Exploring the Causes, Trends and Social Impact of Cybercrime Among Youths in South Eastern Nigeria

Adaeze B. Ekwochi[1*], Ohita P. Asije[2], Iveren B. Agbo[3], Goodness James[4], Opeyemi O. Famodimu[5], Smart T. Obiajunwa[6]

[1]National Open University, Nigeria

[2]University of Ibadan, Nigeria,

[3]Nigerian Defence Academy, Nigeria

[4]Babcock University, Nigeria,

[5]Babcock University, Nigeria,

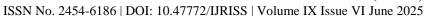**[6]Nasarawa State University, Nigeria**

[*]Corresponding Author

ABSTRACT

This study examined the causes, trends and social impact of cybercrime among youths in south eastern Nigeria. Methodology: Relevant data were drawn from selected one hundred (100) students across various departments in Federal University of Technology Owerri, using a well-structured questionnaire. Findings of the study revealed that factors that drive youths into cybercrime in the area include: unemployment, peers influence, quest for wealth/get rich quick syndrome, lack of internet security and poor parental supervision, among others. Study conclusion and policy recommendations: The study concluded that youths' involvement in cybercrime is influenced by various factors, and if properly contained will have a positive effect on the nation. The government, family, and youths all have a vital role to play in this contest, collective action could better the interest of future existence, regain international reputation and promote the nation economy. Regulating the abusive usage of the internet, social media just like china, japan, and other world power will go a long way to check the excesses of cyber risk. Based on the findings, it was recommended among others that Individuals should adopt basic cybersecurity measures to protect themselves from cyber threats, strict law enforcement and deterrence measures must be meted out on cybercriminals and finally the government and private organizations should establish skill acquisition programs and entrepreneurship initiatives to provide alternative sources of income for youths constructively reducing the lure of cybercrime.

Keywords: Cybercrime, Youths, Crime, Economic Financial Crime Commission, Federal University of Technology, Owerri.

INTRODUCTION

Almost every institution in many societies has seen significant changes as a result of the internet's explosive global growth in the twenty-first century. Nonetheless, there are both positive and negative aspects to these shifts. While the positive aspects of the internet revolution are intriguing, the negative aspects are overwhelming and frequently result in illnesses that jeopardize the social order of society (Ibikunle & Eweniyi, 2013; Odumesi, 2014; Okeshola & Adeta, 2013). The rise in cybercrimes is one of the detrimental effects of the internet revolution worldwide, particularly in developing countries like Nigeria. In the view of Odumesi (2014) In addition to causing a sharp rise in the frequency of cybercrimes, the development of technology and online communications has also given rise to what seems to be a new range of criminal activity. According to
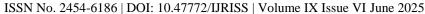
Das and Nayak (2013) Cybercrime, which includes anything from electronic cracking to denial-of-service attacks, is a crime primarily conducted by individuals or organized groups in which computers or computer networks are used as a tool, a target, or a location for illicit activity. Using contemporary telecommunication networks like the internet (Chat rooms, emails, etc.) and mobile phones, cybercrimes also include offences committed against individuals or groups of individuals with the criminal intent to purposefully damage the victim's reputation or cause them physical or mental harm directly or indirectly (Muraina & Muraina, 2015). Denial of service attacks, cyber-theft, cyber trespass, cyber obscenity, critical infrastructure attacks, online fraud, online money laundering, ID fraud, cyber terrorism, and cyber extortions are a few examples of cybercrime, according to Kshetri (2010). Since they are so common, cybercrimes are neither wholly new nor exclusive to underdeveloped countries like Nigeria. In the United States (U.S.), the first widely reported cybercrime happened in November 1988 when a 23-year-old student named Robert Morris posted a virus online known as the "Morris Worm." Of the 60,000 or so systems connected to the Internet at the time, more than 6,000 computers were compromised, and fixing the compromised systems cost over $100 million. As a consequence, Morris got a sentence of 3 years' probation and a $10,000 fine (McAfee, 2009). Cybercrime thus progressively developed as a significant worldwide issue. For example, data theft and cybercrime cost businesses globally over $1 trillion in 2008 in lost intellectual property. Internet-related criminal activity caused losses of approximately $559.7 million, according to the 2009 World Internet Crime Report published by the Internet Crime Complaint Centre (ICC) (2010). This represents a substantial increase from the $264.6 million and $239.1 million reported losses in 2007 and 2008, respectively. In the meantime, the median financial loss in the 146,663 cases that IC3 referred for investigation in the US was $575 million and involved alleged fraud. Once more, the amount is more than the $264.6 million in 2008. It is important to remember that cybercrime is linked to age. In other words, since young people are more likely to commit cybercrimes, the issue is more widespread in developing countries like Nigeria. According to Ndubueze, Igbo and Okoye (2011) a number of factors are thought to be connected to young people's involvement in cybercrime.. Ndubueze, Igbo and Okoye (2011) noted that cyber criminals are mostly people between the ages of 20- 35 years. Okeshola and Adeta (2013) also asserted that cyber-crime is often more prevalent among youths who are males. To buttress this, Internet Crime Complaint Centre (ICC) (2010) revealed that a higher percentage of cybercriminals were men. A number of other factors have been identified by other studies, including exposure to or access to computer/internet facilities, the pursuit of quick wealth, unemployment, the absence of cybercrime laws, underequipped law enforcement agencies, negative role models, the pursuit of socio-political recognition or fame, frustration, corrupt politicians' displays of wealth, and laziness (Okeshola & Adeta, 2013). Furthermore, one cannot hastily draw the conclusion that crimes like cybercrime are common in all societies. This is because, as far as the researcher is aware, there haven't been many studies on the incidence of cybercrime in the setting of south east Nigeria. Therefore, in the context of the current study field, there is a knowledge deficit about the study's theme. It is against this backdrop that this study is positioned to examine cybercrime among youths in eastern Nigeria: causes trends and social impact.

Computer programs are meant to be used to help young people develop their technical knowledge and abilities in a variety of fields, including art, commerce, and—most importantly—technological advancement. The situation in Nigeria, however, has been the opposite. Previous research has demonstrated that youth cybercrimes have increased significantly in various regions of Nigeria (Oluwadare, Oluwasunmi & Igbekoyi, 2018); and occurs in daily bases. The government, religious organizations, and other security organizations have frequently taken notice of the issue and are working to develop rules and procedures that could reverse this tendency. For example, according to the Cybercrime Act of 2015, any person or group of people found guilty of hacking or gaining unauthorized access to a computer system or network faces a fine of up to ten million (N10 million) naira or a five-year jail sentence, depending on the reason for the hack. However, the rise in cybercrime has resulted in a sharp increase in the number of energetic young people engaging in more active types of cybercrime, which places a significant burden on society as a whole. Its impact on victims' physical and mental health as well as the nation's image cannot be overstated. In the setting of eastern Nigeria, one of the most well-known commercial areas in Southeast Nigeria, where many young people work tirelessly to make ends meet, the issues mentioned above might not be out of the ordinary. Additionally, it is feared that as the cybercrime industry grows in popularity and flourishes in Nigeria, more young people will join in, worsening the situation and inevitably having a negative impact on the long-term viability of the Nigerian economy as well as the youths' contribution to socioeconomic development. Therefore, this study aims to

systematically investigate public opinion of the tendency, specifically in south eastern Nigeria, as a means of preventing this undesirable trend. This is in light of the fact that, as far as the researcher is aware, significant research efforts have not been directed towards this field of study, especially in the setting of eastern Nigeria. It is therefore, against this backdrop that this study is positioned.

METHODOLOGY

This study adopted the descriptive survey design as the strategy or plan of action regarding events upon which implementation will enable the researcher to investigate the problem of this study. In this study, structured questionnaire was used as research instrument. For the uniqueness and peculiarity of the subject of the study, the quantitative method of data collection was employed in order to get accurate and reliable information. The design is suitable for this study because data was collected from respondents using questionnaires to give an assessment of cybercrime among youths, its trend, causes and impact on society. The questionnaire is structured for Likert scale questionnaires in such a way that it provides answers to the research questions. The study was conducted in the Federal University of Technology, Owerri, Nigeria. A sample of one hundred (100) youths will be randomly selected and questionnaire will be administered to them. The sample size was calculated using the Taro Yamani scientific formula which is given as:

$$n = \frac{N}{1 + N(e)^2}$$

Where:

N is the Population

1 is the constant

e is the degree of error expected

n is the sample size

$$n = \frac{133}{1 + 133(0.05)^2}$$

$$\frac{133}{1 + 133(0.0025)}$$

$$\frac{133}{1 + 0.3325}$$

$$\frac{133}{1.3325}$$

$$n = 100$$

The quantitative data obtained from the field were processed and analyzed using descriptive statistics such as simple percentages, tables and frequency distribution. Data obtained from respondents through the administration of questionnaires was collated and analyzed using Statistical Package for Social Sciences (SPSS Version 20.0).

DATA ANALYSIS, FINDINGS AND DISCUSSION

Table 1: Unemployment is a driver of cybercrime among youths					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	40	40.0	40.0	40.0
	Agree	50	50.0	50.0	90.0
	Undecided	2	2.0	2.0	92.0
	Disagree	5	5.0	5.0	97.0
	strongly disagree	3	3.0	3.0	100.0
	Total	100	100.0	100.0	

Source: Field survey, 2025.

Table 1 shows the responses of respondents that Unemployment is driver of cybercrime among youths. 40 respondents representing 40.0 percent strongly agree that Unemployment is driver of cybercrime among youths. 50 respondents representing 50.0 percent agree that Unemployment is driver of cybercrime among youths. 2 respondents representing 2 percent were undecided.

Table 2: Poor parenting encourages cybercrime among youths					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	50	50.0	50.0	50.0
	Agree	30	30.0	30.0	80.0
	Undecided	5	5.0	5.0	85.0
	Disagree	10	10.0	10.0	95.0
	strongly agree	5	5.0	5.0	100.0
	Total	100	100.0	100.0	

Source: field survey, 2025.

Table 2 shows the responses of respondents that Poor parenting encourages cybercrime among youths. 50 respondents representing 50.0 percent strongly agree that Poor parenting encourages cybercrime among youths.30 respondents representing 30.0 percent agree that Poor parenting encourages cybercrime among youths. 5 respondents representing 5 percent were undecided.

Table 3: Quest for wealth/get rich quick syndrome causes cybercrime among young people					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	40	40.0	40.0	40.0
	Agree	30	30.0	30.0	70.0
	Undecided	15	15.0	15.0	85.0
	Disagree	10	10.0	10.0	95.0
	strongly disagree	5	5.0	5.0	100.0
	Total	100	100.0	100.0	

Source: Field survey, 2025.

Table 3 shows the responses of respondents that Quest for wealth/get rich quick syndrome causes cybercrime among young people. 40 respondents representing 40.0 percent strongly agree that Quest for wealth/get rich quick syndrome causes cybercrime among young people . 30 respondents representing 30.0 percent agree that Quest for wealth/get rich quick syndrome causes cybercrime among young people. 15 respondents representing 15.0 percent were undecided.

Table 4: Peer pressure is a major cause of cybercrime also known as "yahoo yahoo" among youths in Eastern Nigeria

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	50	50.0	50.0	50.0
	Agree	30	30.0	30.0	80.0
	Undecided	5	5.0	5.0	85.0
	Disagree	10	10.0	10.0	95.0
	strongly agree	5	5.0	5.0	100.0
	Total	100	100.0	100.0	

Source: Field survey, 2025.

Table 4 shows the responses of respondents that Peer pressure is a major cause of cybercrime also known as "yahoo yahoo" among youths in eastern Nigeria. 50 respondents representing 50.0 percent strongly agree that Peer pressure is a major cause of cybercrime also known as "yahoo yahoo" among youths in eastern Nigeria.30 respondents representing 30.0 percent agree that Peer pressure is a major cause of cybercrime also known as "yahoo yahoo" among youths in eastern Nigeria. 5 respondents representing 5 percent were undecided.

Table 5: Reputation damage is a consequence of cybercrime among youths in Eastern Nigeria

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	40	40.0	40.0	40.0
	Agree	30	30.0	30.0	70.0
	Undecided	15	15.0	15.0	85.0
	Disagree	10	10.0	10.0	95.0
	strongly disagree	5	5.0	5.0	100.0
	Total	100	100.0	100.0	

Source: Field survey, 2025.

Table 5 shows the responses of respondents that reputation damage is a consequence of cybercrime among youths in eastern Nigeria. 40 respondents representing 40.0 percent strongly agree that reputation damage is a consequence of cybercrime among youths in eastern Nigeria. 30 respondents representing 30.0 percent agree that reputation damage is a consequence of cybercrime among youths in eastern Nigeria. 15 respondents representing 15.0 percent were undecided.

Table 6: Cybercrime can lead to legal consequences, such as fines, lawsuits, and imprisonment

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	50	50.0	50.0	50.0
	Agree	25	25.0	25.0	75.0
	Undecided	5	5.0	5.0	80.0
	Disagree	10	10.0	10.0	90.0
	Strongly disagree	10	10.0	10.0	100.0

	Total	100	100.0	100.0	

Source: Field survey, 2025.

Table 6 shows the responses of respondents that cybercrime can lead to legal consequences, such as fines, lawsuits, and imprisonment.50 respondents representing 50.0 percent strongly agree that cybercrime can lead to legal consequences, such as fines, lawsuits, and imprisonment. 25 respondents representing 25.0 percent agree that cybercrime can lead to legal consequences, such as fines, lawsuits, and imprisonment. 5 respondents representing 5.0 percent were undecided.

Table 7: Government should provide employment opportunities for the youth					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	40	40.0	40.0	40.0
	Agree	50	50.0	50.0	90.0
	Undecided	2	2.0	2.0	92.0
	Disagree	5	5.0	5.0	97.0
	strongly disagree	3	3.0	3.0	100.0
	Total	100	100.0	100.0	

Source: Field survey, 2025.

Table 7 shows the responses of respondents that the government should provide employment opportunities for the youths. 40 respondents representing 40.0 percent strongly agree that government should provide employment opportunities for the youths. 50 respondents representing 50.0 percent agree that government should provide employment opportunities for the youths. 2 respondents representing 2 percent were undecided.

Table 8: Adequate and strict punishment for fraudsters should be implemented by the government					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	40	40.0	40.0	40.0
	Agree	30	30.0	30.0	70.0
	Undecided	15	15.0	15.0	85.0
	Disagree	10	10.0	10.0	95.0
	strongly disagree	5	5.0	5.0	100.0
	Total	100	100.0	100.0	

Source: Field survey, 2025.

Table 8 shows the responses of respondents that adequate and strict punishment for fraudsters should be implemented by the government. 40 respondents representing 40.0 percent strongly agree that adequate and strict punishment for fraudsters should be implemented by the government. 30 respondents representing 30.0 percent agree that adequate and strict punishment for fraudsters should be implemented by the government. 15 respondents representing 15.0 percent were undecided.

Table 9: Proper education and awareness should be created on ways to prevent cybercrime					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly agree	40	40.0	40.0	40.0
	Agree	30	30.0	30.0	70.0
	Undecided	15	15.0	15.0	85.0
	Disagree	10	10.0	10.0	95.0

strongly disagree	5	5.0	5.0	100.0
Total	100	100.0	100.0	

Source: Field survey, 2025.

Table 9 shows the responses of respondents that Proper education and awareness should be created on ways to prevent cybercrime. 40 respondents representing 40.0 percent strongly agree that Proper education and awareness should be created on ways to prevent cybercrime. 30 respondents representing 30.0 percent agree that Proper education and awareness should be created on ways to prevent cybercrime. 15 respondents representing 15.0 percent were undecided.

DISCUSSION OF FINDINGS

The findings from this study revealed that greater percentage of the respondents support the point that there are several causes of cybercrime among youths in south eastern Nigeria including unemployment, poor parenting, quest for wealth/get rich quick syndrome, and peer pressure. This is in line with the study by Boyu (2016) who investigated the driving factors of cybercrime among youths in Onitsha South Local Government Area (L.G.A), Anambra State, Nigeria. Findings of the study revealed that factors that drive youths into cybercrime in the area include: unemployment, peers influence, quest for wealth/get rich quick syndrome, poverty, greed, lack of internet security and poor parental supervision, among others.
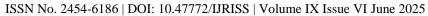
Furthermore, the findings reveals the consequences of Cybercrime among youths in south eastern Nigeria. The consequences include moral decadence and reputational damage. This is in line with the research by Muraina, & Muraina (2015) on cybercrime among youths in Nigeria: Causes, Effects and the Way Out. They assert that cybercrime involves using computers and Internet by individuals to commit crime. The effects of cybercrimes on organizations, the society and the country in general include reducing the competitive edge of organizations, waste of production time and damage to the image of the country. With Nigeria venturing into cashless society, there is a need for cybercrimes menace to be minimized if not completely eradicated.

Finally, the result obtained establishes the ways of curbing cybercrime among youths in south east. This is determined from the responses of the obtained where greater of the respondents strongly agree and agree to this fact respectively. Some of the ways cybercrime can be reduced include the provision of employment opportunities for the youths to keep them busy such as organizing vocational trainings that can equip them with skills to earn a living. Also, the study reveal that enforcing strict punishment on internet fraudsters by the law enforcement agencies should be highly encouraged as it will deter prospective cybercriminals from engaging in the act. Finally, proper education and awareness should be created on ways to prevent cybercrime. The study can be traced to Meke Eze Stanley (2012) who examined cybercrime and strategies for reducing its menace among Nigerian youth through proper implementation of cyber security and employment creation.

CONCLUSION AND RECOMMENDATIONS

Nigeria has lost so much reputation and bilateral trade options from foreign nations. The businesses and investment which was supposed to get into the country goes away because of the huge presence of cybercrime and cybercriminals who lure potential foreign investors and dump them subsequently. It is glaring and obvious that cybercrimes cannot be easily eliminated, but it can certainly be minimized with the collaborative efforts of all stakeholders like individuals, corporate organizations and government to nip the scourge in the bud. It is vital that Nigeria as a nation takes measures to make sure that its penal and procedural laws are adequate to fulfill the challenges posed with the aid of cybercrimes. Government should make sure that regulations cybercriminal activities are formulated and strictly adhered to regardless of the repute and character of the humans involved. Also, the creation of job opportunities for the teeming unemployed youths will limit the threat drastically. Government should also make provision for intensive training of law enforcement agencies on ICT so that they can track down the cybercriminals no matter how intelligent and cunning they may be.

The study has fully shown that youths involvements in cybercrime have been necessitated by diverse reason, if properly contained will have a positive effect on the nation. The government, family, and youths all have a

vital role to play in this contest, collective action could better the interest of future existence, regain international reputation and promote the nation economy.

REFRENCES

1. Akano (2013). Cybercrime: Nigeria redeems image. The Punch. http://www.punchng.com/business/ technology/cyber-crime-nigeria-moves-to-redeem-image/ Retrieved on 10th Feburay 2013.
2. Boyu, G. (2016). Why hackers become crackers – An analysis of conflicts faced by hackers. Public Administration Research, 5(1)
3. Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. International Journal of Engineering Sciences & Emerging Technologies, 6(2), 142-153
4. Ibikunle, F., & Eweniyi, O. (2013) Approach to cyber security issues in Nigeria: Challenges and solution. International Journal of Cognitive Research in Science, Engineering and Education, 1(1) 11-114.
5. Meke Eze Stanley, N. (2012): An article "Urbanization and Cyber Crime in Nigeria: Causes and Consequences". http://www.internetworldstats.com/stats.htm last accessed l9 August 2014.
6. Muraina, M. B., & Muraina, K. O. (2015). Peer pressure, parental socioeconomic status, and cybercrime habit among university undergraduates in South-western Nigeria. International Journal of Technology in Teaching and Learning, 11(1), 50-59..
7. Muraina, M. B., & Muraina, K. O. (2015). Peer pressure, parental socioeconomic status, and cybercrime habit among university undergraduates in South-western Nigeria. International Journal of Technology in Teaching and Learning, 11(1), 50-59.
8. Ndubueze, Igbo, V., Okoye H. (2015). Does empathy predict (cyber) bullying perpetration and how do age, gender, nationality affect this relationship? Learning and individual differences, 45, 275-281.
9. Odumesi, J. O. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. International Journal of Sociology and Anthropology, 6(3), 116 – 125.
10. Okeshola F. B., & Adeta A. 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), 98-114.
11. Oluwadare, Oluwasunmi, Igbekoyi (2015). Empirical Assessment of Lifestyle Routine Activity and Social Learning Theory on Cybercrime Offending (Master of Science Thesis). In BSU Master"s Theses and Projects. Item 25.