

Cyber Security Experts Association of Nigeria (CSEAN)
Society for Multidisciplinary & Advanced Research Techniques (SMART)
West Midlands Open University
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
ICT University Foundations USA
Academic Innovations City University Foundations

Proceedings of the Cyber Secure Nigeria Conference – 2024

Artificial Intelligence in Cybercrime: A West African Perspective on the Evolution of “Yahoo Yahoo”

¹Ayodele Oluwatobi (CISSP) & ²Peter Joy Abosede

¹Cybersecurity Education Initiative (CYSED)

²Educational Technology Veritas University Abuja

E-mails: oluwatobi@cysed.org; peterj@veritas.edu.ng

Phone Nos: +234 803 569 2006; +234 807 830 6888

ABSTRACT

This paper examines the evolution of the cybercrime phenomenon known as "Yahoo Yahoo" in West Africa, focusing on how it has advanced with the proliferation of artificial intelligence to enhance its capabilities. The study reviews various literature on cybercrime and, using a mixed-method approach, combines quantitative analysis to gauge public awareness of AI-related cybercrime with qualitative insights from interviews with threat intelligence experts across West Africa. These interviews explore how AI is used to enhance cybercrime, the tools and techniques employed, the challenges faced in combating AI-driven cybercrime, and recommendations for prevention. The paper concludes with strategic recommendations for staying ahead of this emerging threat.

Keywords: Cybercrime, Yahoo Yahoo, Artificial intelligence, Scam, evolution

Proceedings Citation Format

Ayodele Oluwatobi & Peter Joy Abosede (2024): Artificial Intelligence in Cybercrime: A West African Perspective on the Evolution of Yahoo Yahoo. Proceedings of the Cyber Secure Nigeria Conference held at The Ballroom Center, Central Business District, Federal Capital Territory, Abuja, Nigeria - 25th - 26th September, 2024. Pp 23-34.

<https://cybersecurenigeria.org/conference-proceedings/volume-1-2024/> dx.doi.org/10.22624/AIMS/CSEAN-SMART2024P2x

1. INTRODUCTION

Artificial Intelligence (AI), once a realm of science fiction, is now a potent tool shaping industries worldwide and our daily lives; Shamiulla (2019) also outlined that every human activity has become a subset of AI. Unfortunately, its potential for good is mirrored by its capacity for harm. One stark example of this is its role in the evolution of cybercrime.

In the heart of West Africa, a peculiar and increasingly sophisticated digital underworld has emerged, “Yahoo Yahoo” and AI. This is not just a problem for the future but a pressing issue that demands our attention and action now. Historically, these scams relied on deception and social engineering. However, the integration of AI has catapulted these operations into a new era of complexity and efficiency. This paper delves into the intricate relationship between AI and cybercrime, examining how these technologies are being harnessed to perpetrate the Yahoo Yahoo. By understanding the evolution of these scams through time into the era of AI, we can illuminate the challenges faced by West Africa and explore potential countermeasures to combat this growing threat.

1.1. Problem Statement

The rapid advancement of Artificial Intelligence (AI) has significantly transformed the landscape of cybercrime, particularly in regions with emerging digital infrastructures like West Africa. The "Yahoo Yahoo", a prevalent form of cybercrime in the area, has substantially evolved due to the integration of AI technologies. In a similar study, Kanu et al. (2024) explore the relationship between AI, cybercrime and the underground business economy in Nigeria, focusing on the rise of cybercrime. This research takes a comprehensive approach, investigating how cybercriminals exploit AI to enhance the sophistication and effectiveness of these scams. By examining the transformation of cybercriminal activities, identifying the AI tools and techniques employed, and understanding the methods used to circumvent traditional security measures, this study thoroughly explains the growing challenges posed by AI-powered cybercrime in West Africa.

1.2. Objectives

Specifically, this research aims to Examine the transformation and progression of cybercriminal activities in West Africa, with a focus on "Yahoo Yahoo", and investigate the various AI tools and techniques employed by cybercriminals (Yahoo Boys) to facilitate fraud, phishing and other illicit activities, challenges affecting the detection and develop strategic recommendations for the detection and prevention of AI-enhanced cybercrimes.

2. BACKGROUND

West Africa is Africa’s most populated region, with a combined population of 302.9 million, about one-third of Africa’s population. More than 50% of this total is Nigerian, according to the UN Women Africa report. This increase in ICT penetration, especially along the West African coast, has spurred growth in ICT-based businesses and services, including electronic government, electronic commerce, teledemocracy, telemedicine, and electronic banking services. Unfortunately, this level of globalisation facilitated by ICTs has also simultaneously raised the spectre of new criminal activities arising to exploit them. (Boateng et al, 2011).

In the same vein, Savirimuthu (2008) confirmed that the augmentation of internet accessibility in Nigeria with the new information and communication technologies has brought radiance light for the criminals and fraudsters to carry out their assignments behind the screen. The fraud did not begin with the internet, but the use of the internet enables the criminal to reach a more significant number of clients promptly without a track to be traced.

The First World Cybercrime Index -WCI was published, which placed the African continent as the third continent with a high rate of cybercrime, with North America in second place and Asia in first place. In Africa 2 out of the three countries on the WCI were from West Africa, Nigeria in the 5th position and Ghana in 13th position, closely followed by South Africa in the 14th position the WCI (Bruce et al., 2024), hence why the outlook of this paper is focused on west Africa continent majority of the cybercrime originated from West Africa; as a result, Longe et al. (2007) highlighted that Nigeria has gained a reputation as the source of the majority of fraudulent spam emails found in cyberspace.

2.1 The Evolution

Origin

For us to understand where we are at and where we are going, we need to understand where we are coming from; the social labels “yahoo-yahoo” and “Yahoo Boys” emanated from the late 1990s and the early 2000s through the proliferation of the internet across Nigeria (Tagbo, 2023). Furthermore, Flores et al. (n.d., in a joint paper by INTERPOL and Trend Micro) discussed the prominence and emergence of the name Yahoo Boys in the early 2000s due to their heavy use of Yahoo!® apps for communication via email and instant messaging (IM). Yahoo Mail was predominantly the means of communication at that time, used to send malicious and deceptive emails to their target. Alubo (2011) explains.

From A Scam to A Collection of Cybercrime

The predominant tactic during the early days was social engineering, which leveraged different pretexts, such as the Nigerian Prince scam (advance fee fraud), romance scam, and stranded traveller scam. However, with the advent of social media, financial technology, e-commerce and other advancements in technology that involve human interaction, Yahoo Boys has been able to ride on the trend. They are now using other forms of cybercrime like identity theft, chargeback fraud, drop shipping scams, fake ticket sales, sextortion, carding, and tax fraud, amongst many more. On a broader perspective, Yahoo Yahoo is no longer a scam but a social tag used to describe an all-encompassing collection of different forms of scam and cybercrime activities within the West African region.

Cross-Border Migration

With the borderless nature of the global internet, cybercrime can be perpetrated from anywhere in the world; against this backdrop, to avoid the long-stretched hands of justice and to invade law enforcement in Nigeria, yahoo-yahoo and Yahoo boys like diffusion over the years have moved to regions of lower concentration of cybercrime within the west Africa region most especially but not limited to Ghana, Benin republic and Cameroon. Uthman (2022) reports, “The Seme command of the Nigeria Immigration Service (NIS) says 16 Nigerians have been deported from Ghana for their alleged involvement in cybercrime.”

In West Africa, cybercrime has gradually eroded the region's reputation. For instance, in Nigeria, it is called “Yahoo Yahoo”, while the perpetrators are called “Yahoo boys” (Adeniran, 2008; Longe & Chimeke, 2008; Tade & Aliyu, 2011). In Ghana, it is called ‘Sakawa’ or ‘Yahoo Yahoo’ (Coonsom, 2009) and ‘Faymania’ in Cameroon (Oumarou, 2007), with almost exact TTPs.

Single Entity to Organised Crime Groups - OCGS

Flores et al., n.d., discussing Yahoo Boys from the early 2000s, highlighted the operational model as a single-man entity. Though they work as a group from physical locations called Cyber Cafes and are supervised by more experienced cybercriminals, every cybercriminal manages their entire operation from sourcing victims' email addresses to receiving the defrauded money, which does not require work segmentation and specialisation. In recent times, Cybercriminals have become more structured and organised; in a bid to maintain the sustainability of organised cybercrime, experienced cybercriminals set up an apprenticeship and recruitment system called HK. Tagbo (2023) described HK as initials for “hacker” as primarily a living apartments-based syndicates used to recruit potential yahoo boys in a type of apprenticeship setting providing only accommodation but no feeding or other necessities.

Contrary to Tagbo (2023), Evans-Ibe (2023) argues that Hk, also known as “Headquarters,” in this apprenticeship, provides all social amenities like feeding, data subscription, power, and others are provided in exchange for 60 -70% of all fraud proceeds. They also highlighted the duration as an average of 6 months to 1 year, during which they are expected to cash out (Cashout, a social term, refers to successfully getting financial gains from a victim). However, there is a similarity in their views as both agreed on the fact that in the HKs, there is a form of hardship, violent treatment and a slave-to-master relationship with their bosses. The criminogenic society has given rise to an extensive syndicate network of cybercriminals spread across different regions and countries, with different roles, segmentation, specialisation and experience levels. The role ranges. Below are some of the roles identified in this study that play critical roles in the cybercrime syndicate

Picker: In Yahoo Yahoo vocabulary, a picker is a person who stays in the same country as the scammer's target and collects or receives the money on behalf of the fraudster. (Wangare and Simwa, 2022)

Aza men: Evans-Ibe (2023) classified pickers and aza men as one, describing them as among the most experienced, most connected, and healthiest fraudsters. They specialise in providing account details of third-party collaborators to receive funds. The picker or Aza man usually takes 20% -40% of the money received, with the account details they provide and primarily resides outside Nigeria.

Loader: the fraudster who performs the fraudulent transfers into the victim's bank account from a compromised account (Evans-Ibe, 2023). The West African cybercrime ecosystem is a supportive, open space where newbies can easily share information. Flores et al. (n.d.) described it as a self-learning portal and a self-sustaining system that improves through trial and error and the sharing of best practices.

Cyber Spiritualism - Yahoo Plus

Cybercrime has always been about social engineering, using wit and deceptive techniques to trick victims or maga into falling for a scam or fraud. However, due to the excessive adoption of cybercrime and the oversaturation of cybercriminals in the region, the competition in securing clients (victims) has become stiffer, and the need to make quicker money has grown. Tade (2013), in a study, explores how Yahoo Yahoo in western Nigeria employs spiritual means to enhance cybercrime, which is popularly called Yahoo Plus; he went further to define

it as a cybercrime strategy which blends spiritual elements with internet surfing to enhance victimisation rates on the web. This enhanced cybercrime uses ase or mayehun (incontrovertible order), charmed or magical rings (oruka-ere) and incisions made around the wrist, which are used to surf the net, while ijapa (tortoise) is used to navigate profitable sites. In a somewhat similar study conducted in Ghana, Warner (2011) reports the use of a klepto-theological paradigm created to abet the perpetration of Internet crime. He calls this Sakawa. According to him, Sakawa serves two main functions: it protects the cybercriminal and ensures their financial success. Sakawa ritualised practice of online fraud is practised. In Sakawa, a supreme being is believed to bless criminals with protection and good fortune.

Artificial Intelligence

In a bid to understand how AI is being leveraged by cybercriminals, Hoanca, B., & Mock, K. J. (2020) outline three types of activities; first, it outlines how AI gives cybercriminals the ability to automate and enhance cybercrime; secondly, How AI opens up new threat landscape and channels that can extend to physical space and thirdly how AI is used to attack other AI systems and infrastructure to steal confidential data or in corrupting the operation of the AI algorithms. The above activities have been prevalent in cyberspace since the development of commercialised Generative AI (GenAI) models, such as ChatGPT and Google Bard, and have also been highlighted as a potential cybersecurity concern (Mohammad et al., 2014). These AI models pose vulnerabilities and potential risks, indicating the need for proactive measures to counter potential cyber threats arising from such advancements.

Artificial intelligence (AI) use in cybercrime has become a growing concern, particularly in West Africa, where scams such as "Yahoo Yahoo" have evolved. Olofinbiyi (2022) suggests that socio-cultural pressure on youths to achieve pecuniary success and frustration arising from a sense of discrepancy between individual aspirations and legitimate means to realise these ambitions led to the emergence of the "Yahoo Boys" subculture in Nigeria. This highlights the complex interplay of social and economic factors that contribute to the evolution of cybercrime in the region.

3. METHODOLOGY

This research will employ a mixed-methods approach to comprehensively examine the intersection of AI and cybercrime in West Africa, with a specific focus on Yahoo Yahoo scams. It will use open-ended and closed-ended questionnaires for the general public and interview eight threat intelligence experts in Ghana and Nigeria.

3.1. Research Questions

1. How have cybercriminal activities evolved in West Africa using AI, specifically about the "Yahoo Yahoo"?
2. What are the specific AI tools and techniques utilised by cybercriminals to perpetrate fraud, phishing, and other illicit activities?
3. What are the challenges in combating AI-enhanced crime?
4. What are the strategic recommendations for detecting and preventing AI-enhanced cybercrimes?

4. RESULT AND ANALYSIS

The analysis is based on a survey conducted among professionals and individuals who have either experienced or are knowledgeable about AI-enhanced cybercrime and interviews carried out by eight (8) participating experts.

Cybercriminal Activities Evolved using AI.

Nearly half of the respondents (49%) reported having encountered AI being used in cybercrime, which indicates a significant exposure to AI-driven cybercrime among the surveyed group. The fact that 41% have not encountered such incidents suggests a divide in experience or awareness within the community. The 10% who were unsure might indicate a lack of understanding or recognition of AI's role in cybercrime.

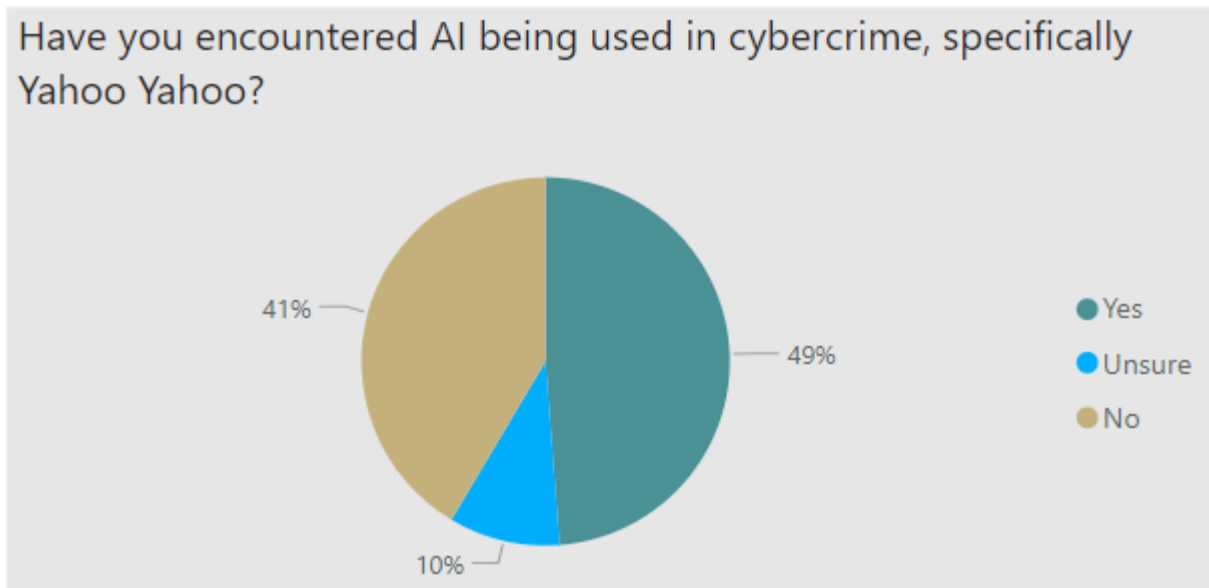


Fig. 4.1: Graph of AI Being Used in Cyber Crime, Specifically Yahoo Yahoo

Concurring, the issue of AI increased cybercriminal activities, which emerged as one of the most prominent subthemes identified by the participants. When the participants were asked to explain and describe their perception of how cybercriminal activities evolved in West Africa, specifically to "Yahoo Yahoo," the interview with participants in the following passages reveals that the participants confirmed that there had been some integration of AI in cybercrime activities.

An expert highlighted that cybercriminal activities in West Africa, especially those related to "Yahoo Yahoo", have expanded beyond simple fraud. He mentioned that advanced techniques such as social engineering, money laundering, and romance scams have been more commonly seen. Additionally, suspects with IT expertise use AI to improve their fraud schemes, making them more complex and challenging to detect.

An expert emphasised the shift from traditional scam methods, like sending mass phishing emails, to more sophisticated and personalised scams enabled by AI. He mentioned that scammers now use AI tools to simulate voice notes and video calls, making scams more convincing. AI allows them to create more realistic interactions, such as mimicking the voice of someone the victim knows, thereby enhancing the believability of the scam. Based on the above responses, it can be observed that cybercrime has evolved, and AI-enhanced fraud has expanded beyond simple fraud among Yahoo. Yahoo is a common theme that emerged from the opinions of the eight respondents.

AI Tools and Techniques Utilised by Cybercriminals

AI applications you have encountered used in Yahoo Yahoo (cybercrime)

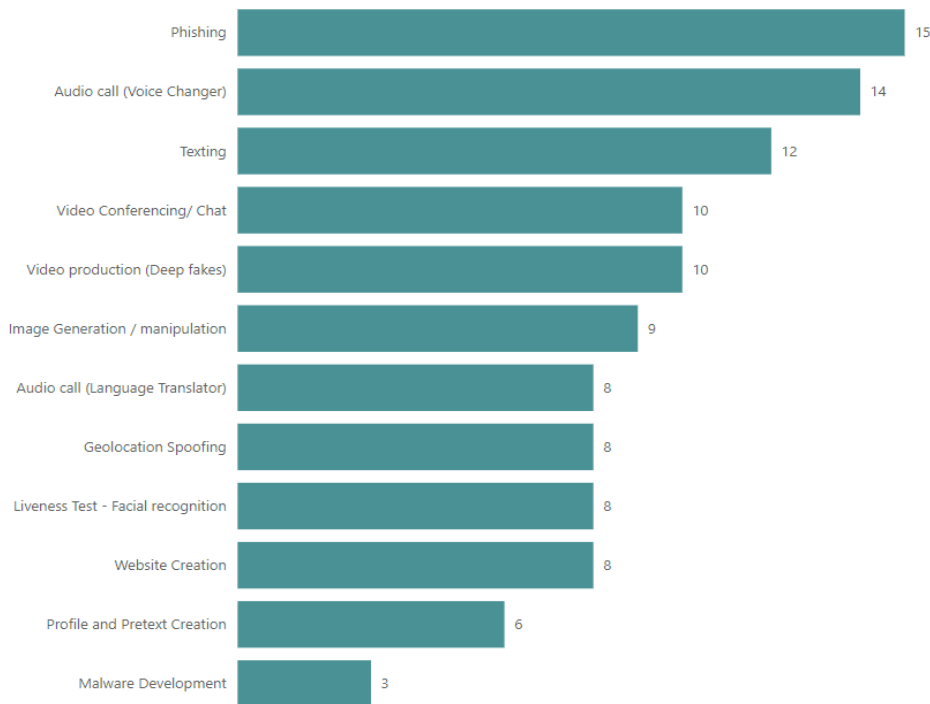


Fig. 4.2: AI Tools and Techniques used by Cyber Criminals

The above data suggests that AI is being leveraged in various ways to enhance the sophistication and effectiveness of cybercrimes, particularly in phishing, voice and video manipulation and texting. Highlighting some techniques, an expert identified tools like FraudGPT and WormGPT, which mimic the popular ChatGPT but specifically promote malicious activities that can be found on Telegram and the dark web marketplace based on subscription. Unable to disclose the name of a tool because the tool did not have a name, the expert explained, are used in celebrity scams; “Criminals have also employed this tool to create fake videos of celebrities or prominent figures, endorsing fraudulent products or giveaways.

The expert gave examples of Nigerian journalist David Hundeyin and one of the P-Square brothers being used in these fake videos to deceive people into participating in scams. Based on another methodology, another expert described the use of AI to generate deepfake videos and voice notes. These tools can be obtained from the dark web, telegram channels, Facebook and WhatsApp groups, the expert explained. Cybercriminals can now extract voices from social media platforms and use AI to replicate those voices in scams. This allows them to impersonate real people and convince victims to fall for fraudulent schemes. The expert described how AI-powered voice-cloning tools are used to send WhatsApp voice notes that sound like a trusted person, thereby convincing recipients to send money or reveal sensitive information.

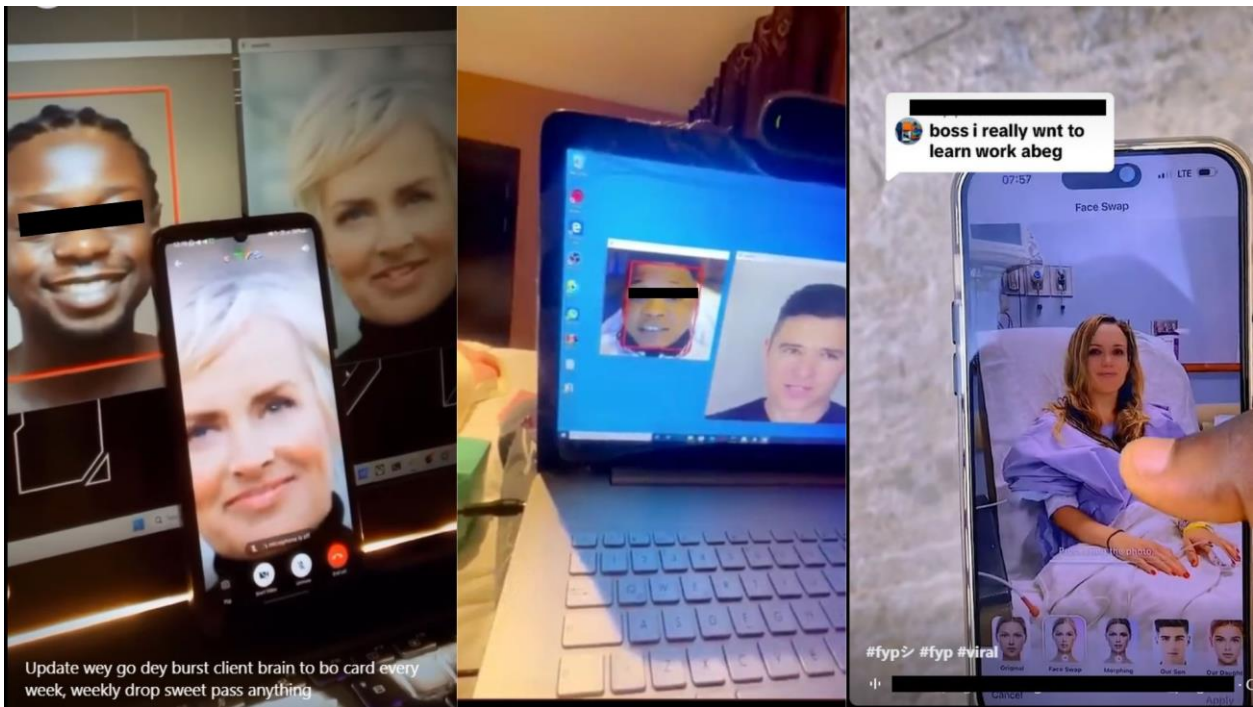


Fig.4.3 Images of the AI tool being used for deep fake video conferencing and face swaps on images

Recommendations for the Detection and Prevention Of AI-Enhanced Cybercrimes

The experts were asked to make recommendations on detecting and preventing AI-enhanced cybercrimes. An expert emphasised the importance of collaboration among West African countries in investigating and preventing cybercrimes, as many scammers operate across borders. Sharing intelligence and resources will help effectively tackle the AI-driven schemes that are becoming more prevalent. The participant recommended using advanced AI-based cybersecurity tools to detect fraudulent activities. These tools can help identify patterns in the criminals' use of AI, such as malware behaviour and data extraction methods. Similarly, another expert recommended that companies and governments invest in AI-based cybersecurity systems that can detect AI-enhanced attacks.

These systems can analyse patterns, detect anomalies, and respond to threats in real time, which is essential in combating AI-driven cybercrime. He also suggested increasing public awareness about AI-driven scams. Many people are still unaware of how convincing AI-generated scams can be, so educational campaigns are crucial to helping the public recognise and avoid these schemes. Based on the above responses and those of other experts, it was observed that AI-driven cybersecurity tools to detect AI-related cybercrime with functionalities to analyze subtle inconsistencies in videos and audio files, helping to identify fraudulent content before it reaches the victim and collaboration of multiple stakeholders in information sharing about AI-related tools and tactics was a common theme that emerged, Security awareness on AI-related technologies and crimes as a preventive method which solves the problem of little to no awareness of AI-enhanced cybercrime that was identified in the survey. (see Fig. 3)

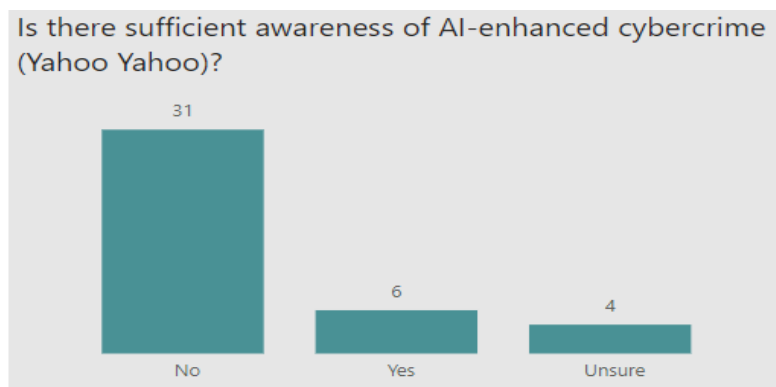


Fig. 4.4: Graph of AI-Enhanced Cybercrime

Triangulation 1: The qualitative data aligns with the quantitative findings by demonstrating that cybercriminal activities, especially "Yahoo Yahoo," have evolved significantly in sophistication. As shown by 60% of respondents, the awareness of these activities mirrors the interviewees' detailed accounts of advanced schemes, such as AI-generated recruitment fraud, voice cloning, and email interception. Both sources underscore the growth and complexity of cybercrime in West Africa.

Triangulation 2:

The qualitative data highlights real-world examples of AI being used for fraud (deepfakes, voice cloning, bots), aligning with the quantitative findings that 82.5% of respondents are aware of AI's involvement in cybercrime. This suggests that both cyber experts and the general population are increasingly aware of the integration of AI into fraudulent activities, affirming the significance of AI in enhancing "Yahoo Yahoo" operations.

Triangulation 3:

The unanimous call for multi-faceted solutions in qualitative and quantitative data reflects a strong consensus on the need for comprehensive strategies. Interviewees provided concrete suggestions such as better AI detection systems and public awareness, which align with the 100% of survey respondents advocating for diverse approaches.

This convergence highlights that experts and the general population agree on the urgency of addressing AI-enhanced cybercrime with multi-layered defence mechanisms.

5. CHALLENGES IN COMBATING AI-ENHANCED CYBERCRIME

The responses from various professionals highlight several challenges in combating AI-related cyber threats. The challenges range from technological limitations to gaps in skills and awareness. **Lack of Awareness:** Many respondents pointed out that a general lack of adequate awareness among the public is a significant challenge. Users are often unaware of the threats posed by AI-enhanced cybercrime, which makes them vulnerable to sophisticated attacks. **Difficulty in Detection:** The rapid evolution of attacker techniques using AI makes detection increasingly difficult. Traditional cybersecurity measures struggle to keep pace with the sophisticated methods employed by cybercriminals, such as identity masking and creating untraceable digital footprints. This evolution complicates efforts to identify and prevent AI-generated content used in cybercrime.

Skill Gaps and Training Deficiencies: The responses reveal a significant gap in the skills required to combat AI-enhanced cybercrime. Many cybersecurity professionals lack the necessary training in AI, which hampers their ability to implement and maintain advanced AI-based solutions. This skill gap is exacerbated by the scarcity of experts who can effectively counter these sophisticated threats. **Technological Limitations:** Respondents highlighted the limitations of current cybersecurity tools in the real-time detection of AI-enhanced threats. The rapid evolution of AI in cybercrime requires equally advanced countermeasures, which are currently lacking. Additionally, the difficulty in tracing AI-generated content and the anonymity it affords to attackers present ongoing challenges.

Legal and Ethical Concerns: Legal and ethical concerns surrounding AI regulation further complicate efforts to combat AI-enhanced cybercrime. The dynamic nature of AI-driven attacks poses significant challenges for law enforcement agencies, which are not always equipped to deal with these rapidly changing threats.

6. RECOMMENDATIONS:

Enhanced Awareness Campaigns: A consistent theme across the responses is the critical need for increased awareness among the public, especially targeting non-tech-savvy individuals who are increasingly the primary victims of AI-enhanced cybercrime. Awareness campaigns should be comprehensive, educating the general public about the risks associated with AI in cybercrime, how to recognise AI-generated scams, and steps to protect themselves. **Specialised Education and Training:** Law enforcement agencies and cybersecurity professionals need specialised training in artificial intelligence to stay ahead of AI-powered cybercrime tactics. This includes understanding the technology behind AI, its applications in cybercrime, and the tools and techniques needed to combat such threats.

Implementation and Enforcement of Regulatory Frameworks: Governments should develop and enforce robust regulatory frameworks that specifically address the safe and responsible use of AI. This includes updating existing laws to reflect the new challenges posed by AI, ensuring that privacy and data protection laws are stringent, and strengthening international

cooperation to tackle cross-border cybercrime effectively. Advanced Threat Detection and Security Tools: AI-driven threat detection systems need to be developed and implemented. These tools should be capable of identifying and recognising AI-related patterns and countering them in real time, providing a proactive defence against evolving cybercriminal tactics.

Multistakeholder Collaboration: AI-enhanced cybercrime is a global issue that requires international and regional collaboration. Governments and private institutions should collaborate to share intelligence, harmonise legal frameworks, and develop countermeasures to combat AI-related cyber threats. Research and Development: Ongoing learning and research in artificial intelligence in cybersecurity will enhance understanding and lead to robust solutions for addressing emerging threats.

7. CONCLUSIONS

In conclusion, this paper identifies how cybercrime has evolved with the integration of AI. Through expert opinions gathered from extensive interviews, the study qualitatively analyses their insights on the evolution of cybercrime in the region, the tools and techniques used, the challenges faced, and offers recommendations. These insights are further supported by a qualitative analysis of both closed and open-ended survey responses. Adopting these recommendations would help ensure that AI-enhanced cybercrime becomes a more manageable threat.

REFERENCES

1. Savirimuthu, Joseph (2008). Identity Theft and the Gullible Computer User: What Sun Tzu in The Art of War Might Teach, *Journal of International Commercial Law and Technology* Vol. 3, Issue 2. P.120. Retrieved from <http://www.jiclt.com/index.php/jiclt/article/viewArticle/49>
2. Bruce M, Lusthaus J, Kashyap R, Phair N, Varese F (2024) Mapping the global geography of cybercrime with the World Cybercrime Index. *PLoS ONE* 19(4): e0297312. <https://doi.org/10.1371/journal.pone.0297312>
3. Danquah, P., Longe, O. B. (2011). Cyber Deception and Theft: An Ethnographic Study on Cyber Criminality from a Ghanaian Perspective. *Journal of Information Technology Impact* 11, No. 3, 169-182
4. Adeniran, A. (2008). The Internet and Emergence of Yahoo Boys Sub-Culture in Nigeria. *International Journal of Cyber Criminology (IJCC)* 2 (2), 368–381.
5. Coomson, J. (2009). Cyber Crimes in Ghana. *Ghanaian Chronicle*, 4 October 2006, from <http://allafrica.com/stories/200610040856.html>
6. Oumarou, M. (2007). Brainstorming Advanced Fee Fraud: ‘Faymania’—the Cameroonian Experience. In N. Ribadu, I. Lamorde and D. W. Tukura (Eds.). *Current Trends in Advance Fee Fraud in West Africa*, pp. 33-34. Nigeria: EFCC
7. Tade, O. (2013). A spiritual dimension to cybercrime in Nigeria: The ‘yahoo plus’ phenomenon. *Human Affairs*, 23(4), 689-705. <https://doi.org/10.2478/s13374-013-0158-9>

8. Longe O. B., Onifade O. F., Chiemeké S. C., & Longe F. A. (2007). User acceptance of Web-marketing in Nigeria: Significance of factors. Proceedings of the International Conference on Applied Business & Economics. Piraeus, Greece.
9. Alubo, O. (2011). The Public Space in Nigeria: Politics of Power, Gender and Exclusion. *Africa Development* XXXVI, 1, 75-95. https://africa.unwomen.org/en/where-we-are/west-and-central-africa_africa
10. Mohammad, R. M., Thabtah, F., & McCluskey, L. (2014). Predicting phishing websites based on a self-structuring neural network. *Neural Computing and Applications*, 25, 443-458.
11. Olofinbiyi, S. A. (2022). A Reassessment Of Public Awareness and Legislative Framework on Cybersecurity In South Africa. *ScienceRise: Juridical Science*, 20(2).
12. Tagbo T. (2023, October 12). In the dark side of Yahoo boys underworld. The Guardian. Retrieved from <https://guardian.ng/opinion/columnists/in-the-dark-side-of-yahoo-boys-underworld/>
13. Wangare, J., & Simwa, A. (2022, September 20). Yahoo boy format in Nigeria: All the details about fraudsters. Retrieved from https://www.legit.ng/ask-legit/guides/1084198-yahoo-boy-format-nigeria-how-work/#google_vignette
14. Flores, R., Matsukawa, B., Remorin, L. A., Sancho, D., Yamazaki, T., & Wong, A. (n.d.-a). Cybercrime in West Africa: Poised for an Underground Market. Retrieved from <https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-africa.pdf>
15. Uthman, S. (2022, October 14). Ghana deports 16 Nigerians over “cybercrime” | TheCable. Retrieved from <https://www.thecable.ng/ghana-deports-16-nigerians-over-cybercrime/>
16. Tade, O. (2013). A spiritual dimension to cybercrime in Nigeria: The ‘yahoo plus’ phenomenon. *Human Affairs*, 23(4), 689–705. <https://doi.org/10.2478/s13374-013-0158-9>
17. Hoanca, B., & Mock, K. J. (2020). Artificial Intelligence-Based Cybercrime. In IGI Global eBooks (pp. 36–51). <https://doi.org/10.4018/978-1-5225-9715-5.ch003>
18. Kanu, I. A., Adidi, D. T., & Kanu, C. C. (2024). Artificial Intelligence and Cybercrime in Nigeria. *Dialogue and Universalism*, 34(1), 207–221. <https://doi.org/10.5840/du202434115>