Nsukka Journal of Communication Studies (NJCS) Volume 2, Issue 2 (2026).
Print ISSN: 2006-0785
E-ISSN: 3115-4328 https://nsukkajcs.com/index.php/NJCS/index

Artificial intelligence awareness and use in cybercrime activities among undergraduates in Enugu State, Nigeria.

Robert Chinweze E. Ezeanwu
Department of Mass Communication
University of Nigeria Nsukka, Enugu State, Nigeria
robert.ezeanwu@unn.edu.ng

Olanrewaju A. Mgboji*
Department of Mass Communication
University of Nigeria Nsukka, Enugu State, Nigeria
olanrewaju.mgboji@unn.edu.ng

Onyebuchi Udeh
Department of Mass Communication
University of Nigeria Nsukka, Enugu State, Nigeria

Chizoba Udensi
Department of Mass Communication
University of Nigeria Nsukka, Enugu State, Nigeria

***Corresponding author:** Olanrewaju A. Mgboji; olanrewaju.mgboji@unn.edu.ng

Abstract
The development of the internet has transformed communication by enhancing human communication systems within the social order in different societies making it an important part of human life. This study aims to assess artificial intelligence awareness and use in cybercrime activities among undergraduates in Enugu State. The survey research was employed, and questionnaire used for data collection. The population size comprised of 47,619 students of the University of Nigeria, Nsukka and Enugu State University of Science and Technology, from which a sample size of 382 was derived. Findings revealed that undergraduates were aware of artificial intelligence use in cybercrime and that media messages were useful and educational but not persuasive enough to ensure compliance. Despite awareness of repercussions in relation to the risks of involvement in crime and criminality, majority respondents indicated that they may still get involved. It was noted that higher motivation factors influencing youth involvement include financial incentives, unemployment and peer influence. The study recommended that media initiatives engage parents and guardians to promote a more holistic strategy for tackling youth involvements in cybercrime activities. Government and society should develop infrastructure to deter AI use and also emphasise that crime is unprofitable in order to dissuade youths from engaging in cybercrime.
Keywords: Awareness, Artificial Intelligence, Cybercrime, Undergraduates, Use.

Introduction

The influence of digital technology in society has made it critical for all students in the 21st century to become literate with the use of digital tools, the development and proliferation of the internet have contributed to the revolution in teaching and learning (Hussaini, Ibrahim,

Wali, Libata and Musa, 2020). Despite this, the rapid growth, development and evolution of digital internet, including its global acceptance is generating increasing security threats to individuals, corporations, enterprise and the government as a whole (Nwajioha and Oshim, 2025). The growing population of internet users especially the youths have escalated the incidence of cybercrime, presenting a significant threat to the national economy, infrastructure, security, governance and technology worldwide (Kshetri, 2010).

Cybercrime refers to unlawful criminal actions executed via a computer or network, serving as a tool, target, or platform for these operations (Moulton, 2010). It denotes the amalgamation of computer into network-related criminal behaviours/activities, including e-fraud, e-pedophilia and e-sexual grooming. Cybercrimes involves using modern telecommunication networks like the internet (chat rooms, emails), electronic hard and soft ware and mobile phones to intentionally harm a person or group's reputation, physical or mental health (Muraina and Muriana, 2015).

The rise of the internet computers and mobile phones in Nigeria has increased cybercrimes as criminals use anonymity to fool victims, these scammers typically mimic others and use the identities to upset family members or to trick their victims. (Ajibike, 2019). Cybercrimes include internet fraud by Yahoo boys, hacking, software piracy, pornography, credit card and ATM fraud, denial of service attacks, virus propagation, phishing, cyber-plagiarism, cyber-stalking and cyber-defamation. Cybercrime affects both the nation and the perpetrator and particularly, the "Yahoo" cybercrime, a variant of advance fee fraud aspect exacerbates the victim’s situation, which may result in depression, restless nights, suicide and a diminished sense of peace of mind (Ajibike, 2019). Das and Nayak (2013) state that cybercrime, which vary from electronic cracking to denial-of-service assaults are mostly committed by individuals or organized groups using computers or computer networks as tools, targets, or venues. It also includes denial of access to personal accounts, personality assaults,

cyber-theft, cyber trespass, cyber obscenity, attacks on essential infrastructure, online fraud, phishing, cat-fishing, money laundering, identity fraud, cyber terrorism and cyber extortion, (Kshetri, 2010).

Eboibi and Ogorugba, (2023) add that while most cybercrimes are committed for financial gain, some damage or disable computer devices, while others spread malware, illicit information, images, or other materials via computers or networks to force the victim to be defrauded. For instance, the Nigerian government arrested 1,700 men and 337 women in 2019 for advance fee fraud cybercrime in 2020 of which majority of these financial and economic offenders are mostly men (Statista, 2022). Okeshola and Adeta (2013) found a strong age-cybercrime link. Youths commit most cybercrimes, making them more prevalent in developing nations like Nigeria with high youthful population. Existing studies link some factors to teenage cybercrime and that most cybercriminals were young males (Ndubueze, Igbo and Okoye, 2011; Internet Crime Complaint Centre (ICC), 2010). Thus, it is crucial to educate young online users about cybercrime and its associated risks and research shows that young people are tech-savvy but may be unaware of online risks.

Several Nigerian teens may have employed the use artificial intelligence to aid their cybercrime activities. These actions may be influenced by several factors such as innovation, creativity, poverty and unemployment and many teenagers have also made cybercrime a career and a way of life (Brody, Kern and Ogunade, 2020). The National Bureau of Statistics (2022) reports 53.4% youth unemployment rates in Nigeria which may significantly influence their behaviour. In Nigeria, several bodies and commissions like the Economic and Financial Crimes Commission (EFCC), Independent Corrupt Practices Commission (ICPC) and Nigeria Cyber Crime Working Group (NCWG) have been set up to help and curb this menace in the country. The Economic and Financial Crimes Commission has issued a warning that over 70 percent of Nigerian adolescents may soon become ex-convicts if the current elevated rate of their

engagement in cybercrime is not curtailed. Rahman, Sairi, Zizi, & Khalid (2020) state that undergraduates from tertiary institutions are capable of using computer and internet facilities for different kinds of cybercrime ranging from credit card fraud to pornography at the expense of their studies. This implies that any youth caught, tried and sentenced for cybercrime is inevitably classified as an ex-convict. Communication is essential in all human endeavors therefore; the media has the obligation to report on any illegal activity in the country, particularly among the youths, in an objective way. Day by day, we are increasingly inundated with news and exposed to disconcerting instances of cybercrimes perpetrated by Nigerian youths especially undergraduates using recent AI innovations in computers. Despite the objective of the Nigerian Cybercrimes Act 2015 to curtail cybercrimes, there seems to be no end in sight because the Nigerian youths are increasingly being involved in domestic and international cybercrime fraudulent activities. Insights into their awareness levels and use of artificial intelligence can inform the development of targeted interventions and educational programs to address the problem effectively.

The media has been the major promoters of campaigns with slogans such as secure your cyberspace, secure your digital life, lock it down, protect it up and block the hackers and so many others. In spite of these campaigns, it seems cybercrime among undergraduates are persisting and the use of innovative software's such as AI is now becoming the norm. This may be because the already disseminated information may be yielding minimal impact or that the message may have no impact at all on audience attitude. The scope of Nigerian youths' involvement has signalled consistent and deliberate attacks on both local and foreign victim's finances which impact negatively on the nation's image and on the global economy. In view of the above, this study seeks to examine the level of artificial intelligence awareness and use in cybercrime activities among undergraduates in Enugu state, Nigeria.

Research Objectives

This study specific objectives are:

1. Assess the awareness level on artificial intelligence use in cybercrime activities among undergraduates in Enugu State, Nigeria.
2. Find out the knowledge level on artificial intelligence use in cybercrime activities among undergraduates in Enugu State, Nigeria.
3. Identify the factors influencing cybercrime engagement and practice among undergraduates in Enugu State, Nigeria.

LITERATURE REVIEW

Cybercrime in Nigerian Society

Muraina and Muraina (2015) explained that cybercrime is a type of crime committed by individuals who utilize computers as tools and the internet as a medium to achieve a wide range of illicit objectives such as illegal downloading of music and films, piracy, spam mailing, and related offences. Similarly, Okeshola and Adeta (2013) opine that cybercrime encompasses any criminal activity involving the use of computers or internet networks, including fraud, phishing, identity theft, blackmail, forgery, and embezzlement. These definitions highlight the broad and evolving nature of cybercrime, particularly as technological advancements continue to expand opportunities for both legitimate and criminal activities in the digital space.

In contemporary society, cybercrime has emerged as a significant global menace in the digital era, affecting individuals, organizations, and governments alike. With the rapid expansion of internet access and digital technologies, youths have become one of the most active participants in cyberspace. However, this high level of engagement also makes them vulnerable to cybercriminal activities, either as victims or perpetrators. Studies reveal that many young individuals lack adequate awareness and understanding of cybercrime and its

consequences. Johnson and Taylor (2018) observed that a considerable proportion of youths demonstrated limited knowledge of cybercrime types such as identity theft, online fraud, and cyberbullying. Likewise, Smith and Anderson (2019) found that only 40% of young people were aware of the legal implications associated with engaging in cybercrime. These findings emphasize the urgent need for increased education and awareness initiatives targeting young internet users.

Cybercrime also has serious implications for the academic performance and overall development of youths. Excessive involvement in online activities such as gaming, social media usage, and exposure to inappropriate content can lead to reduced concentration, decreased productivity, and poor academic outcomes (Machackova, Dedkova, Sevcikova & Cerna, 2018). In addition, experiences of cyberbullying and online harassment can create hostile learning environments, resulting in increased absenteeism, reduced motivation and emotional distress among students (Kowalski, 2018). Consequently, the negative academic impacts of cybercrime may limit the future opportunities and career prospects of affected individuals, thereby hindering national development.

Smith (2019) argued that addressing the effects of cybercrime on youths requires a comprehensive and multi-dimensional approach that integrates prevention, intervention, and support mechanisms. Educational programs focusing on digital literacy, cybersecurity awareness, and responsible internet usage are essential in equipping young individuals with the skills needed to navigate the online environment safely. Furthermore, schools, parents, and communities must foster open communication and create supportive environments where victims of cybercrime can report incidents and receive appropriate assistance. Such collaborative efforts are crucial in mitigating the risks associated with cybercrime among youths.

The term "419," widely associated with fraud in Nigeria, refers to a section of the Nigerian Criminal Code that deals with offences related to advance fee fraud and prescribes penalties for offenders (Balancing Act, 2014). Nigeria has often been portrayed internationally as a hub for internet scams, earning labels such as a center of fraud and, in some instances, derogatory descriptions like the "Absurdity Empire" due to the prevalence of advance fee fraud schemes (Ajayi, 2015).

Although cybercrime is a global phenomenon, its prevalence varies across regions. Aransiola and Asindemade (2011) reported that in 2006, 61% of cybercriminals were located in the United States, 16% in the United Kingdom, and 6% in Nigeria. However, countries such as Ivory Coast, Togo, South Africa, the Netherlands, Spain, and Jamaica have also been identified as major centers of advance fee fraud. Recent reports suggest that Nigeria currently ranks among the top countries affected by cybercrime globally (Sese, 2025; Internet World Stats, 2014).

Adediran (2017) attributed the rise of cybercrime in Nigeria partly to advancements in global telecommunications infrastructure, including widespread access to computers, mobile phones, and the internet. These technologies have made it possible for individuals to connect to the global community from homes, workplaces, and cybercafés. The proliferation of smartphones and internet-enabled devices has further accelerated access to online platforms. However, this increased accessibility has also contributed to the emergence of sophisticated forms of cybercrime, including those involving artificial intelligence (AI). In Nigeria, cyber fraud is commonly referred to as "Yahoo Yahoo," while a more extreme variant known as "Yahoo Plus" involves the use of ritualistic practices believed to enhance the success of fraudulent activities (Idika, 2025). These practices are often linked to organized criminal networks and pose serious threats to societal stability.

The persistence of cybercrime in Nigeria can also be linked to socio-economic challenges such as poverty and unemployment. Despite the country's abundant natural and human resources, many young people face limited economic opportunities, making them more susceptible to engaging in cybercrime as a means of survival or quick wealth acquisition. This underscores the need for policies aimed at youth empowerment, job creation, and economic development as part of broader efforts to combat cybercrime.

Okeshola and Adeta (2013) conducted a study on the nature, causes, and consequences of cybercrime in tertiary institutions in Zaria, Kaduna State, Nigeria. Their findings revealed that various forms of internet-assisted crimes are prevalent, including identity theft, cyber harassment, phishing, hacking, ATM fraud, pornography, piracy, and spamming. These crimes often involve sending fraudulent financial proposals to unsuspecting victims, thereby undermining trust in Nigeria's digital economy and damaging the country's international reputation. As a result, many innocent Nigerians face discrimination and reduced opportunities abroad due to the negative image associated with cybercrime.

Psychological factors also play a crucial role in influencing individuals' involvement in cybercrime. Jaishankar (2017) noted that traits such as impulsivity, thrill-seeking behavior, and lack of empathy may predispose individuals to engage in cybercriminal activities. Additionally, motivations such as the desire for power, financial gain, recognition, or revenge can drive individuals toward cybercrime. Bossler and Holt (2020) further explained that the perceived anonymity of the internet and the reduced likelihood of being caught can encourage individuals to commit cyber offences. Peer influence and social networks also contribute significantly, as individuals may learn and adopt criminal behaviors from others within their social circles (Holt, 2017).

Print ISSN: 2006-0785
E-ISSN: 3115-4328 https://nsukkajcs.com/index.php/NJCS/index

Role of Mass Media in Raising Awareness

Mass media plays a vital role in raising awareness and enhancing public understanding of cybercrime. Through news reports, documentaries, and investigative journalism, media organizations highlight major cyber incidents such as data breaches, online fraud, and hacking attacks, thereby informing the public about potential risks (Bert-Jaap, 2020). This coverage helps individuals understand the methods used by cybercriminals and the consequences of cybercrime on victims and society at large.

In addition, media coverage reinforces the importance of cybersecurity and encourages individuals to adopt preventive measures such as using strong passwords, avoiding suspicious links, and protecting personal information online. Public service announcements (PSAs) are particularly effective tools used by the media to educate the public about cyber threats. Ristock and Siller (2018) noted that PSAs provide concise and targeted messages on issues such as phishing, identity theft, and cyberbullying, promoting safe online practices. The mass media facilitates large-scale educational campaigns through collaborations with government agencies and non-governmental organizations. These campaigns utilize multiple platforms, including television, radio, social media, and online content, to reach diverse audiences. However, the media must balance accurate reporting with the risk of sensationalism, which can sometimes distort public perception of cybercrime.

Cybercrime and the Law

The internet has become an integral part of modern life, offering numerous benefits while also creating opportunities for criminal activities. Cybercrime has thus become a major legal concern globally. Investigating cybercrime presents significant challenges due to the borderless nature of cyberspace and the difficulty in tracing perpetrators. Aghatise (2006) noted that tracking cybercriminals is often complex and time-consuming. Additionally, the lack of comprehensive and reliable data on cybercrime incidents in a country such as Nigeria may limit

the ability of researchers and law enforcement agencies to analyze trends effectively. These challenges highlight the need for stronger legal frameworks, improved data collection systems, and enhanced international cooperation in combating cybercrime.

Recent empirical studies have further explored cybercrime awareness, prevention, and the role of emerging technologies. Gupta and Neha Dubey (2025) examined cybercrime awareness among youths, focusing on their vulnerability to threats such as cyberbullying, phishing, and online fraud. Their findings emphasized the importance of educating young people on safe digital practices.

Hassan, Lass and Makinde (2012) conducted a systematic review on cybercrime prevention and concluded that education, technology, and legal measures must be integrated to effectively combat cybercrime. Similarly, Kanu, Adidi, and Kanu (2024) emphasized the need for an ethical framework to address the intersection of artificial intelligence and cybercrime in Nigeria. Punith and Shalini (2023) noted that while AI can strengthen cybersecurity systems, it can also be misused for malicious purposes.

Mark (2024) highlighted the dual role of AI in Nigeria's cybersecurity landscape, noting its effectiveness in detecting cyber threats as well as its potential misuse by cybercriminals. Onah and Ogwuche (2024) explored the relationship between AI usage and cybercrime behavior, finding that increased interaction with AI tools may influence online behavior patterns.

Finally, Ann, Okike, and Imam (2025) utilized machine learning models to analyze cybercrime victimization in Nigeria. Their findings revealed that certain psychological traits and online behaviors increase individuals' vulnerability to cybercrime, demonstrating the growing importance of AI in cybercrime research and prevention.

Print ISSN: 2006-0785
E-ISSN: 3115-4328 https://nsukkajcs.com/index.php/NJCS/index

Theoretical Framework

This study is pegged on Cybercrime and Criminological theory. This theory highlights the crucial role of computers and the internet in daily life making it imperative to comprehend the dynamics of cybercrime on victims.

Cybercrime and Criminological Theory

In 2013, J. Thomas Holt proposed a criminological theory emphasizing the essential role of computers and the internet in everyday life, necessitating an understanding of the dynamics of cybercrime and its effects on victims. The theory emphasizes the crucial role of technology, making it imperative to investigate the junction of cybercrime and criminological concepts.

This theory explores the motivations of individuals involved in various forms of cybercrime and deviant behavior, encompassing prevalent issues such as media piracy and more specialized offenses like computer hacking. Consequently, the idea is pertinent to this study as it elucidates the utilization of computers, artificial intelligence and the internet in fraudulent actions, including hacking for piracy, theft, and the harassment of individuals and financial institutions. Furthermore, it is important to acknowledge that anti social undergraduates utilize mobile devices to perpetuate examination malpractice and misconduct. Utilizing this theory, the research can proficiently tackle crime-related concerns across several levels, incorporating concepts pertaining to community and social effects.

MATERIALS AND METHODS

Research Design

The survey method of research was adopted to generate data for the study. Nwodu (2006) buttressing the relevance and importance of the survey research design is of the view that survey method focuses on a representative sample derived from the entire population of study.

Population/Sample Size of the Study

The population of consists of undergraduate students of the University of Nigeria, Nsukka (UNN) and Enugu State University of Science and Technology (ESUT). The population of UNN students stands at 29,949 while that of ESUT stands at 17,670 which sums up to 47,619 (Source; Academic Planning Unit UNN & ESUT, 2023). The sample size of the study is 382.

Sampling Technique

The multi-stage sampling was employed that is convenient sampling technique, stratified sampling technique, systematic sampling technique, random sampling technique and accidental sampling technique. The instrument of data collection was the questionnaire. The analysis and interpretation are based on the questionnaire administered for this study. Data generated for this research were presented in frequency distribution tables with mean and standard deviation. However, the study used descriptive techniques which are based on qualitative analysis as it directly addressed the research questions.

ANALYSIS

Table 1: Questionnaire Distribution and Collection

Number Distributed	382	100%
Number Received	360	94%
Number Lost	22	6%
School UNN	226	63%
School ESUT	134	37%
Total	**360**	**100%**

The data presented in Table 1 indicates that a total of 382 questionnaires were distributed to the sampled population under study, out of which 360 (94%) were successfully collected and returned. This notable return rate can be attributed to the researcher's proactive approach in personally distributing the questionnaires and collecting them by hand.

Research Question One: What is the level of artificial intelligence awareness and use in cybercrime activities among undergraduates in Enugu State?

Table 2: Level of Awareness

S/N	Awareness	Mean $\bar{x}$	Standard deviation	Decision
1.	I am aware of artificial intelligence use in cybercrime targeted towards people.	3.78	0.91	Agree
2.	I have come across information about the use of artificial intelligence in cybercrime from peers and on social media platforms (e.g., Facebook, Twitter, Instagram).	3.38	1.01	Neutral
3.	I am familiar with the objectives of the media messages against artificial intelligence use in cyber crime activities.	3.61	0.87	Agree
4.	The media messages against artificial intelligence use in cybercrime activities have been effective in raising awareness among university students.	3.81	0.89	Agree

Source: Field survey, 2023.

The data in Table 2, question 1, 2, 3 & 4 shows the awareness levels among UNN and ESUT undergraduates regarding artificial intelligence use in cybercrime activities. Majority respondents generally expressed awareness, with a mean score of 3.78, reflecting a positive awareness. However, encountering information on social media platforms resulted in a neutral stance (mean = 3.38), displaying variability in awareness. Despite this, respondents showed a reasonably favourable level of familiarity with media messages against artificial intelligence use in cybercrime activities (mean = 3.61), indicating consistent awareness. Also, they agreed on media effectiveness in raising awareness on artificial intelligence use among university students positive (mean = 3.81), showcasing its impact.

Research Question Two: Find out the level of knowledge artificial intelligence use in cybercrime activities among undergraduates in Enugu State?

Table 3: Knowledge on Artificial Intelligence use in Cybercrime.

S/N	Knowledge	Mean $\bar{x}$	Standard deviation	Decision
5.	I am knowledgeable about media messages against the artificial intelligence use in cybercrime.	3.52	0.91	Neutral
6.	I have participated in activities/events related to cyberbullying, identity theft, phising or hacking using AI.	3.34	0.94	Neutral
7.	I think media messages have been effective in raising awareness about artificial intelligence use in cybercrime among university students.	3.66	0.89	Agree

8.	I believe that media messages play a significant role in educating and protecting students from involvement in artificial intelligence use in cybercrime.	3.68	0.85	Agree
9.	I am more interested in participating in workshops or events aimed at promoting cyber-safety and awareness.	3.53	0.88	Neutral

Source: Field survey, 2023.

Table 3, questions 5, 6, 7, 8 & 9 shows the knowledge level on artificial intelligence use in cybercrime activities. Results from the above data shows that UNN and ESUT students perceive their knowledge of artificial intelligence use in cybercrime as neutral (mean = 3.52), reflecting some variability in self-assessment. Similarly, their active participation in the use of artificial intelligence in cyber crime related activities is perceived neutrally (mean = 3.34), with varied engagement levels. However, students generally agree that media messages have effectively raised knowledge about artificial intelligence use in cybercrime (mean = 3.66) and acknowledge the significant role of such messages in education and protection (mean = 3.68). Despite this, their interest in participating in workshops or events aimed at promoting cyber-safety and awareness is neutral (mean = 3.53), indicating varying levels of enthusiasm.

Research Question Three: What are the factors influencing cybercrime engagement and practice among youths in Enugu State, Nigeria?

Table 4: Factors Influencing Cybercrime Engagement and Practice.

S/N	Factors	Mean $\bar{x}$	Standard deviation	Decision
10.	Lack of job opportunities	3.72	0.89	Agree
11.	Desire for quick and easy money	4.15	0.82	Agree
12.	Inadequate cyber-security awareness	3.61	0.87	Agree
13.	Lack of parental guidance and monitoring	3.45	0.96	Neutral
14.	Addiction to the internet and online activities	3.98	0.84	Agree
15.	The easy availability of AI, hacking tools and techniques	4.07	0.79	Agree

Source: Field survey, 2023.

Table 4, questions 10, 11, 12, 13, 14 & 15 shows factors influencing cybercrime engagement and practice. Data reveal that the desire for quick and easy money (mean=4.15),

the easy availability of artificial intelligence software, hacking tools and techniques (mean=4.07), and addiction to the internet and online activities (mean=3.98) were perceived as key drivers of cybercrime engagement. In addition, inadequate cyber security awareness (mean=3.61) and the lack of job opportunities (mean=3.72) were also identified as significant factors. Lack of parental guidance and monitoring (mean=3.45) received a more neutral response. Findings here, clearly shows that factors such as the desire for quick money, easy access to hacking tools, addiction to the internet, and inadequate cyber security awareness contribute to cybercrime engagement among youths. Lack of job opportunities also plays a role.

DISCUSSION OF FINDINGS

Research question one aimed to assess the awareness level on artificial intelligence use in cybercrime activities among youths in Enugu State. Findings revealed a commendably high level of awareness and understanding of artificial intelligence use in cybercrime among the participants. Respondents demonstrated comprehensive knowledge about various forms of cybercrime, potential risks associated with them, and the tactics employed by cybercriminals. This high level of awareness provides a promising foundation for implementing effective cyber security awareness initiatives within the state. This finding is in line with the study of Kanu, Adidi and Kanu, (2024) on undergraduates in Enugu State because students who become aware of AI technologies may use them to facilitate cybercrime activities such as phishing, hacking, or online fraud. This also agrees with Punith and Shalini (2023); Gupta and Neha dubey (2025), whose study emphasizes the importance of ethical AI awareness to prevent misuse by technology users, including university students. The Crime and Criminological Theory is highly relevant in explaining Artificial Intelligence Awareness and Use in Cybercrime Activities among Undergraduates in Enugu State, Nigeria because both the theory and research focus on cybercrime participation, digital subcultures and the social and technological factors

that influence online offending. His framework helps explain how technological skills, online networks, and opportunity structures can encourage cybercrime among young people such as university students.

Research question two sought to find out the knowledge level on artificial intelligence use in cybercrime among youths in Enugu State. Findings of the research clearly shows that UNN and ESUT students hold a neutral perception of their knowledge about artificial intelligence use in cybercrime and their active participation in anti cyber crime campaign-related activities. However, respondents generally agree that media messages have been effective in raising awareness and believe in the significant role of such messages in education and protection from artificial intelligence use in cybercrime. Despite this, students express a neutral interest in participating in workshops or event aimed at promoting cyber-safety and awareness. This insight is accepted by Mark (2024). This is relevant to the study of undergraduates because increasing awareness and knowledge of AI technologies may influence students' capacity to engage in cybercrime activities. This finding is in tandem with Onah and Ogwuche (2024) which suggests that awareness, knowledge and frequent use of AI technologies among students could potentially influence cybercrime participation if ethical controls are weak. Cybercrime and Criminological Theory, helps explains why students become aware of, adopt and possibly misuse AI technologies for cybercrime. Criminological theories help interpret the motivations, opportunities, and social influences behind such behaviour among undergraduates in Enugu State, Nigeria.

Research question three on factors influencing cybercrime engagement and practice among youths in Enugu State, Nigeria, the study identified several contributing factors, including the desire for quick monetary gains, easy access to hacking tools, addiction to the internet, inadequate cyber security awareness, and the lack of job opportunities. These findings highlighted socioeconomic factors and limited opportunities as catalysts for engaging in

cybercriminal activities (Igba, Igba, Nwambam, Nnamani, Egbe and Ogodo, 2018). These contextual factors must be taken into consideration when designing targeted interventions to mitigate cybercrime engagement within the youth population. Undoubtedly the rapid growth of Artificial Intelligence (AI) and digital technologies has transformed cyberspace, creating both opportunities and risks among undergraduates. While AI is widely used for legitimate purposes such as cybersecurity, data analysis and automation, it can also be misused for cybercriminal activities such as phishing, identity theft, automated scams, and hacking by these youths who are largely unemployed. In tandem with the theoretical framework of this study, the accessibility of digital technologies among university students increases the likelihood of both awareness and misuse of AI tools in cybercrime activities. For undergraduates in Enugu State, increased awareness of AI technologies may influence both cybercrime participation and victimization patterns in digital environments which is in line with the studies of Ann, Okike, and Imam (2025). Thus, leading to the urgent need for stakeholders to develop an ethical response to the challenges of cybercrime (Kanu, Adidi and Kanu, 2024).

The theoretical framework emphasizes the importance of understanding cybercrime from various angles especially in regards to the motivations and use by youths involved in various forms of cybercrime and deviant behaviours because it elucidates the utilization of computers, artificial intelligence and the internet in fraudulent actions. Awareness of cybercrime can inspire individuals to promote enhanced cybersecurity measures and regulations in their personal lives, educational institutions, understand crime prevention and intervention initiatives.

CONCLUSION

This study investigated artificial intelligence awareness and use in cybercriminal operations among undergraduates in Enugu State, Nigeria. This study employed a survey methodology for data collection. The problem statement guided the development of three

research enquiries. A questionnaire was employed to gather pertinent data from a sample of 380 respondents, resulting in 360 completed questionnaires from an estimated population of students at UNN and ESUT in Enugu State, Nigeria. A multi-stage sampling procedure was employed due to the substantial population size and the data analysis was presented using distribution tables, mean and standard deviation.

Exposure and awareness to cybercrime messages and campaigns in Enugu State has impacted positively but it has exerted only neutral influence on the attitude of youths; on trust in online platforms; the propensity to exchange personal information online and the promotion of cybercrime prevention among peers. Youth involvement in cybercrime activities in Enugu State, Nigeria, is driven by factors such as the pursuit of rapid financial gain, readily available hacking tools like artificial intelligence software, internet addiction and insufficient understanding of cybersecurity laws. The scarcity of employment opportunities also contributes significantly. Based on the study's findings, we propose the following recommendations:

1. Develop and implement cyber security awareness programs specifically targeting the youths.
2. Collaborate with local community leaders, schools and youth organizations to create awareness campaigns that are embedded in the community fabric.
3. Work towards creating alternative skill development and job opportunities for the youth.
4. Recognize that factors like internet addiction and the desire for quick money contribute to cybercrime engagement.
5. Establish counselling services and support systems that address these underlying issues, providing avenues for guidance and redirection.

REFERENCES

Adediran, A. A. (2017). *Common Trends and Divergences in the Evolution and Development of Social Studies in Nigeria and South Africa*. Accessed 20th January 2025.

Aghatise, E. J. (2006). Cybercrime definition computer. *Crime Research Centre*. Retrieved from http://www.research.org

Ajayi, E. F. G. (2015). The Challenges to Enforcement of Cybercrimes Laws and Policy. *International Journal of Information Security and Cybercrime*, 4(2). pp. 33-48. Retrieved from http://www.ijisc.com/year-2015-issue-2-article-4/

Ajibike, T. (2019). Youth and Cybercrime in Nigeria, *Punch Newspaper* March 15. Accesssed 20th January 2025.

Ann, A. O., Okike, B., & Imam, A. (2025). Cybercrime victim profiling in Nigeria using machine learning and psychological traits. *International Journal of Research and Scientific Innovation*.

Aransiola, J. O. & Asindemade, S.O (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behav. Soc*. Netw. 14 (12), 759e763.

Balancing Act, (2014). *Nigeria Ranked Third in the World for Cybercrime*. Retrieved from http://www.balancingactafrica.com/news/en/issue-no302/computing/nigeria-ranked-third/en (accessed 30.05.2025).

Bert-Jaap, K. (2020). News Coverage of Cybercrime. In K. Jaishankar (Ed.), *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (pp. 237-256). CRC Press.

Bossler, A. M., & Holt, T. J. (2020). Examining the Cybercrime Offending Process: Implications for Predictive Policing. *Policing: An International Journal*, 43(3), 487-502.

Brody, R. G., Kern, S., & Ogunade K. (2020). Am Insiders look at the Rise of Nigerian 419 Scams. *Journal of Financial Crime*, 29 (1), 202-214

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International Journal of Engineering Sciences & Emerging Technologies*, 6(2), 142-153.

Eboibi, F. E., & Ogorugba, O. M. (2023). Cybercrime regulation and Nigerian youths increasing involvement in internet fraud: Attacking the roots rather than the symptoms. *Journal of Legal, Ethical and Regulatory Issues*, 26 (S2), 1-17.

Gupta, R. & Nehe dubey (2025). A Study of Cybercrime Awareness among the Youth. *International Journal of Humanities and Social sciences Invention (IJHSSI)*. 2319-7722: 2319-7714. Volume 14 Issue 3, March 2025. Pp 97-100. DOI:10.35625/7722-140397100. www.ijhssi.org97.

XHaenlein, M., & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. *California management review*, *61*(4), 5-14.

Hassan, A. B., Lass, F. D., & Makinde, J. (2012). Cyber- crime in Nigeria: Causes, effects and way out. International Journal of Science and Technology. 2 (7), 626- 631 http://www.silicon.com, 2013).

Holt, T. J. (2017). Cybercrime: Conceptual Issues for Criminology and Criminal Justice. In A. M. Bossler & J. M. Crisp (Eds.), *Routledge Handbook of International Cybercrime* (pp. 15-34). Routledge.

Holt, T. J., & Bossler, A. M. (2019). Exploring the Social Dimensions of Cybercrime. In M. McGuire & T. J. Holt (Eds.), *The Routledge Handbook of Technology, Crime, and Justice* (pp. 101-116). Routledge.

Hussaini, I., Ibrahim, S., Wali, B., Libata, I. A., & Musa, U. A. (2020). Effectiveness of Google Classroom as a digital tool in teaching and learning: Students' perceptions. *International Journal of Research and Innovation in Social Science, 4(4), 51-54*. Retrieved from https://www.rsisinternational.org/journals/ijriss/Digital-Library/volume-4-issue-4/51-54. pdf

Idika Moses (2025). 'Japa,' 'Gele,' '419,' 'Yahoo Boy,' 'Yahoo plu,' 16 other Nigerian Slangs Among 500 New Words, Phrase in Oxford English. http//factsheet.ng> japa-gele-419-yahoo. Accessed 22nd December, 2025.

Igba, I. D., Igba, E. C., Nwambam, A. S., Nnamani, S. C., Egbe, E. U., & Ogodo, J. V. (2018). Cybercrime among university undergraduates: Implications on their academic achievement. *International Journal of Applied Engineering Research*, *13*(2), 1144-1154.

Internet Crime Complaint Centre (2010). *Internet Crime Report*. Retrieved on May 1, 2023 from http://www.ic3.gov/media/ annualreports.aspx.

Internet World Stats, (2014). *World Internet Usage and Population Statistics – June 30, 2014 Mid-year update*. Retrieved from http://www.internetworldstats. com/stats.htm.

Jaishankar, K. (2017). *Personality Profiling of Cybercriminals: An Analysis of Malware Authors*. In K. Jaishankar (Ed.), Cyber Criminology: Exploring Internet Crimes and Criminal Behavior (pp. 59-78). CRC Press.

Johnson, A., & Taylor, N. (2018). Investigating Secondary School Students' Awareness of Cybercrime. *Journal of Information Warfare*, 17(3), 1-10.

Kanu, I. A., Adidi, D. T. & Kanu, C. C. (2024). Artificial Intelligence and Cybercrime in Nigeria: Towards an Ethical Framework. *Dialogue and Universalism* 34 (1) 2024 207. https://doi.org/10.5840/du202434115.

Kowalski, R. (2018). *Cyberbullying*. In The Routledge international handbook of human aggression. (pp. 131-142). Routledge.

Kshetri, N. (2019). Cybercrime and cyber security in Africa. *Journal of Global Information Technology Management*, 22(2), 77-81.

Machackova, H., Dedkova, L., Sevcikova, A., & Cerna, A. (2018). Bystanders' supportive and passive responses to cyber aggression. *Journal of school violence*, *17*(1), 99-110.

Mark, D. (2024). Impact of artificial intelligence on cybersecurity in Nigeria. *American Journal of Computing and Engineering*.

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.

National Bureau of Statistics (2023). Accessed on September 2025.

Ndubueze, P. N. (Ed.). (2011). *Cyber criminology and technology-assisted crime control: A reader. Kaduna, Nigeria*: Ahmadu Bello University Press Limited.

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

Onah, C., & Ogwuche, C. H. (2024). Cybercrimes and social media addictions: The role of perceived use of conversational GPT-4 AI model among residents in Nigeria. *Academic Journal of Psychology and Counseling, 5*(2), 170–201.

Punith, B. S., & Shalini, M. G. (2023). Transformative role of generative AI in safeguarding cybersecurity and privacy. *Journal of Electronics and Telecommunication System Engineering*.

Raman, Sairi, I., Zizi, N. A. M., & Khalid, F. (2020). The importance of cyber security education in school. *International Journal of Information and Education Technology*, 10(5), 378-382.

Ristock, J., & Siller, A. (2018). The Role of Public Service Announcements in Raising Awareness about Cybercrime: A Canadian Perspective. *Journal of Technology in Human Services*, 36(3), 191-205.

Sese, G. (2025). Cybercrime a threat to National Security in Nigeria. DO-10.5281/zenodo 16729087.

Smith, A., & Anderson, M. (2019). *Teens, Social Media & Technology 2018*. Pew Research Center.

Statista Research Department (2022). Retrieved Dec 12 2025 from http://www.statista.com/statistics/1261253/people-arrested-for-economic-crimes-in-nigeria-by-gender-and-crime.

Taylor, V., & Fritsch, E. J. (2020). Engaging Media for Crime Prevention: Integrating Mass Media into Community Safety Campaigns. *Security Journal*, 33(3), 271-287.