INTERROGATING THE CHALLENGES AND PROSPECTS OF ARTIFICIAL INTELLIGENCE IN CYBER CRIME PREVENTION IN NIGERIA

By

Dr. Osuji, Emma*

Abstract

The global advancement of artificial intelligence has brought about significant changes across various sectors. It has also created new opportunities for cybercrime. Nigeria has witnessed a surge in cybercriminal activities which has affected both the economic and social activities and cast a shadow over her. This paper explored the challenges and prospects of using artificial intelligence in breaking the chains of cybercrime in Nigeria with a focus on cyber fraud which is synonymous to '419 scams' in the global imagination. The paper noted that the current approach largely hinging on law enforcement and regulation has generated little to no significant impact on breaking the chains of cybercrime in Nigeria. It concluded that the integration of artificial intelligence in the fight against cybercrime will significantly boost the capabilities of anti-corruption agencies like the Economic and Financial Crimes Commission. It then recommended that a legal framework should be put in place to ensure its legality and efficacy.

Keywords: *Crime, Cybercrime, Artificial-intelligence, and Legal Framework.*

1.0 Introduction

Crime prevention and detection are the critical components of security upon which public safety is premised in any nation.[1] Traditionally, crime detection and prevention including the detection and prevention of cybercrime in Nigeria relied on human intuition and limited data, resulting in reactive and resource intensive methods. Recent advancement in artificial intelligence offers a paradigm shift, enabling a proactive data driven approach.[2]

This rapid advancement of artificial intelligence also brought about significant positive changes for cyber sectors as well as new opportunities for cyber fraud in Nigeria.[3] Nigeria particularly has witnessed a surge in cybercrime activities and the underground business economy focusing on the rise of fraud, identity theft and hacking among others,[4] which the use of artificial intelligence with elements of cognitive and emotional intelligence can successfully be employed to combat this cybercrime menace. It must be noted that cybercrime has become a threat to various institutions and internet users either through computers or mobile technology.[5] In Nigeria today several internet assisted crimes known as

* (KSM) PhD Lecturer in Department of Public Law, Faculty of Law Imo State University Owerri, Email: osujiemma345@gmail.com, Tel: 08033386163.

[1] Oghenevow, Z.A., Nachamada, V. B. and Gilbert, I.O.A. Advancement in Crime Prevention and Detection: From Traditional Approaches to Artificial Intelligence Solutions, [2024] 2 (2), *European Journal of Applied Science, Engineering and Technology https://www.researchgate.com*. accessed 27/7/2024.

[2] *Ibid*.

[3] Shota, N., The Use of AI in "Detecting and Preventing Cybercrime" *www.inkedin.com*. accessed 27/7/2024.

[4] Shota (n 3).

[5] Dokpesi, T., Adidi, C.C. and Kanu. I. "Artificial Intelligence and Cybercrime in Nigeria. Towards an Ethical Framework. *www.researchgate.net*. accessed 27/7/2024.

cybercrime are committed daily in various forms, ranging from fraudulent electronic mails, child pornography, identity theft, hacking, cyber harassment, spamming, spoofing, piracy and phishing among others.[6] This new phenomenon has occupied the cynosure of global attention simply because all citizen of the world, irrespective of whether they are private or public are vulnerable to it.[7] The emergence of artificial intelligence has opened new avenues for developing and implementing artificial intelligence based cyber security technologies and systems to combat cybercrimes.[8] It not only combats crimes but it detects suspicious network activity and finds dark web forum posts indicating a data breach.[9] It does this by the use of machines in various domains of cyber security.

2.0 Conceptual Issues

a. Crime

When parliament enacts that a particular act shall become a crime or that an act which is now criminal shall cease to be so, the act does not change in nature in any respect other than that of legal classification.[10] The entire characteristics as observed remain the same before and after the statutes comes into force, hence any attempt at a definition will include the act a time when it was not a crime or exclude it when it is. It is this confusion that led to different approaches in the definition of crime.[11]

In the light of the above, the concept of crime according to Cross and Jones is defined as a legal wrong for which the offender is liable to be prosecuted and if convicted, punished by the state.[12] The author further explained the concept to be wrong which is a breach of a rule which may be moral or legal according to whether the rule in question is one of morality or law.

Despite the assertion that the definition of crime is unfashionable, Kenny went further to define a crime as an act capable of being followed by criminal proceedings having one of the types of outcomes (punishable) known to follow these proceedings.[13] Okonkwo aligned himself with the definition of crime posited by the criminal code as offences which constitutes acts or omissions which render the person doing the act or making the omission liable to punishment.[14]

Considering this position carefully, it will be observed that the definition of any particular offence consists of two sorts of elements, namely the physical and mental elements which are identified as the *actus reus* and *mens rea*. The *actus reus* consists of an act or rule rarely an omission which may include the conduct of an accused with its attendant consequences. The mental element which is *mens rea* is that aspect which is required to be proved in some situations. It must be noted that both the *actus reus*

[6] *Ibid*.
[7] Osuji, E., Cybercrime in Nigeria: Issues and Challenges, [2023] XI (1), *Nigeria Journal of Legal Studies*,43.
[8] *Ibid*.
[9] Okorie, C.K. and Mbachu S.C. Complexities, Issues and Challenges on Cybercrime in Nigeria (eds) Chukwumaeze U.U. and Okorie C.K. in *Excellence at the Bench, Essay and Selected Judgments* in Honour of Honourable Justice Ngozi Ukoha, (Owerri Zubic Infinite Concepts 2019), 166.
[10] Chukwumaeze, U.U., *"Electronically Generated Evidence and Prevention of Crimes".* Paper delivered at Nigerian Bar Association Aba Branch, 2008.
[11] Cross, R and Jones, P.A., *Introduction to Criminal Law*, (Seventh Edition, London, Butterworth Co. Publishers), 1972, 9.
[12] *Ibid*.
[13] Molan, M., Lanser, D., and Bloy. D., *Principles of Criminal Law* London, (Cavendish Publisher 2000), 14.
[14] Okonkwo, C., *Criminal Law in Nigeria*, (London Sweet and Maxwell, 1980), 19.

and *mens rea* of an offence must be simultaneous in point of time in grounding convictions for offences considered as being criminal in nature.[15]

Flowing from the above, the question now is what conducts should be considered as crimes? According to the general purposes of the provisions governing the definition of offences in the American Law Institutes Model Penal Code, conducts that unjustifiably and inexcusably inflicts or threatens substantial harm to individuals' public interest should be considered crimes, for instance, cybercrime.[16]

b. Cybercrime

Cybercrime encompasses a wide range of criminal activities that are carried out using digital devices and or networks. Cybercrimes are committed in the impalpable world of computer network.[17] Cybercrimes being technologically driven have continuously and ingeniously made it difficult for cyber investigators to find solutions to such crimes, because they pose a huge number of complications when it comes to investigations. Cybercrime can basically be categorized into four parts namely, cybercrimes which are committed against individuals, against property, against society and against organizations.[18] It is against individual when it is targeted at stealing personal information of people from/through the internet.

Another class of cybercrime revolves around property and involves credit card fraud, intellectual property theft, internet time theft which also deals with stealing, destroying or misusing the source code *et cetera*.[19] Cybercrime can also be committed against an organization. This specie of cybercrime deals with unauthorized access to a computer network without authorized access of the owners.[20]

Cybercrime has spread to such proportion that a formal categorization of the crime is no longer possible. Every single day gives birth to new kind of cybercrime, making every single effort to halt it almost a futile effort.[21] Cybercrime perpetrators have discovered that the internet can provide new opportunities and multiple benefits for illicit businesses. They have employed the internet as a tool for not only fraud and theft among others but also for drug trafficking and criminal organization rackets that are concerned with exploitation and disruption of the society.[22]

In Nigeria, cybercrime is a trend that is rapidly growing in scope and frequency.[23] The revolution in information and communication technology has greatly promoted the trend and scope of cybercrime in Nigeria. The rate at which the Nigerian cyberspace is subjected to daily attacks from unscrupulous minds and criminal elements has continued to remain alarming. Cybercrimes have taken a dangerous

[15] Clarkson, C.M.V., and Keating, H.M., *Criminal Law; Text and Materials*, (London, Sweet & Maxwell, 1998), 3.
[16] Chukwumaeze, U.U., 1998, 3.
[17] Welfinder, "Scope of Cyber Security" https://*www.welfinder24.com* . accessed 29/7/2024.
[18] Osuji, (n 7).
[19] Pander Security "Types of Cybercrime" *www.pandasecurity.com*. accessed 29/7/2024.
[20] *Ibid*.
[21] Admindeepak, "Nature and Scope of Cybercrime" *deepakmiglani.com*. accessed 29/7/2024.
[22] *Ibid*.
[23] Oni, M.J., "Cybercrime in Nigeria" The Implication in our Economy and Society Image" *www.acta-pac.org*. accessed 30/7/2024.

toll on individual businesses, institutions, government and the economy and has become one of the avenues of getting rich very quickly.

The rising cyber-attacks in Nigeria have caused more economic social and cultural harm than good. Fraudulent activities and practices connected to cybercrime have made a lot of young people rich and emergency millionaires. It has become very clear that the escalation of cybercrime cannot be adequately curtailed by local crime prevention agency who use the traditional method of crime prevention in fighting crime, hence the use of artificial intelligence will assist in the breaking of the chains of cybercrime in Nigeria.

c. Artificial Intelligence

Artificial intelligence is the aspect of computer science, which enables the computer to mimic the human behaviour in order to assist humans for better performance in the field of science and technology.[24] It is a combination of many activities which involve the designing of the artificial in computers that are like recognizing the speech, learning, planning and solving problems,[25] in the different areas of human existence including crime detection, crime prevention *et cetera*.

Artificial intelligence has elements of cognitive and emotional intelligence, that is to say that it exhibits characteristics of all types of competencies and is able to be self-aware in its interactions.[26] Artificial intelligence is capable of resolving the several complications that arise during crime prevention efforts. This is due to the variety of crime types, motives, repercussions, handling methods and prevention techniques.[27]

These complications and various attributes have made crime prediction very difficult especially with the use of the traditional method, hence artificial intelligence will be capable of reducing crime and ensuring the lives and safety of people in different locations in Nigeria.

The traditional way of crime prevention and detection has always been manually carried out, and of course it is not without difficulties. By contrast, artificial intelligence collected by law enforcement agencies to extract patterns and predict future events.[28] One of the most useful applications of artificial intelligence for preventing and lowering crime rate is in resource allocation. Law enforcement agencies are challenged by shortages of personnel and funds, the value and importance of resource allocation and deployment plays a vital role in crime prevention.[29]

Artificial intelligence can determine and identify relevant patterns of crime that can best be addressed through adjustment in resource allocation such as timing of police car patrols, walking patrols, security

[24] Ghosh, M. and Arunachalam, T., "Introduction to Artificial Intelligence" *www.researchgate. net*. accessed 30/7/2024.
[25] Vema, M., Artificial Intelligence and its Scope in Different Areas with Special References to the Field of Education. *https://files.eric.edu.gov,* accessed 30/7/2024.
[26] Kanu, I.A., Adidi, D.T., and Kanu, C.C. Artificial Intelligence and Cybercrime in Nigeria. *https://www.researchgate.* accessed 30/7/2024.
[27] Dakalbab, F., Talib, M.A., Waraga, O.A, and Nasir, Q. "Artificial Intelligence & Crime Prediction: A Systematic Literature review" *www.sciencedirect.com*. accessed 30/7/2024.
[28] Dakalbab (n 27).
[29] Voyager, "Leveraging Artificial Intelligence for Crime Prevention" *www.voyager.tabs.com*. accessed 30/7/2024.

guards, physical barriers and response time of emergency[30]. Other uses of artificial intelligence in combating and preventing crime stems from the fact that it can compare data to find connections between incidents that may seem unrelated, helping to solve crime.[31] It can also be used to avoid bias that can influence human decision making by ensuring that decisions are based on facts and patterns rather than beliefs or stereotypes.[32]

Both financial companies and other companies generally can use artificial intelligence to prevent and detect everything concerning crime ranging from employee theft to insider trading.[33] Artificial intelligence can also be used to prevent money laundering and block illicit contents like child pornography,[34] all of which are components of cybercrime.

3.0 Using Artificial Intelligence to Break the Chains of Cybercrime in Nigeria

Nigeria's efforts to combat Cybercrime have primarily focused on the use of traditional methods such as law enforcement and regulatory actions.[35] The Economic and Financial Crimes Commission has remained over burdened with the weight of combating cybercrime in Nigeria, hence it has become an organized threat and an onslaught to the development of the nation. The said threat of cybercrime has expanded beyond conventional criminal activity and has now posed a threat to the national security of all countries, including the most technologically advanced ones.[36] It is not limited to a particular sector but affects a wide range of establishments.[37] Nigeria is not an exception to nations targeted by cybercrime, hence the need to use artificial intelligence to complement the efforts of law enforcement agencies to combat same.

To enhance the efforts of law enforcement agencies on breaking the chains of cybercrime in Nigeria, the integration of artificial intelligence can significantly booster the efforts of anti-corruption agencies like the Economic and Financial Crimes Commission in several ways including;

a. Pattern Recognition

Artificial intelligence trained on vast data sets can be used to detect anomalies in user behaviour. That is to say that unusual transactions and suspicious login attempts can be detected much faster and more accurately than humans. Such situation may assist the agency to move fast in preventing any such cybercrime by nipping it in the bud.[38]

b. Making Prevention a Priority

Artificial intelligence will encourage the making of prevention a priority and not punishment.[39] This it can do by delving into financial systems and online interactions, pinpointing vulnerabilities and areas

[30] *Ibid.*
[31] Police, An Introduction to how Al is transforming real time crime centers. *www.police .com.* accessed 30/7/2024.
[32] *Ibid.*
[33] Oliver Wyman, The Risks and Benefits of using Al to Detect Crime *www.oliver wyman.com* accessed 30/7/2024.
[34] *Ibid.*
[35] Obinna U. "Breaking the chain of cyber fraud in Nigeria: Al Revolution" *www.thecable.ng.* accessed 30/7/2024.
[36] Umah-Baba, M.N. "Entrancing Nigeria's cyber security with Artificial Intelligence *techdigest.ng* accessed 30/7/2034.
[37] *Ibid.*
[38] Obinna (n 35).
[39] *Ibid.*

susceptible to fraud.[40] The risk assessment capacity allows authorities to prioritize preventive measures, allocating resources efficiently and strategically fortifying potential weak spots before they are taken advantage of timeously.

c. Timeous Response to Cybercrime Stimulus

The advancement in information technology has given cybercrime perpetrators numerous advantages to commit cybercrime in Nigeria. Growing trends of complex distributed together with internet corrupting has raised questions about information security and privacy.[41] Hence with the pace and number of cyber-attacks, human intervention is simply not sufficient for timely attack analysis and appropriate responses, hence combating cybercrime with intelligence and semi-autonomous agents that can detect, evaluate and respond to cybercrime attacks[42] has become very necessary in the fight against cybercrime in Nigeria.

However artificial intelligence in not a magic bullet skilled. Security teams are still needed to interpret artificial intelligence insight, tune its detection and manage the response work flow.[43] Nigeria security agencies must view artificial intelligence as a force multiplier and not wholesale replacement for human driven cyber security.[44] Hence it has become necessary for legal mechanism to be put in place in Nigeria for this purpose.

4.0 Use of Artificial intelligence against cybercrime in other jurisdictions

Under the American jurisdiction, the Federal law enforcement agencies are already using artificial intelligence but to the extent of reviewing calls for anything a human might have missed.[45] In as much as artificial intelligence is revolutionizing the fight against cybercrime in America through its fundamental component, which include threat monitoring, behavioral analyses, fraud detection,[46] it is still being used with caution for evidential reasons, and without compromising privacy rules. To ensure that the use of artificial intelligence is not abused, the American government put in place a legislation to regulate the development and deployment of artificial intelligence.[47]

Under the South African jurisdiction, there is no existing legislation or regulatory framework to govern the use of artificial intelligence, rather South Africa is heavily dependent on the application of data protection legislation for the regulation of artificial intelligence.[48] However, the Africa Union through its Artificial Intelligence regulation and policy in Africa has made it crucial that government in Africa must not only develop their artificial intelligence but also ensure effective regulation.[49] Hence the AU

[40] *Ibid.*
[41] Dilek, S., Cakir, H., and Aydin, M. Application of Artificial Intelligence Techniques to combat cybercrimes: A Review, [2015] 6 (1), *IJAIA*, accessed 31/7/2024.
[42] *Ibid.*
[43] Taidum, M., Leveraging Al and machine training for more proactive cyber defence *www.linkectin .com* accessed 31/7/2024.
[44] *Ibid.*
[45] Mckay, T., "Here is how Federal Law enforcement officially are actually using Al" *www.ltbrew.com* accessed 1/8/2024.
[46] Demkorych, T., Cyber security: How Artificial Intelligence is Revolutionizing the fight against cybercrime. *forbytes.com* accessed 1/8/2024.
[47] Mckay (n 45).
[48] BCLP, US State-by-state Al Legislation. www.bclpar.com accessed 1/8/2024
[49] Dentons, "Al Regulation and policy in Africa" *www.dettous.com* . accessed 1/8/2024.

Development agency published a draft policy to advance the idea of setting out a blue print for artificial intelligence regulation by member states.[50] In reaction to this policy, a good number of countries within the African Jurisdiction have taken steps to address this usage policy challenge, hence Nigeria is encouraged to join in this initiative for purposes of tackling crimes of various degrees including cybercrime.

5.0 Challenges to the use of Artificial Intelligence in the fight against Cybercrime in Nigeria

Despite the potential benefits of using artificial intelligence in the fight against cybercrime,[51] Nigeria is faced with a lot of drawbacks. Such draw backs include, the absence of an existing legal framework to back its usage. The Cybercrime (Prohibition and Prevention) Act 2015 did not in any way provide for the use of artificial intelligence. The objectives and purpose of the said act is to provide an effective, unified and comprehensive legal framework for the prohibition, prevention detection, prosecution and punishment of cybercrime in Nigeria,[52] as well as ensure the protection of critical national information, infrastructure and promote cyber security and protection of computer systems and network electronic communication, data and computer programmes, intellectual property and privacy rights.[53]

Certainly, the Act criminalized cybercrime such as unlawful access to computers, unauthorized modification of computer systems, network data, computer associated forgery, computer related fraud, theft of electronic devices. The Act obviously provided for the modalities for holding internet fraudsters liable for internet fraud and crimes and never made any provision for the role of artificial intelligence in this regard.[54]

Another challenge associated with using artificial intelligence to fight cybercrime in Nigeria is the potential for biases. Artificial intelligence systems are only as good as the data they are trained on and if the data is biased or incomplete, the artificial intelligence system will produce biased results.[55] Nigeria may likely face this risk due to low level of technological development and this may not only pose a challenge in the use of artificial intelligence in the fight against cybercrime but also place a negative burden on the prosecution in proving its case beyond reasonable doubt in court. The integration of artificial intelligence in the fight against cybercrime has the potential of heightening impersonation scams.[56] These scams involve creating fake websites and social media profiles, using the names and images of well-known figures to deceive the public.[57]

Furthermore, inadequate proactive measures by the Nigerian government have been identified as a challenge threatening the integration of artificial intelligence in the fight against cybercrime in Nigeria.[58] The continued perpetration of cybercrime by non-state actors without adequate proactive measures put in place would certainly jeopardize the chances of achieving success in the event that

[50] *Ibid*.
[51] Noonan, L., Benefits and Challenges of Al on cyber security =ompliance.com accessed 2/8/2024.
[52] Kalu, U.C and Odama, O.U., An Examination of criminal liability of Artificial intelligence entities: Nigeria law in factors, *wwwseahipaj.com* accessed 2/8/2024.
[53] Part III, SS.5-36 Cybercrimes (Prohibition, prevention…) Act, 2015.
[54] Noonan (n 51).
[55] *Ibid*.
[56] Aina, D., "Al Manipulation will Raise Cybercrime in 2024 *punchng.com* accessed 2/8/2024
[57] *Ibid*.
[58] Akintaro, S. "FG moves to amend Cyber Crime Act over threat of A1, other emerging Technology" *nairametrics.com* accessed 2/3/2024.

artificial intelligence is integrated in the fight against cybercrime in Nigeria. This is so because the activities of cybercrime perpetrators are increasingly becoming sophisticated with recent technological development in the global village. Hence it is suggested that the cybercrime law of Nigeria be amended to accommodate the issues emerging from developments in artificial intelligence.

6.0 Prospects

For Nigeria to integrate artificial intelligence in the fight against cybercrime, it must put in place a legal framework to accommodate the use of same. In addition, the government must prioritize investing in the artificial intelligence technology and ensure adequate international cooperation to combat the malady. Although corruption and limited resources may combine with other factors to hinder effective implementation of certain approaches positive to this development, but adequate political will is key to its success.

As Africa's populous nation and largest economy, Nigeria has the potential to become a leader in artificial intelligence driven Cyber Security. Since it will assist in protecting her citizens, institutions and economy as well as safeguarding its digital future and fostering trust in its online ecosystem.[59]

Fostering trust in an online ecosystem involves the use of artificial intelligence to respond to Cyber-attack in a more effective manner to entrance the detection of threats. Hence the integration of artificial intelligence in the fight against cybercrime will effectively utilize the artificial intelligence powered to solutions to analyze forms of data on real time and identify vulnerabilities that humans can miss. Nigeria is enjoined to put in place a specific law or regulation that directly regulates artificial intelligence for purposes of enabling the development of artificial intelligence as it is the trend in Africa and international community.

7.0 Conclusion

In conclusion, effective measures in the fight against cybercrime are integral to a nation's economic development, investors attraction, tourism and immigration. It must be noted that cybercrime has caused a great financial damage globally including Nigeria, where cybercrime perpetrators often use artificial intelligence for their own purposes. Such purposes include creation of new malware and hacking tools, automating, phishing attacks for loopholes in security, and using fake deep technology and malicious bots to impersonate people.[60]

Artificial intelligence will enable a good fight back in this regard. This can only be possible if it is integrated into the system by creating a legal mechanism upon which it can be anchored to fight this malady. The gains of leveraging on artificial intelligence to fight cybercrime are numerous. For instance, it can assist not only security agencies to prevent cybercrime but also for companies to detect and prevent cybercrime that can cause financial damage and harm their reputation. Findings have disclosed that artificial intelligence has made significant progress in both cybercrime detection and

[59] Obinna (n 35).

[60] Xiau, Z., Havyarimana, V., Nibigira, N., "Artificial Intelligence Adoption for Cybercrime in Africa" *https://www.scrip.org/journal/jis*. accessed 3/8/2024.

prevention and other areas of crime detection and prevention hence, it has the potential of revolutionizing the fight against cybercrime.

8.0 Recommendations

The threat of cybercrimes has expanded beyond the conventional criminal activity and now poses a threat to the national security of the international community, including the most technology advanced ones. Nigeria is also on the target list of cybercrimes; hence it is recommended that a legal framework be put in place to accommodate the artificial intelligence in the fight against cybercrime.

Again, it is suggested that personnel of security agencies and law enforcement agents be trained in areas of the use of artificial intelligence in the prevention and detection of cybercrime. These areas bother on the protection of digital assets and sensitive data, which might require them to do a thorough risk assessment.

In most cases and under certain conditions workers in an establishment may make mistakes and cybercriminals quickly take advantage of such human mistakes to perpetrate their criminal acts hence the need to teach workers the best practices in data protection and keep them informed in cyber security. Integrating artificial intelligence in the fight against cybercrime requires awareness. There should be sensitization and accurate dissemination of information on the need to integrate artificial intelligence in the fight against cybercrime. This will keep the nationals informed about the significance of such development.