTRODUCTION

The notoriety of Nigerian cyberfraudsters popularly known as the Yahoo-boys has consistently positioned Nigeria among the major cybercrime hubs in the world. Indeed, different international organizations and law enforcement agencies such as the United Nations Office on Drugs and Crime (UNODC), the International Criminal Police Organization (INTERPOL), the Federal Bureau of Investigation (FBI) amongst others have over time attested to the criminal ingenuity and the devastating transnational socio-economic impacts of Nigerian cyberfraudsters (Aderinto & Ojedokun 2017; Ibrahim 2016; Internet Crime Complaint Centre 2014; This Day, 2016).

Yahooboyism, a term which emerged in Nigeria in the early 2000s, is locally used to describe a criminal subculture of youths involved in cyber fraud perpetration (Adeniran 2008; Ajayi 2019; Ojedokun 2010). The criminal exploits of Yahoo-boys are not only recognized by the federal government of Nigeria to be a serious problem, they have also become a major cause for concern for other cyberspace users worldwide (Ojedokun & Eraye 2012; This Day 2016). In August 2019, FBI arrested a Nigerian cybercrime syndicate in the United States of America that defrauded its victims of approximately $3 billion through fraudulent wire transfers, business email compromise (BEC) frauds, and dating/romance scams (Oladimeji, 2019; Premium Times, 2019). Similarly, the Dubai Police in June 2020 apprehended a suspected cybercriminal gang headed by a Nigerian for allegedly planning and engaging in cyber fraud worth AED 1.6 billion ($435 million) on a global scale (Vanguard, 2020). Furthermore, the Nigeria Deposit Insurance Corporation's (NDIC) 2014 report stated that frauds on the e-payment platform of the Nigerian banking sector increased by 183% between 2013 and 2014 alone (This Day, 2016).

Despite the fact that the online criminal activities of Nigerian cyberfraudsters have attracted tremendous scholarly attention (Jegede, Elegbeleye, Olowookere & Olorunyomi 2016; Ogunleye, Ojedokun & Aderinto 2019; Tade & Aliyu 2011), there is paucity of empirical information on the tools, techniques and underground networks that this group of criminals are relying upon for the facilitation and sustenance of their criminality. Hence, a study of this nature is significant because

it is capable of promoting knowledge and deepening public understanding about a grossly unresearched aspect of cyber-criminality.

Generally, tools, techniques and underground networks constitute important resources for criminal enterprises (Andress & Winterfield 2014; Hutchings & Benham-Hutchings, 2009). Pastrana, Hutchings, Caines and Butterfly (2018) state that cyber-criminality is to a great extent driven by an active underground economy where attack tools and services are not only being traded, but where cyberattacks are also monetized. Similarly, Portnoff et al. (2017) assert that cybercriminals usually rely on underground cyber forums to establish trade relationships and facilitate the exchange of illicit goods and services such as stolen credit card numbers, compromised hosts, and online credentials.

Allodi (2017) claims that the rise of cyber-security challenges coincides with the emergence of underground economy where attack tools and services are easily accessible at low cost or even for free. In their own contribution, Sood and Enbody (2013) identify the three major types of actors in the underground cyber community as including the providers or producers, the advertisers, and the buyers. Pastrana et al. (2018) maintain that the sense of anonymity associated with underground forums as well as the ease of access to attack tools and services which they offer make them attractive to cybercriminals. In the same vein, Leukfeldt, Kleemans and Stol (2017) note that underground forums offer an environment where cybercriminals are able to learn new tricks and plan attacks as well as search for co-offenders with specific knowledge, and procure criminal tools. Some of the items that are most commonly traded in the underground cybermarket include offline and online payment accounts (such as PayPal, cash, Ukash and Pay-Safe-Cards etc.), datasets, credit card numbers, online currencies, compromised accounts, and drugs (Portnoff et al., 2017; Motoyama, McCoy, Levchenko, Savage & Voelker 2011).

Aneke et al. (2020) identify the major cyber-attack techniques and tools of cybercriminals as including botnets (use for spreading malwares automatically), fast flux (use for transferring information to computers sending malwares so as to make it hard to track the originating source), zombie computer (this is a computer system already hacked into that is being used to distribute malicious malwares), denial of service attack (this involves overfilling a computer network or server with lots of data or messages so as to hinder legitimate users from using it),

skimmers (this technique involves using a smart computer device to steal personal credit card information from unsuspecting owners), and social engineering (this is a manipulative way of playing tricks on the minds of potential targets in order to make them give out sensitive and personal information).

Gordon, Hosmer, Siedsma and Rebovich (2002) assert that cyber weapons and tools would continue to pose serious threat to the Internet and all users of network computers as they are mainly used to exploit the weaknesses inherent in the design of computer procedures and protocols. Cárdenas, Radosavac, Grossklags, Chuang and Hoofnagle (2009) observe that though some of the tools that are essential for the perpetration of cybercrime can be procured in the underground market; some tools can be specifically developed and used solely by members of closed criminal groups as a way of gaining competitive advantage over other criminals. Gordon et al. (2002) mention that authors of cyber weapons and tools generally do find it relatively easy to develop and release updated versions of their products because they usually collaborate with other deviant peers in the open-source project environments. Against this background, the central concern of this study was to investigate the tools, techniques and underground networks of Yahoo-boys in Ibadan city, Nigeria.

Theoretical Framework

The propositions of social learning theory as put forward by Ronald L. Akers provided the theoretical guide for this research. Social learning theory is essentially a combination of differential association and behavioral learning theories (Akers & Jennings, 2016). It posits that crime is a learned behavior that results from the interaction of four principal components which are differential association, definitions, differential reinforcement and imitation. Differential association constituent of the theory connotes that people's interaction with others vary in frequency, duration, priority and intensity with the most essential interactions being those involving intimate personal groups such as family and friends. Thus, associations that occur early in life (priority), last longer (duration), take place more often (frequency), and/or involve people with whom the individual is closely attached (intensity) will have a greater effect on an individual's definitions and subsequent behavior (Akers & Sellers, 2013). Definitions entail the meanings, attitudes, values and orientations which people

attach to crime and deviance as well as conforming behavior, while differential reinforcement centers on the balance of the perceived, experienced, or anticipated reward(s) and punishment(s) that would likely accompany or follow the exhibition of a particular kind of behaviour (Akers & Jennings, 2016). Therefore, behaviors that are frequently exhibited and frequently rewarded (and highly reinforced) are those behaviors that individuals are likely to continue to choose to perform (Akers & Jennings, 2016). Imitation involves engaging in a behavior after observing someone else committing a similar act (Holt, Burruss & Bossler, 2012). Thus, social learning theory submits that individuals are more likely to choose criminal behavior over conforming behavior when they differentially associate with those who expose them to deviant patterns, when the deviant behavior is differentially reinforced over conforming behavior, when they are more exposed to deviant compared to conforming models, and when their own definitions favorably dispose them towards committing deviant acts (Akers & Sellers, 2013). In essence, the theory assumes that a dual directional relationship exists between deviance and conformity, because they are both essentially influenced by the process of modelling and reinforcement. Yahoo-boys are not only relying on their offline and online contacts as their main sources of knowledge and information on the techniques for perpetrating cyber fraud, they are also banking on their social networks for the procurement of essential tools and resources used for facilitating their illegal acts on the cyberspace.

Study Area and Study Population

Ibadan city was the location selected for this research. It is a prominent city in Southwestern Nigeria. Ibadan is the capital of Oyo State and has a population size of about 3,565,108 people (World Population Review, 2020). The choice of Ibadan was predicated on the fact that it is among the cities with high record of cyber fraud in Nigeria (Akanle & Shadare, 2019; PM News, 2021). Equally, the officials of the Economic and Financial Crimes Commission (EFCC) which serves as the law enforcement agency saddled with the responsibility of monitoring and investigating financial crimes in Nigeria had arrested and prosecuted youths involved in cyber fraud within Ibadan city at different points in time (Oyewale 2020; The Guardian 2020). The study population was constituted by youths involved in the perpetration of cyber fraud.

METHODOLOGY

This study was exploratory and cross-sectional in design. Data collection lasted over a period of four months between September and December, 2020. Qualitative method was principally deployed for the elicitation of data. Specifically, in-depth interviews involving face-to-face informal chats were conducted with 11 youths involved in the perpetration of cyber fraud via the aid of a voice recorder. Snowball sampling technique was employed for the selection of the respondents. As regards the procedure for data collection, it is pertinent to point out that eliciting data from the Yahoo-boys was particularly challenging because many of them were skeptical about the intention of the researchers because of the increasing monitoring of their activities by EFCC officials. The researchers had to visit major bars widely reputed as relaxation spots of youths involved in cyber fraud perpetration in Ibadan city and contact was successfully established with one of the Yahoo-boys after about four weeks of frequent visits to those locations. After the initial interactions and confidence-building process, this particular contact agreed to be interviewed and also introduced the researchers to two of his associates. Linkage was subsequently established with other respondents through referral facilitated by these initial contacts.

Generally, interviews were conducted with the respondents at afternoon period (between 1:00pm and 4:00pm) in their chosen locations during weekdays and on weekends subject to their availability. The scheduling of the interviews for afternoon period was essentially necessitated by the fact that youths involved in cyber fraud are usually busy on the Internet at night hours so as to be able to connect and interact with some of their potential victims who are resident in countries with different time zones. Thus, they often need to sleep late into the afternoon. Moreover, it was difficult to interact with them in the evening because that was the period of the day they normally used to unwind. Typically, Yahoo-boys prefer not to be ‘disturbed’ while having fun.

As regards data analysis, the generated tape-recorded data were subjected to manual content analysis involving careful transcription, detailed description and interpretation. Specifically, data were thematically analyzed, explored and

interpreted in line with the research objectives. Also, the verbatim quotation of some of the important responses given by the respondents in the course of the interviews was done to further enhance the lucidity of discourse.

Ethical Consideration

The conduct of this research was strictly guided by the international ethical standard for the conduct of social research. The informed consents of the respondents were sought and obtained before their participation. Also, the objectives of the research were clearly and carefully explained to them. Equally, they were informed of their rights to withdraw from further participation in the interview whenever they deemed necessary. Furthermore, none of the respondents was subjected to any form of harm, coercion or intimidation before, during and after data elicitation. Generally, conscious efforts were made at every stage of the research to protect the identity, rights and integrity of the study participants.

RESULTS AND DISCUSSION

In this section, the major results that emanated from this research are thematically presented and discussed. The themes covered included the factors underlying Yahoo-boys' involvement in cyber fraud, their pathways to cyber fraud techniques and skills as well as the types, sources and costs of their operational tools.

Factors Underlying Yahoo-Boys' Involvement in Cyber Fraud

Information was sought from the Yahoo-boys on the reasons underlying their involvement in cyber fraud as a way of understanding the push and pull factors that attracted them to the crime. All of them attributed their involvement in cyber fraud to a similar reason. One of them remarked:

> My motivation mainly comes from some of my guys that are already balling hard (living ostentatious lifestyles) and driving big cars worth between $11795.54 and $13106.16 (N 4,500,000 and N5,000,000). Can you imagine a 19year-old-boy buying a car (Camry Muscle model) worth about $6,553.08 (N2,500,000) through proceeds gained from his hustle (cyber

> fraud)? The boy in question is my friend's younger brother. So, if one sees all the paparazzi and flexing (glamours and glitz) of guys who are into hustle in one's neighborhood every day, one will also want to try it (cyber fraud). That is what we call ginger (inspiration) (IDI/Yahoo-boy/Male/Yoruba/9years in practice/Aluminum Fabricator/Ibadan).

Another respondent said that:

> Every Yahoo-boy in this game is inspired whenever he sees his friend making a big hit from hustling (cyber fraud perpetration). I am usually motivated whenever any of my friends makes huge proceeds. If he makes it big this week, I can also cash-out from my own hustle next week. In essence, I get inspired by the exploits of my guys who are also in the game (cyber fraud). We are sources of inspiration to one another (IDI/Yahoo-boy/Male/Yoruba/6years in practice/Agriculturalist/Ibadan).

Below is another respondent's submission:

> When there is no financial assistance from one's family, one just needs to keep hustling with others to make it. Also, if one has many friends who are into it (cyber fraud) and one decides not to join them in hustling, they will be calling one all sorts of derogatory names. They would see one as being foolish (IDI/Yahoo-boy/Male/Yoruba/7years in practice /Accountant/Ibadan).

It can be established from the above submissions that Yahoo-boys were mainly motivated to engage in cyber fraud by the desire to get rich like their friends and peers who became wealthy through the perpetration of the crime. A few of the respondents also adduced their involvement in the illegal act to lack of financial support from their family members. The implication of this finding is that Yahoo-boys who became wealthy through cyber fraud were being imitated by

their peers who saw them as their role models. Ojedokun and Eraye's (2012) study established that Yahoo-boys are widely known as maintaining a distinctive socio-economic lifestyle which confers a unique identity on them in Nigerian society. Moreover, Ojedokun (2010) and Tade and Aliyu (2011) separately discovered that many youths in Nigeria were attracted to cyber fraud by the desire to get rich and peer pressure. Furthermore, this finding supports the propositions of the differential association, definitions and imitation constituents of social learning theory. Yahoo-boys were mainly motivated to engage in cyber fraud as a result of differentially associating with friends and peers who were also involved in the criminal act themselves and who also attached positive meanings, attitudes, values and orientations (definitions) to cyber fraud perpetration. Equally, they revered their friends and peers who became wealthy through cyber fraud (modelling) and were consequently inspired to imitate their criminal behavior. Skinner and Fream's (1997) study which analyzed computer crime among a sample of college students similarly revealed that associating with peers who indulge in cybercrime was the strongest predictor for perpetrating cybercrime, while definitions that are favorable to adhering to the law are negatively related to perpetrating cybercrime.

Cyber Fraud Techniques and Skills Acquisition Pathways of the Yahoo-Boys

To gain adequate insights into the underground networks of the Yahoo-boys, investigation was conducted into how they acquired the techniques and skills which they usually deploy for the perpetration of fraud on the cyberspace. All the respondents affirmed that they learnt cyber fraud techniques and skills from their friends and peers who were already established cyberfraudsters. In one of the interviews conducted, a Yahoo-boy stated:

> In this game (cyber fraud), you have to learn from someone. Everything about this hustle (cyber fraud) boils down to the connection one has and the area of the hustle which one wants to learn because Gee-boys know that Yahoo Yahoo (cyber fraud) goes beyond what is being done on Facebook, Instagram and so on. So, for a newcomer, the starting point is to learn from a person that would tell you

> what you really need to know because Yahoo Yahoo is not something that you will just decide to go into without being properly tutored. For my own training, I learnt a lot of things from my own boss who is like an area brother to me. I started with the creation and use of United States citizens' Facebook account profiles. There are so many processes to it (cyber fraud). So, one just has to seek information from those who truly know. It is not about what you just know on your own as an individual (IDI/Yah oo- boy/Male/Yoruba/10years in practice/Graduate/Ibadan).

In one of the interviews, a respondent declared:

> I feel the most important thing in this hustle (cyber fraud) is to have someone who is very knowledgeable about it and willing to show one the way. At the training stage, there are certain things one needs to have so as to facilitate a successful learning process. For instance, there are some logs or log-ins that one needs to buy because there are some access-restriction sites that someone residing in Nigeria will not be able to access. It is through these log-ins that one would be able to access such sites. All this process involves constant training and learning. I learnt from my friends (IDI/ Yahoo-boy /Male/Igbo/6years in practice/Undergraduate/Ibadan).

A respondent explained:

> I was introduced into the hustle (cyber fraud) by my childhood friend. He is someone that I look up to because he has made it big. He has always encouraged me to hammer (become rich) like him. However, my parents tried to separate us when they got to know that he is into Gee (cyber fraud) (IDI/Yahoo-boy/Male/Igbo/7years in practice/Un dergraduate/Ibadan).

It can be inferred from the above narratives that learning from social networks (friends and acquaintances) played important role in the respondents' acquisition of cyber fraud techniques and skills. Yahoo-boys attach serious importance to learning criminal techniques and skills from established cyberfraudsters because they recognized the fact that cyber fraud is a complex crime that cannot be successfully perpetrated by a novice who has not been strategically initiated and socialized into its intricacies. This result supports the submission of Leukfeldt (2014) that social relationships is very important for the recruitment and growth of cybercriminal networks. Also, Leukfeldt et al. (2017) have similarly stated that the role which social ties play in the origin and growth of cybercriminal networks cannot be overemphasized. This finding also validates the differential association and imitation aspects of social learning theory. Friends and acquaintances of Yahoo-boys' did not only play prominent roles in their initiation into cyber fraud, but equally constituted the most important nodes for the transmission of ideas, knowledge, skills and techniques associated with cyber fraud. Furthermore, this outcome corresponds with the research of Lee, Hong, Yoon, Peguero and Seok (2018) on correlates of adolescent cyberbullying in South Korea which found that delinquent peer association was positively associated with both cyberbullying perpetration and victimization.

Tools Commonly Used by the Yahoo-Boys for Cyber Fraud Perpetration

Criminals frequently rely on the deployment of certain tools for crime perpetration (Chiu & Leclerc, 2017; Wells & Horney, 2002). Therefore, it was deemed necessary to seek information on the essential tools commonly utilized by the Yahoo-boys. Findings indicated that Yahoo-boys were making use of both hardware and software tools for different purposes. Below is a revelation that was given by one of the respondents:

> For me, the most important tools in this business are one's phone, laptop and the Internet. Also, one needs a very strong VPN (virtual private network). If one needs to interact with people in Europe or South America, one would have to use a VPN to indicate that one is also a resident in such a country. The benefit is that it makes one real and

> legitimizes one's online profile. Also, there are many other types of tools; and their usage depends on the type of hustle (cyber fraud) one is into. For example, people involved in money transfer or account loading need to buy cheque samples and IP (Internet protocol) log-in because it is very important for them to always change their IP codes (IDI/Yahoo-boy/Male/Yoruba/11 years in practice /Self -employed/Ibadan).

Another respondent reasoned in a similar manner:

> When we are talking about tools that we normally use for this hustle, we are talking about VPN. For example, VPN basically is used to change one's location. You know many clients (potential victims) have trust issue. When they discovered that one is a Nigerian, they basically stop interacting with one. So, using a VPN would indicate that one is based in the United States of America; and clients (potential victims) would automatically believe and fall for it. They will basically believe that one is also one of them. In fact, there are some dating sites with very strict access-restriction policy for certain countries. One cannot access them without using a VPN. Sites such as Plenty of Fish (POF), Emily Dates, Match.com. amongst others. Also, there are some dating sites for which one needs to have international telephone numbers to access because they have to send one certain code to enable one to be able to successfully register. Also, we normally buy foreign SIM (subscriber identification module) cards from people willing to sell them (IDI/Yahoo-boy/Igbo/Male/7years in practice/Und ergraduate/Ibadan).

Furthermore, in terms of their illicit financial transactions, one of the interviewees explained the tools they normally use thus:

> Cash App, PayPal, and Zelle are my main tools for cash transfer. Now the ones that is becoming rampant these days among hustlers (Yahoo-boys) is bitcoin and blockchain. The app on which you save your Bitcoin is Paxful. Ethereum is another form of digital currency which one can convert to cash. There are different cryptocurrencies but the one that is high in value compared to the dollar is bitcoin. Some digital currencies are even better than bitcoin but we do not trade in them because few people own them in Nigeria (IDI/Yahoo-boy/Male/Yoruba/11 years in practice/Self-employed/Ibadan).

Also, another respondent emphasized that:

> I cannot use my normal bank account details to receive money from my clients (victims). So, I basically make use of online mobile payment apps that are not traceable like the Cash APP. It is not wise to receive money using my details or passport from the Western Union. Although this is possible, but it is not advisable because one can be easily traced (IDI/Yahoo-boy/Male/Yoruba/9years in practice /Alumi num Fabricator/Ibadan).

The above submissions of the respondents clearly demonstrate that the operational tools of the Yahoo-boys are broadly in two categories which are: (a) tools for facilitating crime commission on the cyberspace (such as laptop, mobile phone, printer, Internet, virtual private network (VPN), Internet protocol (IP) log-ins, and cheque samples) and (b) tools for driving illicit cash flows (such as Bitcoin, Blockchain, Cash App, Ethereum, Paypal, and Zelle). A major deduction that can be made from this finding is that both hardware and software tools being utilized by the Yahoo-boys for cyber fraud perpetration were not originally created and/or designed for illegitimate purposes. Rather, Yahoo-boys are converting them from their primary status as legitimate resources to criminal tools. In February 2021, the Central Bank of Nigeria, the apex monetary authority in Nigeria, banned the use of cryptocurrencies claiming that they are increasingly being employed for money laundering, financial terrorism and other criminal

activities (Komolafe, 2021). The implication of finding this is that criminals would always find a way of exploring the downside of any technological breakthrough to facilitate crime perpetration. This outcome is in line with the observation of Gordon et al. (2002) that cybercriminals are increasingly utilizing tools primarily designed for legitimate usage for the commission of cybercrime. Also, this finding brings to bear the relevance of the concepts of definitions and differential reinforcement aspects of social learning theory. Yahoo-boys were positively oriented towards cyber fraud because they recognized the usefulness and values embedded in the adoption of diverse operational tools. More so, their access to some operational tools which can be employed to deflect the risk of being detected and/or apprehended provided them with negative reinforcement as they aided them to avoid potential punishments that their online criminality attracts. Furthermore, this result is similar to the outcome of Ogunleye, Ojedokun and Aderinto's (2019) study which revealed that female undergraduate cyber fraudsters operating in south-west Nigeria capitalized on the wider interconnectivity and interactive advantages presented by the ubiquity of social media platforms after learning and acquiring essential knowledge and skills on ways to clandestinely deploy information and communication technology (ICT) resources for fraudulent activities from their brothers and boyfriends.

Means Through Which Yahoo-Boys Sourced for their Operational Tools

Studies conducted elsewhere have established that cybercriminals usually procure their attack-tools and other illicit criminal commodities in the underground cyber market (Leukfeldt et al., 2017; Pastrana et al., 2018). Thus, it was considered important to investigate how Yahoo-boys operating in Ibadan city usually source for their operational tools. Nearly all the respondents submitted that they normally procure cyber fraud tools from their international contacts and through underground online forums. One of the interviewees expressed that:

> To get some of these operational tools, one just need to search anonymous (unicc.ru). When one searches for anonymous on Google, one would be able to make right contact with hackers. For example, if one wants to buy a credit card now, one just need to search anonymous. One

> can get these tools at cheap prices all over the world. For example, just type I need so and so in Mexico, then google the anonymous in Mexico. It is a done deal (IDI/Yahoo-boy/ Male/Yoruba/11 years in practice/Self-employed/Ibadan).

A respondent also commented:

> There are some contacts who have turned legit (criminal accomplice) over time. These people normally helped us to get whatever tool and information we need over there in the U.S. There are some clients who have turned legit to the extent that they know the kind of person they are interacting with in terms of nationality and country of residence. If there is a strong connection between one and the person (contact), one can start colluding with him/her to get any vital tools that one needs. For instance, such contact(s) can help one get an American SIM card. He or she would then courier same through the DHL or any other means of delivery to Nigeria. U.S. SIM is very useful, and that is why most Yahoo-boys prefer to use iPhone. iPhone will support such a SIM card in Nigeria (IDI/Yahoo-boy /Male/Yoruba/Agriculturalist/6years in practice/Ibadan).

Another interviewee stated that:

> We do get our vital tools and information from people like us. That is their own area of hustle (cyber fraud). They are hackers - they hack into so many things. For example, they hack to get clients' credit card information. They will then give us the 14 digits at the front side of the card and the CVV (card verification value) number. There are some hackers that normally assist us when we need SSN (social security number) and residents' dates of birth. We do get these tools through online buying and selling. In fact, there are some hackers that can conveniently sell companies'

> accounts information to us. They usually give us details of such accounts, and we will pay them in return. One will then make use of such sensitive information to transfer money from the company whose account had been so compromised to one's client (potential victim) account. It could take up to one week before the affected company detects such a move. By that time, one would have received such a cash from one's client. Of course, he or she (client) would be subsequently arrested (IDI/Yahoo-boy/Male/Yoruba/ 8years in practice/Accountant/Ibadan).

It can be deduced from the above submissions that Yahoo-boys mainly sourced and procured their operational tools from underground online forums, foreign criminal contacts and abroad-based criminal associates. This result does not only demonstrate the increasing organized transnational dimension of cyber fraud, but it equally showcases the way through which cyberfraudsters are exploiting the power of both virtual and social networks to gain access to illicit resources. This outcome is in tandem with Portnoff et al.'s (2017) study which found that cybercriminals were relying on forums not only for the initiation of trade relationships, but also for facilitating the exchange of illicit goods and services. Another major implication of this finding is that the relatively easy means through which tools and resources essential for the perpetration of cyber fraud can be procured from underground online forums and other criminal networks will continue to negatively impact the Nigerian government's efforts at controlling the illegal online activities of the Yahoo-boys. Gordon et al. (2002) have equally asserted that cyber tools and weapons will continue to pose serious threat to the Internet and all users of networked computers. This result also demonstrates the efficacy of social learning theory. Yahoo-boys mainly gained access to their illicit resources from delinquent peers with whom they associated. However, despite the fact that Yahoo-boys' duration and intensity of interactions with their foreign criminal contacts and abroad-based criminal associates played important role in their bonding, they were less significant in their sourcing for operational tools in underground online forums where relationships are mainly transactional and transient. Hollinger's (1993) research on correlates of software piracy and unauthorized account access similarly established that individuals are more likely

to engage in computer crimes as the number of friends they have who also engage in such illegal activities increases.

Cost of Cyber Fraud Operational Tools of the Yahoo-Boys

Respondents were also probed on the cost associated with the procurement of their operational tools as a way of gaining insights into the extent of their financial investment in the illegal act. Generally, all of them submitted that the cost of their operational tools is largely dependent on the type of cyber fraud they intend to perpetrate. One of the Yahoo-boys explained that:

> It (cost of procurement) is dependent on the way you interact with people that have such tools. There are Some tools one does not need to pay for. They will just give one for free. And even if one needs to buy, most tools are not too costly to get. You could purchase a tool of $5 (N2,000.00) or $7 (N3,000.00) to facilitate a hustle that could yield like $100 (N40,000.00) (IDI/Yahoo-boy/Male/Yoruba/11 years in practice/Self-employed/Ibadan).

Also, a respondent mentioned:

> The cost of procurement of tools depends on the area of hustle you are engaging-in. For instance, if one wants to load an account, there are some tools that one can purchase for about $786.36 (N300, 000) or more. If one wants to buy a log-in or a spam, one can purchase either of them for about $786.36 (N300,000). They are costly because they contain all the details that one needs. The only thing that one needs to do is just to shoot the target account. For example, one can only purchase a Wells Fargo account from hackers in the dark web. Although I can buy it for about $786.36 (N300,000), but I can make up to $2621.23 (N1,000, 000) using it (IDI/Yahoo-boy/Male/Yoruba/7 years in practice /Undergraduate/Ibadan).

An interviewee equally said:

> One can get a VPN for $4 (N1,500.00) or $10 (N4,000.00). If one wants to buy a cheque, it is dependent on how genuine it is. A cheque of $20 (N8,000.00) will be more genuine than a cheque of $10 (N4,000.00), a company's account of $100 (N40,000.00) will be more genuine than that of $50 (N20,000.00). At times, one can buy some that are expensive and get scammed. Sellers can still scam one. There are also some Yankee citizens' hacked Facebook accounts that are sold with malwares as operational tools (IDI/Gee boy/Male/Yoruba/Over 7years in practice /Accounta nt /Yoruba/ Ibadan).

It can be established from this result that though the cost of operational tools is largely dependent on the type of cyber fraud to be perpetrated. Yahoo-boys are investing capital in their procurement because they have seen cyber fraud as a profitable business that has the potentials for yielding huge financial gains. Thus, the potential reward is seen as higher than the cost of investment. A major implication of this finding is that Yahoo-boys may not be easily discouraged from perpetrating cyber fraud by the prescribed negative sanctions it attracts because they see the cost of investing in the crime as very cheap when compared with the potential rewards derivable from it. This result affirms the position of Allodi (2017) that the rise of cybersecurity incidents coincides with the development of the underground economy where attack tools and services are easily accessible at low cost or even for free. It equally demonstrates the validity of social learning theory. Yahoo-boys were positively reinforced towards perpetrating cyber fraud because the anticipated rewards which they associated with the deployment of certain operational tools for cyber fraud far outweighs their cost of procurement. Furthermore, this output is in tandem with Shadmanfaat et al.'s (2019) study among University of Guilan undergraduates which found that an individual's sense of personal and social gain from engaging in cyberbullying is directly related to engaging in cyberbullying perpetration.

Limitations of the Study and Suggestions for Future Research

A major limitation of this study lies in the small population size of the Yahoo-boys that were interviewed. Thus, the small size of the study population may negatively impact the overall generalizability of the major findings. Equally, it exclusively focused on male youths involved in the perpetration of cyber fraud. Consequently, the perspectives of their female counterparts on the subject matter were not taken into account. Therefore, future studies focusing on this aspect of cyber-criminality should expand their scope in terms of size of sample and the gender composition of respondents as a way of further enriching the diversity of respondents' submissions. However, in-spite of these identified limitations, this study expands the frontiers of knowledge by providing significant insights into an important aspect of cyber-criminality that had hitherto been a neglected area of research. Equally, it provides an important comparative benchmark that will be beneficial to future studies focusing on the tools, techniques and underground networks of cybercriminals particularly from the viewpoint of social learning theory.

CONCLUSION

The online criminal activities of Yahoo-boys are not only negatively impacting Nigeria in multiples ways, they also constitute serious socio-economic threats to other Internet users worldwide. For this reason, it is expedient to suggest some useful strategies that can be adopted to combat their illegal acts. At the global level, it is important for national governments to design durable and effective strategies through which the use of international online payment systems and digital currencies primarily designed for legitimate financial transactions and monetary exchange purposes can be properly monitored, regulated and secured. This step becomes imperative as a practical means of combatting the criminal activities of cyber-fraudsters that are utilizing these international monetary transactions platforms to perpetrate money laundering and drive illicit cash flows. Also, the dominant role which underground online forums and international criminal networks played on the availability of some operational tools and illicit resources aiding the perpetration of cyber fraud underscores how transnational criminal networks are promoting the occurrence of cybercrime and threatening the online activities of other Internet users. Therefore, it is important for global law enforcement agencies and relevant international cybercrime-fighting institutions to forge strategic alliance and collaboration for the purpose of constantly reviewing and analyzing the latest operational tools and techniques being employed by cyberfraudsters as a way of combatting their criminal activities and the threats posed by the underground cyber economy.

At the national level, it is germane for the National Orientation Agency of Nigeria, the government agency charged with the promotion of values, morals and patriotism among Nigerians to champion the cause for values reorientation among Nigerians by consistently launching massive public campaigns against youth involvement in cyber fraud perpetration while simultaneously promoting the value of hard work. This can be achieved through strategic collaboration and partnership with the mass media and other agents of socialization, particularly family and school as well as religious bodies. Finally, apprehended cyberfraudsters should be promptly prosecuted by law enforcement agents, and the punishments meted out to them in the court of law should be giving as much publicity as possible so as to discourage other youths from engaging in cyber fraud perpetration.

References

Adeniran, A. I. (2008). The Internet and emergence of Yahooboys sub-culture in Nigeria. *International Journal of Cyber Criminology, 12*(2), 368–381.

Aderinto, A. A., & Ojedokun, U. A. (2017). Cyber underground economy in Nigeria. In P. Ndubueze (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 219-228). Ahmadu Bello University Press, Limited, Zaria.

Ajayi, T. M. (2019). Anti-language, slang and cyber scam subculture among urban youth in southwestern Nigeria. *International Journal of Cyber Criminology, 13*(2), 511-533.

Akanle, O., & Shadare, B. R. (2019). Yahoo-plus in Ibadan: Meaning, characterization and strategies. *International Journal of Cyber Criminology*, *13*(2), 343-357.

Akers, R. L., & Jennings, W. G. (2016). Social learning theory. *The handbook of criminological theory*, 230-240.

Akers, R. L., & Sellers, C. S. (2013). *Criminological theories: Introduction, evaluation, and application* (6th edition). New York: Oxford University Press.

Allodi, L. (2017, October). Economic factors of vulnerability trade and exploitation. *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security* (pp. 1483-1499).

Andress, J., & Winterfeld, S. (2014). *Cyber warfare: techniques, tactics and tools for security practitioners*. Elsevier Inc.

Aneke, S. O., Nweke, C. N., Udanor, I. A…Ezema, M. E. (2020). Towards determining cybercrime technology evolution in Nigeria. *International Journal of Lates Technology in Engineering, Management and Applied Science*, *ix*(iv), 37-43.

Cárdenas, A., Radosavac, S., Grossklags, J., Chuang, J., & Hoofnagle, C. J. (2009). An economic map of cybercrime. Retrieved from https://papers.ssrn.com/soI3/papers.cfm?abstract_id=1997795.

Chiu, Y. N., & Leclerc, B. (2017). An examination of sexual offenses against women by acquaintances: The utility of a script framework for prevention purposes. In: Crime prevention in the 21st century (pp. 59-76). Springer, Cham.

Gordon, G. R., Hosmer, C. D., Siedsma, C., & Rebovich, D. (2002). Assessing technology, methods, and information for committing and combating cybercrime. Retrieved from https://www.ojp.gov/pdffiles1/nij/grants/198421.pdf.

Hollinger, R. C. (1993). Crime by computer: Correlates of software piracy and

unauthorized account access. *Security Journal, 4*, 2-12.

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 the virtual world. *Journal of Crime and Justice*, *33*(2), 31-61.

Hutchins, C. E., & Benham-Hutchins, M. (2010). Hiding in plain sight: Criminal network analysis. *Computational and Mathematical Organization Theory*, *16*(1), 89-111.

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

Internet Crime Complaint Centre. (2014). The internet crime complaint report - 2014. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2014_ IC3 Report.pdf

Jegede, A. E., Elegbeleye, A. O., Olowookere, E. I., & Olorunyomi, B. R. (2016). Gendered alternative to cyber fraud participation: An assessment of technological driven crime in Lagos State, Nigeria. *Gender & Behavior, 14*(3), 7672-7692.

Kayode-Adedeji, D. (2019, August 29). Nigeria: EFCC arrests suspect who 'assisted' Nigerian cyber-crime syndicate in U. S. *Premium Times*. Retrieved from https://www.premiumtimesng.com/news/more-news/349261 -efcc-arrests-sus pect-who-assisted-nigerian-cyber-crime-syndicate-in-u-s.html

Komolafe, B. (2021, February 8). Cryptocurrency ban is to protect Nigerians, financial system– CBN. *Vanguard*, February 8. Retrieved from https://www.vanguardngr.com/2021/02/cryptocurrency-bans-to-protect-nigeria ns-financial-system-cbn/

Lee, J. M., Hong, J. S., Yoon, J., Peguero, A. A., & Seok, H. J. (2018). Correlates of adolescent cyberbullying in South Korea in multiple contexts: A review of the literature and implications for research and school practice. *Deviant Behavior, 39*(3), 293-308.

Leukfeldt, E. R. (2014). Cybercrime and social ties: Phishing in Amsterdam. *Trends in Organized Crime*, *17*, 231–49

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). Origin, growth and criminal capabilities of cybercriminal networks: An international empirical analysis. *Crime, Law and Social Change*, *67*(1), 39-53.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011, November). An analysis of underground forums. *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference* (pp. 71-80).

Ojedokun, U. A. (2010). *Cybercrime and changing lifestyle among students of*

some selected universities in south western Nigeria (Unpublished master's thesis). University of Ibadan, Ibadan, Nigeria.

Ojedokun, U. A., & Eraye, M. C. (2012). Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology 6*(2), 1001-1013.

Ogunleye, Y. O., Ojedokun, U. A., & Aderinto, A. A. (2019). Pathways and motivations for cyber fraud involvement among female undergraduates of selected universities in south-west Nigeria. *International Journal of Cyber Criminology*, *13*(2), 309-325.

Oladimeji, R. (2019, October 8). Cyber fraud: Court orders Invictus Obi's 280m forfeited. *The Punch*. Retrieved from https://www.punchng.com/cyber-fraud-court-orders-invictus-obis-n280m-forfeited/

Oyewale, W. (2020, October 3). EFCC arrests 10 suspected yahoo boys in Oyo. *The Punch*. Retrieved from https://www.punchng.com/efcc-arrests-10-suspected-yahoo-boys-in-oyo/

Pastrana, S., Hutchings, A., Caines, A., & Buttery, P. (2018, September). Characterizing Eve: Analyzing cybercrime actors in a large underground forum. Proceedings of *international symposium on research in attacks, intrusions, and defenses* (pp. 207-227). Springer, Cham. Retrieved from https://doi.org/10.1007/978-3-030-00470-5_10.

PM News. (2021, January, 20). EFCC arrests seven "Yahoo Yahoo boys" in Ibadan. *PM NEWS*. Retrieved from http://pmnewsnigeria.com/2021/01/20/effc-arrests-seven-yahoo-yahoo-boys-in-ibadan/

Portnoff, R. S., Afroz, S., Durrett, G., Kummerfeld, J. K., Berg-Kirkpatrick, T., McCoy, D., ...& Paxson, V. (2017, April). Tools for automated analysis of cybercriminal markets. *Proceedings of the 26th international conference on world wide web* (pp. 657-666). Retrieved from https://dl.acm.org/doi/abs/10.1145/3038912.3052600.

Shadmanfaat, S., Howell, C. J., Muniz, C. N., Cochran, J. K., & Kabiri, S. (2019).Cyberbullying perpetration: An empirical test of social learning theory in Iran. Deviant Behavior. doi: 10.1080/01639625.2019.1565513.

Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college student. *Journal of Research in Crime & Delinquency, 34*, 495-518.

Sood, A. K., & Enbody, R. J. (2013). Crimeware-as-a-service—a survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection*, *6*(1), 28-38.

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

The Guardian. (2020, March 4). EFCC arrests 'Yahoo' boy with coffin, five others arrested in Ibadan. *The Guardian*. Retrieved from https://guardian.ng/news/efcc-arrests-yahoo-boy-with-coffin-five-others-in-ibadan/

This Day. (2016, April 16). Nigeria loses over N127bn annually through cybercrime. Retrieved from www.thisdaylive.com/index.php/2016/04/18/cyber-security-nigeria-loses-over-n127bn-annually-through-cybercrime/

Wells, W., & Horney, J. (2002). Weapon effects and individual intent to do harm: Influences on the escalation of violence. *Criminology*, *40*(2), 265-296.

World Population Review. (2020). Nigeria population 2020. Retrieved from https://worldpopulationreview.com/countries/nigeria-population