SOCIOLOGICAL INVESTIGATION OF FACTORS DRIVING CYBERCRIME AMONG UNDERGRADUATES WITH SEVERE IMPLICATION IN THE EDUCATIONAL SYSTEM IN NIGERIA

Falusi W. Peace[1]*, Matthew E. Egharevba[2], Tayo O. George[2]

[1]Mr., Department of Sociology, Covenant University, NIGERIA, wunmi.falusipgs@stu.cu.edu.ng

[2]Prof., Department of Sociology, Covenant University, NIGERIA, matthew.egharevba@covenantuniversity.edu.ng

[3]Prof., Department of Sociology, Covenant University, NIGERIA, tayo.george@covenantuniversity.edu.ng

*Corresponding Author

Abstract

The trend in crime participation in recent times revolves around the use of information communication technology (ICT) for its perpetuation. This development has resulted in different types of vices, including cyber-crime. The problem of cyber-crime today in Nigeria has taken root and has become pervasive among undergraduates with severe implication in the Educational System in Nigeria. The theory used for this study is Neutralization theory. The study adopted a survey design and data gathered was analyzed using descriptive and inferential statistical tools. The findings of this study identified the idea of get rich quick, bad parenting, peer influence, dishonesty, poor moral values, and family pressure as major factors driving undergraduates' involvement in cybercrime. Furthermore, it was also discovered that cybercrime has a negative impact on the nation's image and educational system in Nigeria. The study recommended that there should be increased internet security to help protect data, proper awareness about cybercrime should be implemented and also, government should put in place strict penalties on offenders as this would help curb the desire for undergraduate involvement in cyber-crime.

Keywords: Cybercrime, youths, involvement, undergraduates, perception, education.

1. INTRODUCTION

Criminal activity is not a recent phenomenon. It has existed from the beginning of time and has become a threat to human and societal development as it discourages domestic and foreign direct investments and creates a culture of fear and untold suffering among people (Clough, 2015). The challenge of cybercrime keeps growing and putting a definitive end to it remains a difficult task because such criminal acts could be carried out secretly from any part of the globe. It is against this backdrop that this study seeks to examine predisposing factors driving undergraduates' involvement in cybercrime and also identify its severe implication in the educational system in Nigeria.

Folashade and Abimbola (2013), collaborated their position when they also identified high unemployment, greed, poverty and weak educational system as variables driving undergraduate engagement in cybercrime. Babatunde & Olanrewaju (2015), identified Peer pressure as a factor too. In addition, this study findings also identified the following: quick money, bad parenting, social influence, dishonesty, poor moral values, and family pressure.

Despite the efforts of social services, law enforcers, and justice system establishments to reduce crime, the world is quickly becoming a more complicated place where homicide, abductions, burglary, attack, child molestation, indecent assault, robberies, societal crime, economic crime, political crime, and cybercrime are all prevalent. The impact of technological innovations and change, especially ICT on our daily lives and activities has increased in the last three decades. Every day, billions of people worldwide use various internet-enabled services; s Digital communication, the Website (WWW), Transmission Control Protocol (FCP), chat sessions, email lists, text messaging, chat, and news outlets were among the example. We live with our mobile devices as the primary resource for collecting data and communications in a continuously integrated society (Kotler, Kartajaya & Setiawan 2017).

The usage of Information and Communication Technology (ICT) Applications (ICT) has influenced practically every sphere of activity, including e-commerce, e-governance, finance, agriculture, education, medical, military, and transportation (ICT). In both the corporate and governmental sectors, technological progress and Internet promotion have been strengthened to achieve higher efficiency by speeding up current processes and providing new and flexible ways of carrying out various duties (Fielder 2016; Hughes 2017). This progress, however, has attracted several vices such as cybercrime, money laundering, cyberbullying and pornography.

Technological advancement in general is quickly changing the kind, size, severity, and scale of cyber fraud in Nigeria (Aderinto & Ojedokun, 2017; Tade & Aliyu, 2011; Adeniran, 2008). According to available research, the urge to choose an easy approach to generate quick and huge sums of money has resulted in cyber fraud among youngsters, particularly college students (Adeniran, 2008; Aransiola & Asindemade, 2011; Tade & Aliyu, 2011; Aghatise, 2006). Such desire is most often born from frustration due to the socio-economic condition of the respective country, lack of job opportunities and absence of means of livelihood. Based on a report released by the Economic and Financial Crime Commission (2021), 80% of its 978 convictions in 2021 were connected to cybercrime and cyber related offenses, of which youths were the culprits. In Nigeria, cyber fraud is the most common and prevalent type of cybercrime, resulting in large yearly financial and monetary losses. (2015) (Babatunde & Olanrewaju) (Anyawnu, Oforegbu, Igbo, & Obiyo, 2012) (Idehen, Ojewumi, & Olasupo, 2013) (Okeshola & Adeta, 2013, Amosun & Ige, 2009). According to the Nigeria Deposit Insurance Corporation (NDIC) annual reports for 2018, the number of suspicious transactions climbed by 44.4 percent from 26,182 in 2017 to 37,817 in 2018 and 52,754 from 2019-2020. In addition, the total amount involved in the scam jumped by 224 percent, from 12.01 billion naira ($31.6 million) in 2017 to 38.93 billion naira ($102.4 million) in 2018. (NDIC, 2018). E -payment channels powered by the internet and technological advancements, such as Paypal, Amazon Pay, Prepaid cards, and Apple Pay, among others, are the causes of these fraud and forgeries, which were done not only by individuals operating outside of the system, but also by financial institutions (Ibrahim, 2014; NDIC 2018).

According to Jegede, Oyesomi, and Olorunyomi (2013) and Popoola (2021), cyber fraud is a huge threat to the current global economy because of its appeal to criminal groups ranging from individuals who conduct basic fraud to big organized crime operations. Nigeria has a reputation for being a refuge for cyber-enabled fraudulent operations (Ebenezer, Paula & Allo, 2016). According to a report by the Nigerian Communication Commission (NCC, 2017), Nigeria is ranked as the third highest country in cybercrime activities worldwide. This raises a question on the factors promoting such activities within the country. According to Folashade & Abimbola (2013), Babatunde & Olanrewaju (2015), Igba & Nwambam (2018), poverty, get rich quick syndrome, and peer pressure are factors propelling undergraduates' involvement in cyber-crime. On the other hand, Okeshola & Adeta (2013) identified defective socialization, weak laws, unrestricted access to the internet as major factors encouraging cyber-crime. However, for Tade and Aliyu (2011), the greed, porous nature of the internet and lack of e-policing are some of the major factors that responsible for the perpetuation of cyber-crime.

The consequence of cybercrime activities on Nigeria's educational system is undergraduates dropping out of schools, getting arrested, leading to poor academic performance and defamation of its national image and prestige. If not controlled, cybercrime is completely impotent and will bring poor integrity to the educational sector. Other nations now consider Nigeria as a country where cybercrime thrive and its residents are treated with contempt. Furthermore, the continued prevalence of cybercrime would intensify

the level of criminality and corruption in the country and there's a possibility of the present generation projecting a bleak future for the coming generation, making cybercrime to be a norm and excusable, so long as the perpetrator are searching for a means of survival.

1.1. Literature Review

The review of relevant literature to the topic is the emphasis of this part.

The Concept of Cybercrime

Cybercrime has become one of the fastest expanding sectors of criminal activity, as criminals increasingly stay ahead of the efficiency, ease, and confidentiality that contemporary technology provides to conduct malicious and fraudulent acts (Parodi, 2013).

2. EDUCATIONAL SYSTEM OF NIGERIA

According to WES (2017) and Egharevba (2017), educational institutions are overseen by the government and private stakeholders such as non-governmental organizations and private individuals. The federal ministry of education regulates both public and private educational establishments. Nigeria has three tiers of government: federal, state, and local. The federal and state governments oversee public tertiary and secondary institutions, while the local government oversees public, pre-primary, and primary schools. Previously, the Nigerian educational system was structured using the 6-3-3-4 formula, which stands for one year pre-primary, six years primary, three years junior secondary, three years senior secondary, and four years university education. Tertiary education includes institutions such as universities, polytechnics, and educational college.

2.1. The Effect of Cybercrime on Educational System of Nigeria

According to George et al, (2021) and Oyebade (2019), the impact of cybercrime on undergraduates is that it tarnishes their reputation, the integrity of their school, and the reputations of their parents and guardians; as a result, students who are caught are sometimes paraded in front of news reporters. The introduction of social media has made cybercrime more widely known among Nigerian young. This has considerably increased the temptation to participate in cybercrime as a result of witnessing the lavish lifestyle widespread on social media, at clubs, and at other social gatherings while being uninformed of the hazards involved with such money. Some pupils even quit out to join the online criminal organization.

3. RESEARCH METHODS

This section focuses on the methodology used to carry out this study and achieve its aims. It describes the research design, study population, sample size, sampling process, data collecting equipment, accuracy and reliability of data collection instrument, and data processing.

3.1. Research design

This study will adopt descriptive Research Design. The method intends to gather information about people's experiences, opinion, and attitudes on the subject matter under investigation. The sample size for this study is 329. This number was shared across the 12 faculties in UNILAG in relation to their population.

3.2. Population of the Study

The population of this study includes students of the University of Lagos, Akoka, Lagos State.

3.3. Sampling Techniques

The study's participants will be people (both male and female) aged 18 and up, from the selected university (The University of Lagos). The multistage sampling procedure will be used, which involves purposive selection of a public university based on their population. The qualities of the needed sample dictated the use of each procedure. Similarly, respondents were chosen at random from various departments or faculties at the chosen institution. The sample size for the study was shared across the 12 faculties in UNILAG in relation to the population of each faculty.

3.4. Sources and Methods of Data Collection

This study's structured questionnaire was sent to undergraduate students at the University of Lagos. There were five (5) sections in the structured questionnaire. Section one focuses on the respondents'

socioeconomic factors. Section two discussed students' awareness of cybercrime activities. The final section dealt with questions on the various sorts of cybercrime among students. The fourth segment included questions about the socioeconomic repercussions of cybercrime activities on student lifestyles. The fifth segment is concerned with the influence of cybercrime on Nigeria's educational system.

This study's questionnaire is a self-administered structured questionnaire with open and closed-ended questions. The questionnaire was distributed in 329 copies for the investigation. The questionnaire was delivered to each of UNILAG's twelve faculties in proportion to their population.

3.5. Method of Data Analysis

Questionnaire data was examined using descriptive statistics. With the help of the Statistical Package for the Social Sciences (SPSS) version 28, the collected data were explained using frequencies and percentages.

3.6. Response Rate

The table below shows the response rate from the questionnaire administered to students of UNILAG.

Table 4.1: Questionnaire Administered and Response Rate

	Frequency	**Percentage**
Retrieved questionnaire	306	93%
Unretrieved questionnaire	23	7%
Total Questionnaire Administered	329	100%

Source: Field Survey (2022)

As shown in Table 4.1, 329 questionnaires were administered, out of which the researcher retrieved 306 (representing 93%), whereas 23 (representing 7%) of the administered questionnaire is not retrieved. Thus, only 93% retrieved were utilized for analysis in this study.

Table 2: Socio-demographic characteristics of respondents

Variables	Items	Frequency	Percentage (%)
Gender	Male	164	53.6
	Female	142	46.4
	Total	306	100.0
Age group	18-22	118	38.6
	23-27	149	48.7
	28-32	39	12.7
	Total	306	100.0
Academic Level	100l	78	25.5
	200l	125	40.8
	300l	67	21.9
	400l	31	10.1
	500l	5	1.6
	Total	306	100.0
Academic Sponsor	Parents	170	55.6

	Guardian	73	23.9
	Self	58	19.0
	Scholarship	1	.3
	Others	4	1.3
	Total	306	100.0
Religion	Christianity	207	67.6
	Muslim	98	32.0
	Traditional	1	.3
Ethnicity	Igbo	77	25.2
	Yoruba	204	66.7
	Hausa	16	5.2
	Edo	4	1.3
	Ibibio	3	1.0
	Efik	2	7
	Total	306	100.0

Source: Field survey (2022)

This table shows the socio-demographic characteristics of the respondents according to their sex. It is clear that 54 percent of responders were males, while 46 percent were females; this suggests that males outnumbered females.

The table shows that 37% of the respondents were within the age range of 18-22 years while 49% were within the age range of 23-27 years and 13% were within the age range of 28-32.

From the table above, the academic level for the respondents showed that, 26% were in 100level, 41% were in 200level, 22% were in 300level, 10% were in 400level, and 2% were in 500level.

The table shows that parents sponsor 56% of students; Guardians sponsor 24% of the students, 19% sponsor themselves while, 3% of the students are on scholarship basis and 1.3% have other forms of sponsorship not listed on the table.

The distribution according to the table ethnicity indicate that response of 25.2% were Igbo, 66.7% are Yoruba, 5.2% are Hausas, 1.3% come from Edo, .7% are from Efik and 1.0% belong to the Ibibio ethnic group.

Table 5: Distribution of consequences of cybercrime to the Nigerian Educational system

S/N	Statement	SA		A		D		SD		Total
		F	%	F	%	F	%	F	%	F(%)
1	Crimes perpetuated through the internet has emerged as a significant contributor to the economic meltdown	125	40.8	71	23.2	72	23.5	38	12.4	306 (100%)
2	Is the economic impact of cybercrime devastating/alarming	106	34.6	98	32.0	71	23.2	31	10.1	306 (100%)

3	Some youth go as far as withdrawing from school to join the pyramid of cyber criminals.	106	34.6	69	22.5	89	29.1	42	13.7	306 (100%)
4	Undermines economic growth of nation	107	35.0	95	31.0	66	21.6	38	12.4	306 (100%)
5	Defamation of image of nations and people as corrupt and rogue or thieves	157	51.3	63	20.6	36	11.8	50	16.3	306 (100%)

Source: Field Survey (2022)

In determining the consequences of cybercrime on the society and Its implication to education system in Nigeria, five statements were put forward to elicit responses from the respondents. For the first statement 64% of the respondents agreed with this while 35.9% disagreed. The responses to the second statement showed that 66.6% agreed and only 33.3% disagreed. Majority of the respondents (57.1%) agreed that cybercrime reduces the competitive edge of organizations, while 42.8% of the respondents disagreed. 66% of the respondents agreed that cybercrime makes Some youth go as far as withdrawing from school to join the pyramid of cyber criminals, whereas 34% of those polled disagreed Finally, 71.9 percent agreed that cybercrime tarnishes the nation's image, while just 28.1 percent disagreed.

4. CONCLUSION AND RECOMMENDATIONS

The findings of this study identified lack of jobs, poverty, greed, social influence, quick money, family pressure, and poor moral values as the major factors responsible for undergraduate's involvement in cyber-crime. According to the study's findings, the study recommends to combat cybercrime in our society and enhance Nigeria's educational system. These are some examples:

1. There is a need for a value re-orientation of our youths, particularly undergraduates through the diverse social institutions particularly the family, which is the first point of a child's socialization, should ensure that good morals and values are inculcated in our young ones growing and those in higher institutions.

2. The Government should put in place strict penalties for offenders and enforce those laws accordingly; this would help curb youth interest in cyber-crime.

3. All schools should return to teaching values in order to instill in all pupils a sense of stewardship, while lecturers live lives that represent truth, kindness, labor dignity, and honesty.

5. ACKNOWLEDGMENT

REFERENCE LIST

Adesina, S. O. (2017). Cybercrime and Poverty in Nigeria. Canadian social science, 13(4), 19-29.

Andeme Bikoro, D. M., Fosso Wamba, S., & Kala Kamdjoug, J. R. (2018). Determinants of cyber security use and behavioral intention: Case of the Cameroonian public administration. Advances in Intelligent Systems and Computing, 1087-1096. doi: 10.1007/978-3-319-77712-2_104

Babatunde, M. M., & Olanrewaju, K. M. (2015). Peer Pressure, Parental Socioeconomic Status, and Cybercrime Habit among University Undergraduates in Southwestern Nigeria. International Journal of Technology in Teaching & Learning, 11(1).

Clough, J. (2015). Principles of cybercrime. doi: 10.1017/cbo9781139540803/

Cullen, F. T., & Wilcox, P. (2010). Sykes, gresham m., and david matza: techniques of neutralization. In Encyclopedia of criminological theory (Vol. 1, pp. 920-926). SAGE Publications, Inc., https://dx.doi.org/10.4135/9781412959193.n254.

Cohen, R., Lam, D. Y., Agarwal, N., Cormier, M., Jagdev, J., Jin, T. … Wexler, M. (2014). Using computer technology to address the problem of cyberbullying. ACM SIGCAS Computers and Society, 44(2), 52-61. doi:10.1145/2656870.2656876

Ebenezer, J. A. (2014). Cyber risks and Fraud in the Nigeriaâ€™s business environment: A postmortem of youth crime. Journal of Social and Development Sciences, 5(4), 258-265. doi:10.22610/jsds.v5i4.825

Ebenezer, A. J., Paula, A. M., & Allo, T. (2016). Risk and Investment Decision Making in the Technological Age: A Dialysis of Cyber Fraud Complication in Nigeria. International journal of cyber criminology, 10(1), 67-78. Retrieved from DOI: 10.5281/zenodo.58522

Egharevba, M.E. (2017). Demographic dynamics, governance and the attainment of democratic development: The case of Nigeria. Etude de la Population African. 31(1): 3769-3786.

Folashade B. & Abimbola K. (2013). The nature, causes and consequences of cyber-crime in tertiary institutions in Zaria-Kaduna State, Nigeria. American International Journal of Contemporary Research, 3(9), 14-17.

George, T.O., Oladosun, M., Oyesomi, K., Ajayi, L. (2021). Usefulness and expectations on skills development and entrepreneurship among women of low socioeconomic status in Ogun State, Nigeria. African Journal of Reproductive Health. (Special Issue). 25(5) Pp. 171-187

Hassan, B. A., Lass, D. F., & Makinde J. (2012). Cybercrime in Nigeria: causes, effects and the way out. ARPN Journal of Science and Technology, 2(7), 626-631.

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. International Journal of Law, Crime and Justice, 47, 44-57. doi:10.1016/j.ijlcj.2016.07.002

Idom, M. A., & Tormusa, O. D. (2016). Causes, types, and likely victims of cybercrimes in selected higher institutions, south South, Nigeria. FULafia Journal of Social Sciences, 1(1), 202, 218.

Lange R., & Burger, W. E. (2017). Long-term market implications of data breaches, not. Journal of Information Privacy and Security, 13(4), 186-206.

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

Matthew, O., Adeniji, A., Osabohien, R., Olawande, T., & Atolagbe, T. (2020). Gender   inequality, maternal mortality and inclusive growth in Nigeria. Social Indicators   Research, 147(3), 763-780.

Odo, R. C., & Odo, I. A. (2015). The extent of involvement in cybercrime activities among students' in tertiary institutions in Enugu State of Nigeria. Global Journal of Computer Science and Technology.

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

Okeshola, B. F., & Adeta, K. A. (2013). The nature causes and consequences of cyber-crime in tertiary institutions in Zaria-Kaduna state, Nigeria. American International Journal of Contemporary Research, 3(9), 98-114.

Ololade, B. M., Salawu, M. K., & Adekanmi, A. D. (2020). E-Fraud in Nigerian Banks: Why and How?. Journal of Financial Risk Management, 9(3), 211-228.

Onimisi, C. A., & Nonyelum, O. F., F. O. (2018). Evaluation and Analysis of Cyber Attacks in Nigeria. IUP Journal of Information Technology, 14(1).

Pettalia, J. L., Levin, E., & Dickinson, J. (2013). Cyberbullying: Eliciting harm without consequence. Computers in Human Behavior, 29(6), 2758-2765. doi:10.1016/j.chb.2013.07.020

Popoola, R.O., Egharevba, M.E., & Fayomi, O.O. (2021). Democratic governance, gender, and women's rights in Nigeria: 1999-2019. African Journal of Reproductive Health. (Special Issue). Pp. 188-201.

Sutherland E. (1939). Principles of Criminology (4th ed.). Chicago: Philadelphia J.B. Lippincott Company.

Tade O. & Aliyu I. (2011). Social organization of Internet fraud among university undergraduates in

Nigeria. International Journal of Cyber Criminology, 5(2).

Taiwo, C. O., & Igbekoyi, E. K. (2019). Prevalence and consequences of cybercrime perpetrated by students in Public Tertiary Institutions in Ekiti State. International Journal Of Arts, Languages And Business Studies, 2(1).

Wenr.wes.org/2017/03/education-in-nigeria.