THE ROLE OF ARTIFICIAL INTELLIGENCE IN OFFENSIVE AND DEFENSIVE STRATEGIES IN CYBERSPACE ARMS RACE IN THE 21ST CENTURY DIGITAL LANDSCAPE IN NIGERIA

Mahmood Usman
Department of Computer Science, Nigerian Army College of Environmental Science and Technology, Makurdi, Benue State.
mahmoodusman2015@gmail.com

Abstract
The 21st century's digital transformation has heightened cyber threats, making traditional defenses inadequate. Artificial Intelligence now drives cybersecurity with adaptive, real-time threat detection and response. However, its adoption introduces ethical, strategic, and operational challenges that require urgent consideration to balance innovation with responsible cyber governance. This study explores the evolving arms race in cyberspace, analyzing how AI is shaping both offensive and defensive strategies. It emphasizes the importance of international cooperation, ethical considerations, and the development of regulatory frameworks to govern the use of AI in cyberspace. Drawing secondary datasets from published reports, and industries whitepapers particularly from Nigeria, the study calls for integrated, forward-looking cybersecurity strategies capable of adapting to the accelerating complexity of digital threats.

Keyword: Artificial Intelligence (AI), Cybersecurity, Cyber Warfare, Cybercriminals, Phishing.

Introduction

Digital transformation has exploded in the twenty-first century, changing the way governments, corporations, and individuals function in the cyberspace. The volume, diversity, and

sophistication of cyber threats have grown alarmingly as digital ecosystems become more complex (Anda et al., 2025). Conventional cybersecurity methods, which are frequently reactive and rule-based, are becoming less effective against these changing threats. As a result, artificial intelligence (AI) has become a potent instrument in the field of cybersecurity, providing proactive and flexible defenses. Cyber-attacks have grown more complex and challenging to counter security threats as a result of the incorporation of AI into many aspects of digital infrastructure, such as threat detection, authentication, and response mechanisms (Familoni, 2024).

According to recent reports, Sub-Saharan African countries have spent over two decades actively promoting rapid growth in their information and communication technology (ICT) sectors. At present, leading nations are increasingly prioritizing the development of hybrid intelligent systems capable of managing highly complex tasks (Pantserev, 2022). AI has both advantages and disadvantages in cybersecurity. In one sense, artificial intelligence (AI) tools like machine learning, deep learning, and natural language processing facilitate automated incident response, predictive analytics, anomaly recognition, and quicker threat detection. The ability to fight inside threats, zero-day assaults, and major breaches in real time is greatly improved by these skills. However, cybercriminals are also using AI to carry out increasingly complex assaults, such as automated vulnerability exploitation, AI-generated phishing, and the development of malware that may avoid detection. demonstrates the need for more comprehensive studies on AI in cybersecurity, taking into account the non-technical elements that may affect risks produced by AI (Malatji and Tolah, 2025).

The cybersecurity sector is about to enter a new era of complexity and arms-race dynamics as both attackers and defenders incorporate AI into their toolkits. The revolutionary role of AI in cybersecurity is examined in this study, along with its main advantages, new risks, and wider ramifications for 21st-century digital security. It is essential to comprehend all aspects of AI's effects in order to create robust cybersecurity

plans that are morally sound, efficient, and flexible enough to change with the always shifting threat landscape. Osimen et al. (2024a) examined in their contribution on how AI-driven technologies are changing military tactics and the significance of creating global standards to control their application. It is imperative that researchers, policymakers, and the global community comprehend these implications (Osimen et al., 2024b). Nigeria ought to emulate nations like the United States of America (USA), Russia, China, Israel, and Estonia that have successfully incorporated artificial intelligence into their comprehensive national security framework, according to Falode (2021).

Aim and Objectives of the Study

The primary aim of this study is to examine the evolving role of Artificial Intelligence (AI) in the context of the cyber arms race, with a focus on how AI technologies are being developed and deployed for both offensive cyber operations and defensive cybersecurity measures. With the specific objectives to:

i. Analyze the role of Artificial Intelligence in enhancing cybersecurity systems.
ii. Identify and assess the opportunities offered by AI in cybersecurity.
iii. Examine the emerging threats and risks associated with the use of AI in cybersecurity.
iv. Evaluate the ethical, legal, and regulatory implications of AI-driven cybersecurity tools.
v. Propose recommendations for the responsible and secure deployment of AI in cybersecurity.

Significance of the Study

This study is significant as it examines how Artificial Intelligence (AI) influences both offensive and defensive strategies within Nigeria's evolving cybersecurity landscape. By analyzing AI's dual capacity to enhance cyberattacks and strengthen defense mechanisms, the research provides valuable insights into managing the emerging cyberspace arms race in the 21st

century. The study benefits policymakers by emphasizing the need for robust national cybersecurity frameworks, AI governance policies, and ethical guidelines to address AI-driven threats. It also aids security agencies, private organizations, and IT professionals in developing adaptive, AI-based security solutions to safeguard digital infrastructure. Academically, it expands knowledge on cyber warfare, technological sovereignty, and digital ethics from an African perspective. Ultimately, the findings aim to strengthen Nigeria's preparedness, resilience, and competitiveness in the global digital landscape.

Artificial Intelligence in Enhancing Cybersecurity Systems
Artificial Intelligence (AI) is revolutionizing cybersecurity by enhancing the ability to detect, prevent, and respond to cyber threats in real time. Through machine learning and predictive analytics, AI-driven systems analyze vast data, identify anomalies, and automate defenses, providing stronger, adaptive protection against evolving digital attacks in complex cyber environments. Chukwudi, (2019) in his submission stated that Nigeria, like many developing nations, is undergoing rapid digital transformation, driven by increased internet penetration, mobile technology adoption, and the digitization of government and business services. However, this digital growth has also exposed the country to rising cyber threats, ranging from online fraud and ransomware attacks to identity theft and data breaches. In this context, Artificial Intelligence (AI**)** is emerging as a crucial tool for strengthening Nigeria's cybersecurity posture.

Improving Threat Detection and Response: Tools with AI capabilities that are commonly used in cyber security and IT operations like CrowdStrike Falcon, Sophos Intercept X, Cisco Secure X, Microsoft Defender 365, Fortinet FortiAI, and others can examine enormous volumes of user activity and network traffic to find irregularities that might point to threats. AI provides a scalable solution for real-time threat identification in Nigeria, where many institutions lack sophisticated human

monitoring skills. These threats include malware infections, phishing attempts, and illegal access.

Combating Fraud in Finance and Telecom: The financial sector in Nigeria, especially banks and Fintech platforms, is constantly at risk from scammers. To identify fraudulent account activity, flag anomalous transaction patterns, and safeguard mobile banking systems, artificial intelligence (AI) algorithms are being used. AI is also useful to the telecom industry in tracking attempts at call interception, identity spoofing, and SIM card fraud. In order to improve national cybersecurity infrastructure, government organizations such as the Nigerian Communications Commission (NCC) and the National Information Technology Development Agency (NITDA) are starting to investigate artificial intelligence (AI) as a component of larger national cybersecurity plans. By automating compliance monitoring, intrusion detection, and security assessments, AI can help with these initiatives.

Resolving Skill Gaps and Resource Limitations: Nigeria is experiencing a scarcity of qualified cybersecurity experts. AI lessens the strain on scarce human resources and automates intricate security procedures, thereby bridging this gap. Tasks like log analysis, and alert prioritization, can be completed more quickly and precisely by AI-driven security solutions than by human workers.

Securing Critical Infrastructure and e-Government Platforms: The expansion of Nigeria's digital government services, including national identity systems, e-health, and e-

irregular internet and power supplies hinder the deployment of AI in Nigeria's cybersecurity ecosystem. AI has a lot of potentials to improve cybersecurity in Nigeria by providing scalable, intelligent, and proactive defenses. However, to fully harness its potential, the country must invest in infrastructure, policy development, capacity building, and public-private partnerships to create a secure and AI-ready digital future.

Opportunities offered by AI in Cybersecurity in Nigeria

As Nigeria continues to expand its digital footprint across banking, government services, education, and telecommunications, the role of Artificial Intelligence (AI) in cybersecurity is becoming increasingly relevant, enabling greater accessibility (Rashid and Mujadi, 2021). AI offers a range of opportunities that can significantly enhance Nigeria's ability to defend its digital infrastructure and respond to rising cyber threats. Such opportunities are outlined below, meanwhile the stakeholders' engagement in cybersecurity is shown in Table 1.

Table 1: Indicating Areas of Stakeholders Engagement

Area	Recommendation	Stakeholders
Governance	National AI-cybersecurity framework	NITDA, NCC, NSA
Privacy	Enforce NDPA 2023	NDPC, Legal Sector
Ethics	Transparency & human oversight	All sectors
Skills	AI cybersecurity training	Universities, NGOs
Risk	Security auditing & standards	ngCERT, private firms
Innovation	Support local AI tools	Startups, NITDA
Infrastructure	Critical sector AI safeguards	CBN, NNPC, Discos
Response	National AI incident strategy	ngCERT
Public Trust	Public education campaigns	Media, NGOs

Source: OpenAI, (2025)

Some of the opportunities offered by AI in cybersecurity in Nigeria are presented in Figure 1.

Figure 1: Representing opportunities offered by AI in cybersecurity.

Automated Threat Detection and Real-Time Monitoring: With AI, networks and systems can be continuously monitored to identify irregularities and possible risks instantly. This is especially helpful in Nigeria, where resource shortages frequently make manual monitoring impossible. Artificial intelligence (AI)-driven intrusion detection systems (IDS) can automatically spot suspicious patterns, such as illegal access or odd data transfers, which speeds up response times and increases threat visibility. Detecting insider threats and data breaches with little human involvement has a high potential for adoption in public organizations, banking, and telecommunications.

Fraud Prevention in Financial Services: The financial industry in Nigeria is frequently the subject of cybercrimes such as SIM switch schemes, account takeovers, and phishing. Artificial intelligence (AI)-driven systems can identify fraud in milliseconds by analyzing transaction history and consumer behavior, highlighting high-risk activity for further examination, immediate use and financial gain, particularly

for banks and mobile money providers. Building consumer trust in digital financial services and lowering fraud losses are two benefits of AI.

Enhanced Cyber Threat Intelligence (CTI): AI is capable of processing enormous volumes of global threat data to produce useful cyber threat intelligence. Nigerian firms are able to proactively protect against both local and international cyber threats by employing machine learning to track malware signatures, dark web activity, and phishing efforts. Additionally, national cybersecurity agencies can gain a Strategic advantage for national cybersecurity agencies (e.g., NCC, NITDA) to share intelligence across sectors and develop predictive protection systems. Companies should focus ongoing training for cyber-security specialists and invest in AI-driven cyber-security systems to improve overall security resilience and their capacity to handle new attacks (Chigozie et al., 2025).

Workforce Optimization: Given Nigeria's lack of qualified cybersecurity specialists, artificial intelligence (AI) solutions can automate a number of standard security duties, including log analysis, alarm prioritization, and system auditing, freeing up human experts to concentrate on more complex decision-making and reaction tactics. Both the public and private sectors stand to gain a great deal from the incorporation of AI in Nigeria's cybersecurity environment. AI provides a scalable and clever method of protecting Nigeria's digital environment, from threat intelligence and fraud detection to infrastructure protection and labor assistance. However, deliberate investments in AI infrastructure, data quality, and policy frameworks are necessary to fully achieve these advantages.

Emerging Threats and Risks Associated with the use of AI in Cybersecurity in Nigeria

While there are many cybersecurity advantages to artificial intelligence (AI), its use also brings with it new and complicated threats, especially in a developing country like Nigeria. Numerous risks and weaknesses have surfaced as a result of the growing integration of AI into cybersecurity defenses and

hackers' tactics, which could jeopardize the security of organizational data and national digital infrastructure. Research report has revealed that over 90% of African enterprises lack basic cybersecurity protocols, leaving them susceptible to attacks like phishing, ransomware, and hacking. (Ogene, 2024). In order to cause the system to misclassify threats, adversarial inputs can be used to discreetly change data in AI models. This presents a significant risk to systems that mostly rely on machine learning for threat detection in Nigeria. Attackers could exploit these flaws to bypass intrusion detection, compromising biometric security systems used in digital identification programs and banking services.

Cybercriminals are leveraging AI to automate and scale attacks, this includes: AI-generated phishing emails that mimic human language patterns, Voice cloning and deep fakes for social engineering scams (e.g., impersonating bank officials), AI-enhanced password cracking and botnet attacks. In Nigeria, where cyber fraud is already a significant challenge, such techniques could dramatically increase success rate and reduce detection time. This is critical because it would make assaults on financial institutions, SMEs, and government agencies substantially more sophisticated and effective. AI systems require large datasets to function effectively. In Nigeria, where data privacy regulations are still evolving, the use of personal or sensitive data for AI training can lead to violations of citizens' privacy rights. Poor data governance may also result in unauthorized data sharing or breaches, which can lead to regulatory violations, reputational damage, and erosion of public trust in digital services. In a country with limited cybersecurity personnel, organizations may over depend on AI systems without sufficient human oversight. This could result in missed alerts due to algorithm bias, false positives that overwhelm IT teams, undetected novel attacks outside the AI model's training scope. Human oversight remains essential to validate AI decisions and intervene in complex scenarios. Only a few large financial institutions and tech companies in Nigeria

currently have the resources to deploy advanced AI cybersecurity solutions. This leaves many small and medium-sized enterprises (SMEs) and public institutions unprotected, increasing the overall vulnerability of the national cyber ecosystem. This creates a digital divide in cybersecurity capabilities, potentially making SMEs soft targets for attackers.

While AI brings transformative potential to Nigeria's cybersecurity efforts, it also introduces sophisticated and evolving threats. Policymakers, cybersecurity professionals, and stakeholders must recognize these emerging risks and invest in building AI systems that are not only intelligent but also secure, transparent, and ethically governed. A hybrid approach combining AI with human expertise, robust regulations, and international cooperation is essential for mitigating these threats in Nigeria's rapidly digitizing economy. Violations can result in legal penalties if AI systems collect, store, or analyze data beyond legal bounds. AI decisions (e.g., access denial) must be explainable and reviewable, especially in regulated sectors. Legal issues may arise if individuals cannot challenge AI-driven actions that affect them. Determining liability for damages caused by erroneous AI decisions is complex. Organizations must clarify whether the AI developer, the user, or the organization bears responsibility

There is ambiguity since current legislation frequently lag behind AI breakthroughs. Although they have not yet been unified globally, regulatory frameworks (such as the EU AI Act) are changing. International data rules must be followed by AI cybersecurity technologies that evaluate data from throughout the world. Principles of data sovereignty may be violated by errors in cross-border processing. Therefore, for safety and compliance, regulatory agencies may demand that AI technologies undergo routine audits. Insurance eligibility or certifications may be impacted if changing standards are not met.

Strategic Future Directions for Nigeria

As Nigeria advances in its digital transformation journey, the

integration of Artificial Intelligence (AI) into cybersecurity presents a double-edged reality, offering immense opportunities for innovation and enhanced protection. By adopting these frameworks and best practices as well as working together, Nigeria can create a secure and prosperous digital future (Ahmed, 2023). While simultaneously introducing new threats that could compromise national security and personal privacy. The following key future directions are outlined:

The Needed Opportunities

AI will evolve to detect complex, previously unseen cyber threats (zero-day attacks) using unsupervised learning and anomaly detection, enabling Faster, real-time mitigation of threats across critical infrastructure such as banking (BVN systems), telecoms, and government databases. AI-driven Security Orchestration, Automation, and Response (SOAR) tools will automate routine incident responses. It enhances efficiency in Nigeria's under-resourced cybersecurity teams and shortens the lifecycle of threat resolution.

Table 2: AI Focus Areas and Action Plan

Focus Area	Action Plan
National Strategy	Develop a comprehensive National AI-Cybersecurity Masterplan
Legislation	Update NDPA and ICT laws to cover AI-specific cyber risks
Innovation Ecosystem	Fund R&D in AI-based cybersecurity tools through TETFund, BOI, and NITDA
International Cooperation	Collaborate with AU, ECOWAS, and global bodies on AI security standards
Infrastructure	Invest in secure cloud platforms and national cybersecurity labs
Public Awareness	Launch national campaigns to educate citizens on AI threats and cyber hygiene

Source: Open AI

Threats

Criminals may use AI for phishing, deep fake scams, and automated penetration testing. Harder-to-detect scams targeting financial institutions, political actors, or the general public. On the other hands, over- reliance on AI surveillance tools without proper safeguards could infringe on citizens' rights. Violation of NDPA 2023 and potential loss of public trust in digital services. AI's pace of evolution may outstrip Nigeria's regulatory capacity. Unregulated AI deployment in critical sectors could lead to unintended consequences. AI is set to redefine the future of cybersecurity in Nigeria transforming both the threats and the tools to defend against them. With proactive policies, investments in skills and infrastructure, and robust regulatory oversight, Nigeria can position itself as a regional leader in secure and ethical AI deployment for cybersecurity.

Findings

The following findings were deduced from this paper:

i. The ongoing competition between attackers and defenders using AI has led to rapid innovation on both sides. However, this has also introduced instability and unpredictability, as new vulnerabilities emerge with each advancement.

ii. Malicious actors are increasingly using AI to develop

evasive malware, generate deep fake content, automate phishing campaigns, and conduct adaptive reconnaissance. These tools allow cybercriminals to bypass traditional defenses, making attacks more targeted, scalable, and difficult to detect thus intensifying the arms race in cyberspace.

iii. The lack of comprehensive governance frameworks especially in developing countries limits the ability to manage AI-enabled threats and enforce responsible use of autonomous defense tools.

iv. Integrating AI with skilled human oversight is essential to maintain control and adapt to future cyber challenges.

Conclusion

The integration of Artificial Intelligence into cybersecurity marks a significant turning point in the digital defense landscape of the 21st century. As this paper has explored, AI technologies such as machine learning, deep learning, and natural language processing have empowered organizations and governments to detect threats faster, automate incident responses, and predict attacks with remarkable accuracy. These capabilities are vital in an era where cyber threats are not only increasing in frequency but also growing more sophisticated and adaptive. However, this same technology is being weaponized by malicious actors, giving rise to an AI-driven arms race in cyberspace. The ability of cybercriminals to exploit AI for automated attacks, evasion techniques, and synthetic content generation has elevated the threat level far beyond what traditional security tools can manage.

As a result, the cybersecurity community must both use AI for defense and reduce the dangers associated with crimes made possible by AI. A balanced approach is required in this arms competition, one that incorporates strong moral principles, regulatory supervision, ongoing innovation, and global collaboration. The development of flexible, accountable, and open systems that can foresee and thwart AI-enhanced threats

will be just as important to cybersecurity in the future as technological growth. In order to stay ahead in this changing battlefield, protecting the digital landscape in this AI-driven future will ultimately necessitate a confluence of machine capabilities, policy innovation, and human intellect.

Recommendations

The following recommendations are made:

i. The Federal Government, through agencies such as National Information Technology Development Agency (NITDA) and Nigerian Communications Commission (NCC), should develop a regulatory framework specific to AI in cybersecurity to provide clear guidance on ethics, data protection, and acceptable AI use in both public and private sectors.

ii. Build local capacity and skills through training programs for cybersecurity professionals, emphasizing AI, machine learning, and ethical tech deployment.

iii. Encourage Public-Private Partnerships (PPPs) to foster collaborations between government, fintechs, telcos, and cybersecurity firms like NIIT or Cisco Networking Academy. To share threat intelligence, pool resources, and co-develop AI tools adapted to Nigerian threat landscapes.

iv. Support Local AI Innovation by providing grants, tax incentives, and incubation for local startups developing AI-driven cybersecurity tools, in order to reduce dependency on foreign tools and tailor solutions to local needs (e.g., fraud detection in mobile money platforms).

v. Protect critical infrastructure with AI safeguards to deploy vetted AI tools with strong fail-safes, to prevent AI-driven systems from becoming points of failure in national infrastructure.

vi. Establish a Nigerian Computer Emergency Response Team (ngCERT) extension specifically for AI in order to develop a national AI incident response strategy that will enable prompt national coordination and response

to AI-related cyber incidents.

vii. Participate in civil society initiatives and inform the public about AI in cybersecurity and the rights of citizens under data protection regulations. to stop false information from spreading, foster trust, and guarantee that everyone involved uses it responsibly.

References

Ahmed, A. A. (2023). A Multi-Pronged Framework for a Cyber secure Nigeria. *Scientific and Practical Cyber Security Journal (SPCSJ)* 8(1): 69 – 75. ISSN 2587-4667

Afieroho, P., Perkins, R., Zhou, X., Hoanca, B. and Protasel, G. (2023). Adopting e-government to Monitor Public Infrastructure Projects Execution in Nigeria: *The Public Perspective*. *Heliyon*. 9(8):e18552. doi: 10.1016/ j.heliyon.2023.e18552.

Anda, J., Kulugh, V., Aimufua, G., Ozogwu, Y. and Bala, H. (2025). Applications and Challenges of Artificial Intelligence in Cybersecurity. *Dutse Journal of Pure and Applied Sciences.* 11(1):130 – 143.

Rani, V., Kumar, M., Mittal, A. and Saluja K. K. (2022). Artificial Intelligence for Cybersecurity: Recent Advancements, Challenges and opportunities. Studies in Computational Intelligence. Pp 73 – 88.

Chigozie, E., Ikebude, O. D. and Okure, E. (2025). Artificial Intelligence and Cyber-Security in Nigeria: Communicative Strategies for Risk Mitigation and Opportunities in Digital Security. *Researchgate*. DOI:10.5281/zenodo.1518339

Chukwudi, C. E., Gberevbie, E. D., Abasilim, U. D., and Imhonopi, D. (2019). IPOB Agitations for Self-Determination and the Response of the Federal Government of Nigeria: Implications for Political Stability. *Academic Journal of Interdisciplinary Studies*. 8(3), 179-19.

Falode, A. (2021). Artificial Intelligence: The Missing Critical Component in Nigeria's Security Architecture. *LASU Journal of History and International Studies.* https:// www.academia.edu/50309377/Artificial_Intelligence.

Familoni, B. T. (2024). Cybersecurity Challenges in the Age of AI: Theoretical Approaches and Practical Solutions. *Computer Science and IT Research Journal*. 5(3):703 – 724.

Felix, A. O. and Oluwapelumi, O. S. (2020). Challenges and Opportunities of Ai-Driven Cybersecurity for Small and Medium Enterprises (SMEs) Towards Poverty Reduction in Nigeria. *Scientific and Practical Cyber Security Journal.* 8(3):74 – 83.

Malatji, M., Tolah, A. (2025). Artificial Intelligence (AI) Cybersecurity Dimensions: A Comprehensive Framework for Understanding Adversarial and Offensive AI. *AI Ethics* (5):883–910. https://doi.org/10.1007/s43681-024-00427-4

Ogene, F. (2024). Cybersecurity and IT Governance Challenges in Nigeria: Strategic Investment Needs and the Path Forward for a Resilient Digital Economy. International Journal of Computer Applications. 186, (55) (0975 – 8887).

Osimen, G., Newo, M. and Fulani, O. (2024). Artificial Intelligence and Arms Control in Modern Warfare. *Cogent Social Sciences*. 10 (10):2407514.

Osimen, G. U., Fulani, O. M., Chidozie, F., & Dada, D. O. (2024). The Weaponisation of Artificial Intelligence in Modern Warfare: Implications for Global Peace and Security. *Research Journal in Advanced Humanities*, *5*(3). https://doi.org/10.58256/g2p9tf63.

Pantserev K.A. (2022). Malicious Use of Artificial Intelligence in Sub-Saharan Africa: Challenges for Pan-African Cybersecurity. *International Relations*. 22(2).288 - 302. doi: 10.22363/2313-0660-2022-22-2-288-302

Rashid, F. and Mujadi, M. (2021). Achieving Cyber Resilience in Nigeria E-Government Platforms using Adaptive Zero-Trust Models. *Research.* https://

www.researchgate.net/publication/394521552

Saladin, Q. A. (2018). Evaluation of Protection of Critical Infrastructure in Nigeria: A Case Study of Protection of Power Facilities in Abuja. *European Scientific Journal*. 14 (11):80-95. Doi: 10.19044/esj.2018.v14n11p80 URL:http://dx.doi.org/10.19044/esj.2018.v14n11p80

Temilade O. A. (2025). The Impact of Cybersecurity Governance on National Security by Strengthening Critical Infrastructure through IT Auditing and Risk Management. *Asian Journal of Research in Computer Science*. 18 (4):301–322. https://doi.org/10.9734/ajrcos/2025/v18i4621.