UCC Law Journal. Volume 4 Issue 2, March, 2025, 157-208
DOI:10.47963/ucclj.v4i2.1722

STRIKING A BALANCE: AI, NATIONAL SECURITY, AND PRIVACY RIGHTS IN NIGERIA

Oghomwen Rita Ohiro[1]

ABSTRACT

Nigeria, like many other nations, is increasingly utilising artificial intelligence (AI) for national security purposes. While AI presents opportunities such as enhanced threat detection and cybercrime prevention, its use also raises concerns about individual privacy and potential misuse. This paper investigates the challenges Nigeria faces in balancing national security with privacy rights in deploying AI technologies. The research employs a doctrinal approach, analysing legal frameworks, government policies, and relevant academic literature, complemented by insights from structured interviews from reputable newspapers and credible publications featuring industry experts in national security and technology. It highlights the benefits and risks of AI in national security while offering recommendations for a national AI strategy tailored to Nigeria's unique context. The proposed strategy emphasizes clear legal frameworks, robust oversight mechanisms, ethical guidelines for data use, and public education on AI and privacy rights. These measures aim to enable Nigeria to leverage AI for national security while safeguarding the rights of its citizens.

Keywords: Artificial Intelligence, Data Privacy, National Security, Nigeria, Oversight Mechanisms

INTRODUCTION

Artificial intelligence (AI) is rapidly becoming a powerful tool for national security, playing a crucial role in several areas such as enhanced intelligence gathering and analysis, planning and support for military operations, autonomous weapon systems (future potential), human-machine teaming, managing and utilizing big data among others.[2] By harnessing the power of AI in these ways, nations can gain a significant advantage in protecting their citizens and deterring

[1] University of Benin, Benin City, Nigeria, Senior Lecturer, oghomwen.igbinedion@uniben.edu

[2] I Szabadföldi, 'Artificial Intelligence in Military Application - Opportunities and Challenges' (2021) XXVI *Land Forces Academic Review* 157.

potential threats. Therefore, countries, for example, the United States, are actively exploring AI applications across a spectrum of military operations.[3] Research in AI spans intelligence gathering and analysis, logistical support, cyber warfare, information manipulation, command and control systems, and the development of semi-autonomous and autonomous vehicles.[4] Notably, AI has already found its way into military endeavours in regions like Iraq and Syria.[5]

Similarly, countries like China and Russia, regarded as strategic rivals, are heavily investing in AI for purposes related to national security.[6] Nigeria is currently grappling with intricate security issues and is following the global trend of exploring the use of Artificial Intelligence (AI) for enhancing national security measures.[7] Artificial intelligence (AI) refers to the ability of machines to mimic human cognitive functions such as problem-solving, communication, and interacting with the world.[8] AI leverages machine learning, where algorithms sift through mountains of data to identify patterns.[9] These patterns can then be used for making predictions, planning, and problem-solving.[10] AI can be used in big

[3] Congressional Research Service 'Artificial Intelligence and National Security' <https://sgp.fas.org/crs/natsec/R45178.pdf> accessed 9 May 2024.

[4] Ibid.

[5] Ibid.

[6] US Government Accountability Office 'How Artificial Intelligence Is Transforming National Security' (*GOA Watchblog*, 19 April 2023) <https://www.gao.gov/blog/how-artificial-intelligence-transforming-national-security#:~:text=AI%20in%20national%20security%2C%20on,integrate%20AI%20into%20defense%20systemson> accessed 9 May 2024.

[7] R Ibeh, 'Deploying Artificial Intelligence To Tackle Nigeria's Security Challenges' (*National Economy*) <https://nationaleconomy.com/deploying-artificial-intelligence-to-tackle-nigerias-security-challenges/#:~:text=In%20line%20with%20this%2C%20the,and%20information%20and%20communication%20security> accessed 9 May 2024.

[8] H Gil De Zúñiga and others, 'A Scholarly Definition of Artificial Intelligence (AI): Advancing AI as a Conceptual Framework in Communication Research' (2023) 4(2) *Political Communication* 317-344.

[9] Guinn Center for Policy Priorities, 'Introduction Artificial Intelligence Defined' <https://guinncenter.org/wp-content/uploads/2024/04/AI-General-Overview-KBC-Edit-V2-040424.pdf > accessed 23 May 2024.

[10] Ibid.

data analysis and decision-making systems.[11] AI is rapidly developing and having a significant impact on national security capabilities.[12]

Numerous national security challenges confronting Nigeria today stem from diverse terrorist organisations.[13] Nigeria's national insecurity results from several factors, such as elevated poverty and unemployment levels, religious intolerance, income disparities, ethnic tensions, increasing assimilation, demands for resource control, limited industrial productivity, fluctuating and declining exchange rates, soaring inflation, insufficient infrastructure, substantial domestic debt, escalating external debt, and widespread lack of awareness.[14] Since 2009, the activities of the Boko Haram group have presented a significant security challenge for the nation, leading to northern Nigeria, especially the northeast region, being characterized as the most perilous area to reside in.[15]

Boko Haram's activities surged in August 2011, marked by frequent bombings in public areas and churches across north-eastern Nigeria. [16] Since then, the group has continued to carry out attacks, resulting in loss of life, property destruction, exacerbation of food and nutrition insecurity, propagation of infectious diseases, hindrance of education access for millions of children and youths, and a rise in the

[11] A Zimmermann, K Vredenburgh and S Lazar, 'The Political Philosophy of Data and AI' (2022) 52(1) *Canadian Journal of Philosophy* 1–5.

[12] E Afsah, 'Artificial Intelligence, Law and National Security' in S. Voeneky *et al* (eds), *The Cambridge Handbook of Responsible Artificial Intelligence*, (Cambridge University Press, 2022)

[13] A Abiodun, 'A Comparative Analysis of the Legal Framework for the Criminalization of Cyberterrorism in Nigeria, England, and the United States' (2021) 12(1) *Nnamdi Azikiwe University Journal of International Law and Jurisprudence* 99.

[14] OI Eme and TO Oyinshi, 'Boko Haram and Security Challenges in Nigeria' (2014) 2(11) *Kuwait Chapter of Arabian Journal of Business and Management Review*, 14*;* L Raimi, I Akhemonkhan . and OD| Ogunjirin 'Corporate Social Responsibility and Entrepreneurship (CSRE): Antidotes to Poverty, Insecurity and Underdevelopment in Nigeria' 6th International Conference held in Universiti de Lome, Togo) from 1st to 2nd November 2012), Gubak HD and Bulus K, 'National Security Challenges and Sustainable Development in Nigeria: A Critical Analysis of the Niger Delta Region' (2018) 4 *Global Journal of Political Science and Administration*, 34. J I Ebeh, 'National Security and National Development: A Critique' (2015) 4 IJCR 1.

[15] OI Eme and TO Oyinshi, 'Boko Haram Insurgency in Nigeria: Implications for National Security and Restorative Justice' (2019) 19 *African Journal on Conflict Resolution* 1-17.

[16] Ibid, 16.

number of internally displaced persons in Nigeria.[17] The efforts of state security agencies against Boko Haram have proven ineffective, as the group's activities and membership continue to grow.[18] Similarly, the Nigerian government's conflict-resolution methods, implemented through the military Joint Task Force, have fallen short of fostering peaceful coexistence in the affected communities. [19]

There have been calls for the integration of AI as a tool in combating insecurity, including insurgency, in Nigeria.[20] According to an interview conducted with Senator Jimoh Ibrahim, who represents Ondo South and chairs the Senate Committee on Inter-Parliamentary Affairs, President Bola Tinubu's administration is set to integrate artificial intelligence (AI) into its security strategy to tackle Nigeria's ongoing challenges by 2025.[21] Ibrahim revealed that ₦4.91 trillion has been earmarked for defence and security in the 2025 budget proposal, underscoring the administration's prioritization of national security.[22] Speaking during a televised discussion on *Politics Today*, the senator emphasized the government's intention to deploy advanced technological tools, including AI-driven applications, to monitor and combat threats such as banditry, kidnapping, and terrorism.[23] He predicted that 2025 would mark a turning point in Nigeria's fight against criminal activity, as these innovative measures aim to bolster security efforts across the nation. Currently, Nigeria is developing a comprehensive National AI Strategy by engaging global Nigerian AI experts.[24] The Federal

[17] NS Amalu, 'Impact of Boko Haram Insurgency on Human Security in Nigeria' (2015) 14 *Global Journal of Social Sciences* 35.
[18] Eme and Oyinshi,, (n15) 16.
[19] A Akubo and BI Okolo, 'Boko Haram Insurgency in Nigeria' 1-17 < https://www.accord.org.za/ajcr-issues/boko-haram-insurgency-in-nigeria/> accessed 26 August 2024.
[20] F Olokor, 'Nigeria Can Fight Boko Haram, insecurity with AI, Says Borno's Chief Judge' <https://www.arise.tv/nigeria-can-fight-boko-haram-insecurity-with-ai-says-bornos-chief-judge/> accessed 15 May 2024.
[21] T Ajose, 'Nigeria to Deploy AI for Tackling Insecurity in 2025' (News Central, December 18, 2024) <https://newscentral.africa/nigeria-to-deploy-ai-for-tackling-insecurity-in-2025/> accessed 23 January 2025.
[22] Ibid.
[23] Ibid.
[24] Ibid.

Ministry of Communications, Innovation, and Digital Economy made Nigeria's first National Artificial Intelligence Strategy (NAIS) draft public in August 2024.[25]

However, this growing adoption of AI in national security applications presents a significant challenge: striking a balance between safeguarding a nation and protecting the privacy rights of its citizens.[26] While AI offers undeniable benefits for security, its use raises concerns about mass surveillance, potential misuse of data, and the lack of transparency in decision-making processes. The adoption of AI has introduced new risks concerning the exploitation and manipulation of Nigerian citizens' data highlighting the need for policy interventions to address issues such as algorithmic bias, privacy infringement, lack of transparency, and the challenge of educating Nigerians about their interactions with AI.[27] It is essential to recognize that decisions should not solely rely on AI assessments due to the inherent uncertainty in their predictions.[28] Therefore, Nigeria's AI policy must carefully consider the appropriate roles and limitations of AI systems, particularly in critical public sectors such as law enforcement, criminal justice, immigration, and national security.[29]

This article examines this complex tension in the context of Nigeria's national security strategy. It analyses the alluring benefits of AI in national security and its inherent challenges and risks. It also analyses the current state of legal frameworks governing AI in Nigeria, highlighting the need for a comprehensive framework for AI governance. It compares Nigeria's framework with that of the United Kingdom to draw valuable lessons for Nigeria. It proposes key recommendations for creating a robust national AI strategy in Nigeria.

[25] NCAIR and NITDA, 'National AI Strategy 2024' <https://ncair.nitda.gov.ng/wp-content/uploads/2024/08/National-AI-Strategy_01082024-copy.pdf> accessed 23 January 2025.

[26] K Srivastava, 'Artificial Intelligence and National Security: Perspective of the Global South' (2023) 2(2) *International Journal of Law in Changing World* 78.

[27] JO Effoduh, 'Towards a Rights Respecting Artificial Intelligence Policy in Nigeria' <https://paradigmhq.org/wp-content/uploads/2021/11/Towards-A-Rights-Respecting-Artificial-Intelligence-Policy-for-Nigeria.pdf> accessed 23 April 2024.

[28] Ibid.

[29] Ibid.

POTENTIAL BENEFITS OF AI IN NATIONAL SECURITY

Overall, AI offers significant benefits for national security by enhancing efficiency, productivity, and overall power in the cyber domain.[30] Incidents of cyberattacks targeting government agencies and organizations are increasing in Nigeria, as well as in other African nations and across the Middle East.[31] Thus using AI in the cyber domain can be of immense benefit to Nigeria. AI use leads to increased efficiency in cyber defence as AI can automate tasks like vulnerability scanning and system monitoring, freeing up human experts to focus on complex threats.[32] This allows for faster detection and response to cyberattacks. Secondly, it leads to enhanced productivity in cyber operations, similar to how digital surveillance tools empower fewer personnel to monitor vast amounts of data; AI can further amplify the effectiveness of cyber defence teams.[33] Cybersecurity experts in Nigeria are in high demand.[34] AI can automate routine tasks like threat detection and incident response, freeing up these experts to focus on complex cyber investigations and strategic planning. AI-powered tools can analyse massive datasets and identify patterns that can be missed by humans, leading to more targeted and efficient cyber defences.[35]

AI can analyse massive datasets of cyber threats, identifying patterns and trends that can be missed by humans.[36] A recent study identified several critical challenges facing Nigeria's intelligence agencies, including data scarcity, underutilised existing data, concerns over data quality, and fragmented data

[30] G Allen and T Chan, ‘Artificial Intelligence and National Security’ 18 <https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf> accessed 14 May 2024.

[31] T Jaiyeola, ‘Cyberattacks on Nigerian Govt Agencies Rise — Report’ <https://punchng.com/cyberattacks-on-nigerian-govt-agencies-rise-report/> accessed 13 May 2024.

[32] Allen and Chan, (n 30) 18.

[33] Ibid.

[34] G Elimian, ‘Nigeria has only 8,352 Cybersecurity Professionals as Global Demand Rises to 4 Million’ <https://leadership.ng/nigeria-has-only-8352-cybersecurity-professionals-report/> accessed 13 May 2024.

[35] Allen and Chan, (n 30) 18.

[36] G Iashvili and M Iavich, ‘Enhancing Cyber Intelligence Capabilities through Process Automation: Advantages and Opportunities’ in A Lopata *et al* *Advanced Information Networking and Applications, the 36th International Conference on Advanced Information Networking and Applications* (AINA-2022), Sydney, NSW, Australia, 13-15 April 2022, 92-101.

sharing.[37] These issues include insufficient data to understand threats comprehensively, failure to fully analyse or leverage existing information, inaccuracies or unreliability in available data, and inconsistent management practices that create silos and hinder collaboration among agencies.[38] By leveraging AI, Nigeria's intelligence system can overcome these data challenges and transform its effectiveness in safeguarding national security.

Thirdly, it results in amplified power in countering threats.[39] AI can automate tasks associated with cyber offences as well, such as reconnaissance and probing for vulnerabilities.[40] This can allow Nigerian security forces to quickly identify and exploit the weaknesses in enemy systems.[41] However, it is important to note that responsible use of AI in cyber offences is crucial to avoid escalation and unintended consequences.

THE NIGERIAN LEGAL LANDSCAPE

Black and Murray have argued that instead of building an entirely new regulatory system for AI, existing regulations can be leveraged.[42] Activities already covered by specific regulations would still be subject to those same rules even if AI were involved.[43] Existing regulatory bodies simply need to adapt their approaches to address the unique aspects of AI within their existing frameworks.[44] This can be done by developing specific norms, or guidelines, for AI within their domain. Therefore, this study analyses existing laws and regulations that might be relevant to AI applications and evaluates how these existing frameworks can be adapted to address the use of AI in these areas. It also identifies gaps where new regulations may be needed, or overlaps that need to be streamlined for clarity.

[37] OO Awotayo and others, ‘ Intelligence System and National Security in Nigeria: The Challenges of Data Gathering’ (November 2023-April 2024) 4(2) *Janus.net e-journal of International Relations* 193

[38] Ibid.

[39] Allen and Chan, (n 30) 18,

[40] Ibid.

[41] Ibid.

[42] J Black and AD Murray, ‘Regulating AI and Machine Learning: Setting the Regulatory Agenda’, [2010] 10(3) *European Journal of Law and Technology* 10.

[43] Ibid, 10,

[44] Ibid.

However, before delving into the analysis of existing laws and regulations relevant to AI applications, as well as identifying gaps and areas for improvement, it is essential to examine the AI projects Nigeria has adopted and explore other emerging technologies that hold the potential for reshaping the country's national security landscape. This contextual understanding will provide a solid foundation for assessing how the legal framework can be adapted to address these advancements effectively. Nigeria has initiated several AI projects and pilot programs within its national security sector, achieving notable successes while also encountering certain challenges. Other notable examples of AI in the context of national security in Nigeria include:

1. The Nigerian military employs drones and unmanned vehicles, such as unmanned aerial vehicles (UAVs) and tethered hexacopter UAVs, for purposes including intelligence gathering, surveillance, and executing precision strikes.[45] Examples include the Aerostar UAVs for maritime patrol and intelligence during the Niger Delta crisis, although most are now non-operational due to lack of spare parts.[46] The Nigerian Air Force (NAF) employs modern UAVs such as the Wing Loong IIs, CH-4Bs, and CH-3As, armed with missiles and guided bombs, for operations against Boko Haram and ISWAP.[47] Locally developed UAVs, including the Amebo, Gulma, and Tsaigumi, enhance self-reliance and training.[48] Additionally, the Nigerian Navy and Police use advanced systems like the Tekever AR3 and Elistair Orion for maritime and border security, integrating AI for day-and-night surveillance and operational efficiency.[49] These efforts underline Nigeria's commitment to leveraging AI technologies for strategic defence objectives.

[45] David Oliver 'Pioneering Unmanned Fleet in Sub-Saharan Africa' (*Times Aerospace*, 20 March 2024) <https://www.timesaerospace.aero/features/defence/pioneering-unmanned-fleet-in-sub-saharan-africa#:~:text=Nigeria%20is%20the%20only%20country,have%20used%20them%20in%20combat.> accessed 21 January 2025.

[46] Ibid.

[47] Ibid.

[48] Ibid.

[49] Ibid.

The use of AI-driven technologies like unmanned aerial vehicles (UAVs) for national security in Nigeria faces significant challenges, particularly in the North East. The Operation Hadin Kai Joint Task Force has banned unauthorized drone usage across Borno, Yobe, and Adamawa states due to security concerns.[50] These concerns include the proliferation of drones for domestic and commercial purposes without adherence to regulations, leading to potential misuse by non-state actors and criminal elements for subversive activities.[51] Instances of drones being used to target military installations and critical national infrastructure highlight the risks, further exacerbated by reports of unauthorized drone operations.[52] However, enforcing compliance and addressing the disregard for existing regulations by individuals and organizations continue to pose significant hurdles for the Nigerian military.

2. Nigerian Navy's Adoption of Artificial Intelligence: The Nigerian Navy is adopting artificial intelligence to enhance its operational capabilities and stay aligned with advancements in maritime technology.[53] This initiative was highlighted by Chief of the Naval Staff, Vice Adm. Emmanuel Ogalla, during a presentation by navy participants at the National Defence College.[54] Ogalla emphasized that AI and other emerging technologies are becoming integral to modern shipbuilding, making their adoption essential. Vice Admiral Emmanuel Ogalla emphasized that AI is significantly transforming the maritime industry, and the Navy is embracing it to enhance ship availability and operational effectiveness. Ogalla

[50] Abisola Adigun, ‘BREAKING: Nigerian Military Bans Drone Operation in North Eas’ (*Nigerian Tribune*, 15 January 2025) https://tribuneonlineng.com/breaking-nigerian-military-bans-drone-operation-in-north-eas/> accessed 21 January 2025.

[51] Ibid.

[52] Ibid.

[53] African Defence Forum, ‘Nigerian Navy to Harness AI’ (July 9 2024) <https://adf-magazine.com/2024/07/nigerian-navy-to-harness-ai/#:~:text=Emmanuel%20Ogalla%20made%20the%20announcement,are%20used%20in%20ship%20construction.> accessed 16 January 2025.

[54] Ibid.

made this statement during the presentation of a paper by participants of the National Defence College (NDC) Course 31, titled "Artificial Intelligence and Ship Maintenance: Strategic Options for the Nigerian Navy by 2035."[55] The integration of AI is expected to modernize the Navy's maintenance systems and provide a competitive edge in maritime operations. AI can enhance a Navy's decision-making capabilities by optimizing operations, such as identifying the most fuel-efficient methods to run a vessel.[56] It can also be integrated into navigation systems, radar functions, and threat-detection systems, enabling operators to process information more quickly and effectively.[57] The Nigerian Navy's integration of AI is anticipated to streamline maintenance processes, reduce downtime, and improve the readiness of naval assets. The Nigerian Navy's integration of AI is anticipated to streamline maintenance processes, reduce downtime, and improve the readiness of naval assets.

3. The National Centre for Artificial Intelligence and Robotics (NCAIR) established by the National Information Technology Development Agency (NITDA)[58] serves as a hub for AI, robotics, and other Fourth Industrial Revolution technologies in Nigeria and Africa. The centre focuses on research and development, skills and capacity building, technology transfer, and policy formulation.[59] By promoting the adoption of AI and robotics, NCAIR aims to contribute to national security by developing advanced technological solutions to address security challenges.[60] The centre has significantly boosted Nigeria's AI research and development capacity through upgrades, including 2,500 virtual Central

[55] Agency Reporter, 'Nigerian Navy Adopts AI to Enhance Operational Effectiveness – Ogalla' (*Nation Newspaper*, August 11 2023) <https://thenationonlineng.net/nigerian-navy-adopts-ai-to-enhance-operational-effectiveness-ogalla/> accessed 16 January 2025.

[56] African Defence Forum, (n 53).

[57] Ibid.

[58] NCAIR, <https://ncair.nitda.gov.ng/> accessed 22 January, 2025.

[59] Ibid.

[60] Ibid.

Processing Units and 1 petabyte of storage.[61] NCAIR is fostering a skilled workforce proficient in AI and related technologies, which is crucial for sustaining and advancing AI initiatives in the security sector. Despite these advancements, ensuring sufficient funding and long-term support for such initiatives remains a challenge.

Mantra, a prominent security services provider in Nigeria, is actively leveraging Artificial Intelligence (AI) to enhance national security through innovative technologies and practices.[62] The company's participation in the American Society for Industrial Security (ASIS) Chapter 206 Lagos reflects its commitment to integrating cutting-edge solutions. At the ASIS AGM, the keynote theme, *"Leveraging Artificial Intelligence for Enhanced Security in Nigeria,"* highlighted critical security challenges, including high crime rates, terrorism, and the difficulty of data collection in remote areas.[63] However, challenges persist, such as difficulties in data collection in remote areas and limited access to technology in certain regions, which hinder the full potential of AI solutions. These initiatives highlight Nigeria's progress in incorporating AI into its national security sector, with successes in improving operational efficiency and capacity building, while challenges related to funding, infrastructure, and data collection continue to be obstacles.

Building on Nigeria's adoption of various AI-driven projects to enhance national security, it is essential to explore how advanced technologies like natural language processing (NLP) and generative AI can further reshape the country's security dynamics, offering new tools and insights to address emerging threats effectively. Natural Language Processing (NLP), a subfield of AI that focuses on computer-human language interaction, offers a powerful solution for analysing the massive amounts of unstructured text generated online.[64] By employing techniques like

[61] K M Murithi, 'AI News: Nigerian Government Debuts AI Tool with Multilingual Capabilities' (*Coingape*, April 20 2024) <https://coingape.com/ai-news-nigerian-government-debuts-ai-tool-with-multilingual-capabilities/> accessed 17 January 2025.

[62] S Hawkes,'Mantra Embraces Artificial Intelligence in Security' (*Mantra Protection Solutions Limited,* November 25 2024) <https://www.mantraoperations.com/blog/2024/11/25/mantra-embraces-artificial-intelligence-in-security?utm_source=chatgpt.com> accessed 17 January 2025.

[63] Ibid.

[64] F Olaoluwa and K Potter, 'Natural Language Processing (NLP) for Social Media Threat Intelligence' *Preprints* (2024) https://doi.org/10.20944/preprints202409.0488.v1.

sentiment analysis, topic modelling, and entity recognition, NLP enables the automated processing and extraction of valuable insights from this data.[65] Sentiment analysis gauges the emotional tone of the text, topic modelling identifies recurring themes, and entity recognition extracts and categorizes key entities.[66]

In today's data-driven world, Natural Language Processing (NLP) plays a critical role in enabling machines to comprehend and analyse human language.[67] This AI-powered technology addresses the overwhelming volume of unstructured text data by enabling analysts to extract relevant information efficiently. NLP techniques, such as sentiment analysis, topic modelling and entity recognition are instrumental in identifying and mitigating threats, including the spread of misinformation and extremist propaganda.[68] Sentiment analysis gauges the emotional tone of the text, topic modelling identifies recurring themes, and entity recognition extracts and categorizes key entities.[69] For example, AI models can effectively distinguish between factual and fabricated news articles, and identify potential terrorist propaganda by analysing subtle linguistic cues. These insights can significantly enhance threat intelligence efforts. NLP can transform national security by enabling the analysis of vast amounts of text and speech data from various sources, including social media, communication channels, and intelligence reports.

Communications Minister, Bosun Tijani announced that the Nigerian Federal Government has unveiled the nation's first multilingual Large Language Model (LLM) aimed at advancing artificial intelligence (AI) capabilities.[70] This innovative AI system is designed to process and generate text in multiple languages, supporting Nigeria’s ongoing efforts to develop AI technology.[71] This multilingual LLM was introduced during a four-day AI workshop held in Abuja,

[65] Ibid.

[66] Ibid.

[67] E Blasch and others, ‘Artificial Intelligence Strategies for National Security and Safety Standards’ <https://arxiv.org/pdf/1911.05727> accessed January 21 2025.

[68] Ibid; Olaoluwa and Potter, (n 64) .

[69] Ibid.

[70] Inclusion Times, ‘Nigeria Launches First Multilingual AI-Language Model’ (April 22 2024) <https://www.inclusiontimes.com/nigeria-launches-first-multilingual-ai-language/#:~:text=The%20Federal%20Government%20has%20launched,relaunch%20in%20partnership%20with%20Cisco.> accessed 17 January 2025.

[71] Ibid.

which brought together over 120 AI professionals.[72] The model is specifically tailored to work with five low-resource languages, as well as accented English, with the goal of enhancing linguistic diversity within AI datasets.[73] The development of this model is supported by more than 7,000 fellows from the 3MTTNigeria program and has been created through collaboration between local and international technology companies.[74] These findings suggest that Nigeria's AI policy is actively evolving, with an emphasis on inclusivity, collaboration, and the enhancement of linguistic and cultural diversity in AI applications.

Generative AI offers significant potential for enhancing national security in Nigeria. Enabling advanced simulations can help predict the outcomes of various security strategies and model potential threats like cyberattacks or geopolitical conflicts.[75] However, this powerful technology also presents risks, including the potential for misuse in creating deepfakes and the spread of misinformation, which could undermine public trust and national cohesion.[76] To leverage the benefits of NLP and generative AI while mitigating these risks, Nigeria must prioritize responsible integration.[77] This requires careful consideration of ethical

[72] Ibid.

[73] Ibid.

[74] Ibid .

[75] D Appel and A Black, 'Generative AI for National Security' <https://www.thecipherbrief.com/column_article/generative-ai-for-national-security> accessed 16 January 2025.

[76] M A Joshi, 'The Security Risks of Generative Artificial Intelligence' (2024) 7(2) *International Journal on Integrated Education (IJIE)* 91-95.

[77] Justin Fanelli, the Acting Chief of Technology Officer to the United States Navy, while discussing the future of AI in the national security and defence stated that AI in national security is not about the technology, it is about measuring mission accomplishment, advantage and including divestment in the actions we take. See Caitlin Dohrman, CEO of Tangram Flex, Mihai Filip, CEO of Oves Enterprises, and Sean Moriarty, CEO of Primer AI discuss the future of AI in the national security and defense sector. 'Putting AI to work for National Security' Atlantic Council, 14 November 2024, Washington DC https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqbGRCTmt6c0J1Z2d6WEhmSU5DUURmSkkxaHBQQXxBQ3Jtc0tteFZQMXNZQ2pfSU10bUZZc2ZYb0kybUc5LXJTYUFtUXVZUm9XU2lYeEIwMTVTSXdpM2dwWk5TU0Z2Qy1tRUdxbFIwSHV5TUdudGRFWVNLbmtYbWVvQ3FDc2hOTS1WUlkwYnd2bHVpcHl5bDFqWGFTcw&q=https%3A%2F%2Fwww.atlanticcouncil.org%2Fevent%2Fputting-ai-to-work-for-national-security%2F&v=dXs7tQiGQaI accessed 9 May 2023.

implications, robust oversight mechanisms, and a proactive approach to addressing potential misuse.

The proliferation of private actors and nascent enterprises engaged in Artificial Intelligence research and development within Nigeria underscores the nation's preparedness to integrate AI-powered advancements.[78] The state itself has demonstrated its commitment to advancing AI technology through the establishment of the National Centre for AI and Robotics (NCAIR).[79] Presently, Nigeria lacks dedicated legislation specifically targeting AI, there are, however, existing general and sector-specific laws applicable to their operations within the country.

As mentioned earlier, there is the draft National AI strategy released in August 2024. Babalola's critique of Nigeria's draft National AI Strategy highlights significant shortcomings that have implications for AI deployment in national security.[80] Babalola observed that the document lacks a clearly defined purpose and fails to outline resource allocation plans, which are essential for effective implementation.[81] Furthermore, it provides insufficient attention to privacy and data protection, mentioning "human rights" only sparingly and omitting critical references to the Nigerian Constitution.[82] The author argues that despite proposing ethical principles, the document omits enforceable privacy protections and fails to integrate these principles into actionable strategies, raising concerns about the ethical deployment of AI.[83] Additionally, the proposal to establish a new AI governance body is problematic, given the existing underfunding of the Nigeria

[78] J Uba, 'Nigeria: Artificial Intelligence (AI) Regulation In Nigeria: Key Considerations, Recommendations, Legal Framework, And Policy Development For Artificial Intelligence (AI) In Nigeria' <https://www.mondaq.com/nigeria/new-technology/1373830/artificial-intelligence-ai-regulation-in-nigeria-key-considerations-recommendations-legal-framework-and-policy-development-for-artificial-intelligence-ai-in-nigeria> accessed 9 May 2023.

[79] Ibid.

[80] O Babalola, 'The (Draft) National Artificial Intelligence (AI) Strategy: A Diminution of Privacy and Data Protection?' (*Itedgenews,* 7 August 2024) <https://www.itedgenews.africa/the-draft-national-artificial-intelligence-ai-strategy-a-diminution-of-privacy-and-data-protection/#:~:text=By%20Olumide%20Babalola.%20On%20the%203rd%20day,make%20'input'%20and%20'further%20dissect%20its%20contents.'.> accessed 23 January 2025.

[81] Ibid.

[82] Ibid.

[83] Ibid.

Data Protection Commission (NDPC) and the availability of agencies like the National Centre for AI and Robotics (NCAIR), which could be empowered to avoid unnecessary financial strain.[84] These deficiencies could lead to operational inefficiencies, ethical risks, and public distrust, ultimately hindering the deployment of AI technologies for national security. To address these gaps, the strategy must clearly define its objectives, strengthen its commitment to privacy and data protection, align with existing frameworks like the NDPA, and propose practical, resource-efficient solutions for governance and implementation.

A crucial aspect of utilising AI lies in data privacy and AI algorithms require vast datasets for training to ensure accurate outputs.[85] Nigeria adopted a data protection law in 2023, the Nigeria Data Protection Act 2023 that has some notable provisions.[86] The establishment of the Nigerian Data Protection Commission is worth mentioning, a provision relating to the priority of the Act over all other sector-specific legislation on data privacy in Nigeria. [87] The Act also establishes enforcement and accountability methods, including penalties for non-compliance.[88]

However, concerning AI, the Act does not specifically address AI-related data terms like ‘data mining,’ ‘anonymisation,’ or ‘models.’ However, it does cover crucial aspects pertinent to the advancement of AI, such as ensuring data security and regulating data transfer across borders.[89] The Nigeria Data Protection Act 2023 includes provisions that directly and indirectly affect various aspects of AI utilisation in the country. For example, the requirement for a Data Protection Officer (DPO) can indirectly affect AI by creating an additional layer of bureaucracy and potentially slowing down development processes.[90] The right to rectify personal data allows individuals to control the information used by AI

[84] Ibid.

[85] S Timi-Koleolu and O Atanda, ‘Artificial Intelligence In Nigeria: Legal and Regulatory Guidance’ <https://pavestoneslegal.com/newsletters/ > accessed 9 May 2023.

[86] For example, the provision for legitimate interest assessment s 23(1), Nigeria Data Protection Act 2023 Federal Republic of Nigeria Official Gazette No.119 Vol. 110 (1 July 2023).

[87] Ibid, s 4 and 63.

[88] Ibid, pt X.

[89] Ibid, s 39-43.

[90] Ibid, s 32.

systems.[91] To an extent, the information security measures mandated by the Nigeria Data Protection Act 2023 protect personal data from unauthorised access or misuse.[92] The requirement for clear communication about data use can compel developers to be more transparent about how AI algorithms work.[93] Overall, the Nigeria Data Protection Act 2023 promotes the development of AI that respects human rights by fostering transparency, accountability, and individual control over data. This can help mitigate potential risks associated with AI, such as algorithmic bias and discrimination.

There is also the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 which aims to provide an effective and comprehensive legal, regulatory, and institutional framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes in Nigeria.[94] In addition, the Act aims to guarantee the protection of critical national information infrastructure, promote cyber security and protect electronic communications, data and computer programs, intellectual property, and privacy rights.[95]

This study submits that the emergence of AI presents significant challenges to upholding the rule of law, protecting fundamental rights, and maintaining the integrity of Nigeria's national security framework. These challenges are amplified when considering the potential integration of AI-based decision-making tools within the realm of national security. Preserving the core principles of the rule of law, which are grounded in fundamental rights, remains paramount and cannot be compromised for the sake of expediency or cost-effectiveness within the legal framework and its beneficiaries. Therefore effectively navigating this transformative landscape requires the enactment of precise guidelines and regulations, along with a setting well-defined role for AI systems within Nigeria's national security apparatus. In other words, Nigeria needs clear rules for how to use AI safely and fairly in national security. Uba argues that when drafting a comprehensive AI policy, Nigerian authorities and relevant stakeholders should

[91] Ibid, s 34.
[92] Ibid, s 39.
[93] Ibid, s 27.
[94] Cybercrimes Act 2015, s.1 (a).
[95] Ibid.

consider the most effective means to uphold citizens' human rights while fostering an AI-powered economy that follows best practices.[96] These guidelines include ensuring algorithmic accountability, protecting data, maintaining transparency in decision-making based on machine learning, and more.[97] This paper submits that by prioritising these considerations, Nigeria can effectively harness the benefits of AI in enhancing national security while upholding fundamental rights and ethical standards.

There is no national policy on AI deployment for national security purposes in Nigeria. However, it is commendable that Nigeria was the first in Africa to establish a national centre for artificial intelligence.[98] Nigeria currently has seven governmental ministries, departments, and agencies tasked with promoting or overseeing the application of AI within the country.[99] There is a significant shift in how governments are approaching national security in the age of Artificial Intelligence (AI). Traditionally, data privacy, cybersecurity, and national security were seen as separate issues.[100] Now, governments realize that these issues are interconnected, especially when dealing with AI. This new approach aims to develop regulations that protect both privacy and national security from the risks posed by AI in the hands of foreign adversaries.[101] Traditional threats like physical attacks are joined by cyberwarfare, information warfare, and manipulation of public opinion ("soft war") due to rapid advancements in AI.[102] Therefore, strong data privacy laws and information security measures are vital to protect sensitive

[96] Uba (n 78).
[97] Ibid.
[98] Effoduh, (n 27).
[99] These include: the Federal Ministry of Communications and Digital Economy, Federal Ministry of Science, Technology, and Innovation, National Information Technology Development Agency, National Office for Technology Acquisition and Promotion, Nigerian Communications Commission, Securities and Exchange Commission and the Corporate Affairs Commission.
[100] Swire P and Sacks S, 'Limiting Data Broker Sales in the Name of U.S. National Security: Questions on Substance and Messaging' https://www.lawfaremedia.org/article/limiting-data-broker-sales-in-the-name-of-u.s.- national-security-questions-on-substance-and-messaging [https://perma.cc/UA98-94Q2 on 15 May 2024, M Hu, E Behar D and Ottenheimer, 'National Security and Federalizing Data Privacy Infrastructure for AI Governance' (2024) 92(5) *Fordharm Law Review* 1831.
[101] Hu, Behar and Ottenheimer, (n 100) 1831.
[102] Ibid.

information and prevent its exploitation.[103] This is a key foundation for any effective national security strategy.[104] Therefore, regulations are necessary to ensure responsible development and use of AI. The European Union's AI Act and China's AI regulations are examples of attempts to govern the development and use of AI.[105] It has been argued that there is a need to consider the national security implications of AI governance alongside the focus on protecting individual rights from AI's potential harms.[106] Data privacy, cybersecurity, and national security are no longer separate issues. They are interconnected, especially when dealing with AI. This study submits that Nigeria should develop a comprehensive strategy that addresses all three aspects. There is a need to balance national security concerns with protecting individual rights from the potential harms of AI. Striking this balance is crucial for effective AI governance in Nigeria.

CHALLENGES AND RISKS OF AI USE IN NATIONAL SECURITY IN NIGERIA

Considering the evident advantages for military operations through enhanced automation and the highly adaptable civilian applications of AI, outright prohibitions on autonomous weapon systems, robotics, and unmanned vehicles seem untenable from legal, policy, and operational perspectives.[107] States that are in the process of developing new weapons have the responsibility to engage in a continuous review process, starting from the initial conception and design phase, progressing through technological development and prototyping, and culminating in production and deployment.[108] Indeed, AI stands as a profoundly potent

[103] Ibid.
[104] Ibid.
[105] EU ‘Artificial Intelligence Act Final Draft (2024)’ https://artificialintelligenceact.eu/the-act/ on 15 May 2024 The EU AI Act is a proposed regulation by the EU to establish uniform rules for using AI. For details on China’s AI regulations see, Sheehan M, ‘Tracing the Roots of China’s AI Regulations’ <https://carnegieendowment.org/2024/02/27/tracing-roots-of-china-s-ai-regulations-pub-91815> accessed 15 May 2024.
[106] Hu, Behar and Ottenheimer, (n 100) 1832.
[106] Ibid.
[107] MN Schmitt and JS Thurnher, ‘’Out of the Loop’: Autonomous Weapons Systems and the Law of Armed Conflict’ (2013) 4 *Harvard National Security Journal* 233.
[108] International Committee of the Red Cross (ICRC), A Guide to the Legal Review of New Weapons, Means and Methods of Warfare (2006) 23

technology, yet it comes with its own set of obstacles.[109] When not used judiciously and accompanied by suitable protections, this technology may have adverse effects on civil liberties and human rights.[110]

While AI holds promise for various military applications, it also presents unique challenges that demand swift responses.[111] For instance, AI for national security can be powerful, but it often relies on collecting and analysing vast amounts of personal data.[112] Some have raised concerns that AI-powered surveillance systems can facilitate the unobtrusive invasion of individual privacy, without obtaining informed consent or providing transparency about data collection practices.[113] Some have argued that AI has the potential to significantly improve data privacy and security, but it is important to address the ethical challenges involved.[114] The successful implementation of an AI strategy hinges on achieving an appropriate balance between data privacy, security, and innovation.[115] This requires meticulous evaluation and well-considered choices.[116] Below are some of the challenges of AI deployment for national security in Nigeria:

1. Uncertainty of AI's Impact on Nigeria's National Security: Nsude lists the potential dangers of AI in warfare in Nigeria. Firstly, AI could make it easier for insurgent groups to develop and deploy weapons, potentially giving them an advantage over traditional military forces.[117] The author submits that the terrorists in Nigeria seem to have access to modern weapons of

https://www.icrc.org/en/doc/assets/files/other/icrc_002_0902.pdf on 13 May 2024, Afsah , (n 13) 461.

[109] I Nsude, 'Artificial Intelligence (AI), The Media And Security Challenges in Nigeria' (2022) 11 *Communication, technologies et développement* 11.

[110] Ibid.

[111] Ibid.

[112] S D Devineni, 'AI in Data Privacy and Security' [2024] *International Journal of Artificial Intelligence and Machine Learning* 44.

[113] S H Park, 'Ethics for Artificial Intelligence: Focus on the Use of Radiology Images' [2022] 83(4) *Journal of the Korean Society of Radiology* DOI: 10.3348/jksr.2022.0036.

[114] Ibid, 38.

[115] Devineni, (n 112) 44.

[116] Ibid.

[117] Nsude (n 109) 11.

warfare.[118] It has been argued that the effectiveness of applying artificial intelligence in Nigeria's fight against Boko Haram and Herdsmen is not solely determined by its deployment but by which side—government or insurgent—adopts it first.[119] This is because it is arguable that advancements in information technology could decrease insurgent attacks by aiding states in gathering intelligence, or conversely, increase attacks by facilitating better coordination among insurgents.[120] If the primary concern becomes insurgent use of AI, development efforts might prioritize offensive capabilities over defensive ones. This could lead to an arms race where both sides develop increasingly sophisticated AI weapons, escalating tensions.[121]

2. Poor Data Infrastructure: Artificial Intelligence (AI) relies on the availability of high-quality, well-structured data to function effectively.[122] However, Nigeria faces significant challenges due to its fragmented and often outdated data systems.[123] Other issues include a lack of robust data infrastructure, privacy concerns, and limited data collection capabilities, hindering the training and effectiveness of AI in various sectors. Studies reveal Nigeria's data and statistical systems are fragmented, suboptimal, poorly coordinated, and largely ineffective.[124] They fail to meet the needs of policymakers, business investors,

[118] Ibid

[119] Ibid

[120] Ibid

[121] KF Maisha, 'AI & Arms Race: The Rivalry Between the U.S. & China in the Field of Tech Supremacy' (BIPSS Commentary) <https://bipss.org.bd/pdf/AI%20&%20Arms%20Race%20The%20Rivalry%20Between%20the%20U.S.%20&.pdf> accessed 13 May 2024.

[122] O Baruwa, 'Nigeria: Is Nigeria Ready for Artificial Intelligence (Ai)?' (*allafrica,* 9 October 2024) <https://allafrica.com/stories/202410100476.html#:~:text=AI%20thrives%20on%20high%2Dquality,currently%20lack%20sufficient%20data%20infrastructure> accessed 23 January 2025.

[123] Ibid.

[124] OE Olubusoye, GO Korter, and O Keshinro, ' Nigerian Statistical System: the Evolution, Progress and Challenges' <http://doi/10.13140/RG.2.1.3136.4569> accessed 22 January 2025.

.and citizens. This deficiency poses significant challenges for deploying AI in national security, as the effectiveness of AI systems depends on reliable, accurate, and well-structured data. Without a robust data infrastructure, the potential of AI to enhance national security initiatives may remain unrealised, limiting its ability to provide actionable insights or support critical decision-making processes. Limited internet access and digital infrastructure, particularly in rural areas, further restrict data collection and the equitable deployment of AI solutions.[125] Additionally, evolving policies on data privacy and governance remain insufficient to address concerns around security, ethics, and accountability in AI systems. The shortage of skilled AI professionals and data scientists further exacerbates these challenges, hindering the country's ability to implement AI technologies effectively. Addressing these barriers is crucial for Nigeria to harness the transformative potential of AI across various sectors, including national security.

3. Resource Constraints: Nigeria faces financial and technological limitations and infrastructural deficits in building robust AI systems.[126] Governments require significant institutional capacities, such as skilled personnel and financial resources, to govern AI effectively.[127] Budgetary constraints often prioritise

[125] A study investigates the cause of digital divide in Nigeria: O F Oluda and C G Josephs, 'The Causes of Digital Divide in Nigeria: The Context of the Nigerian Law Reform Commission' Master Thesis, Lund University School of Economics and Management 2023, <https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9123699&fileOId=9123921> accessed 23 January 2025.

[126] Chibuzo Charles Nwosu and others, 'Artificial Intelligence in Public Service and Governance in Nigeria' (2024) 4(2) *Journal of Governance and Accountability Studies,* 116; Tonye Al-Onyanabo, 'Harnessing AI for Financial Inclusion in Nigeria: Opportunities and Challenges' (2024) <://www.researchgate.net/publication/381161690_Title_Page_Title_Harnessing_AI_for_Financial_Inclusion_in_Nigeria_Opportunities_and_Challenges> accessed 16 January 2025.

[127] MR Martins, 'From On-Premise to Cloud: Evolving IT Infrastructure for the AI Age' (2023) 20(03), *World Journal of Advanced Research and Reviews,* 1898-1934; Jenny Lyons-Cunha, 'What is AI Infrastructure?' (11 December 2024) <https://builtin.com/artificial-intelligence/ai-infrastructure> accessed 16 January 2024; Emmanuel Ogiemwonyi Arakpogun and others

immediate security needs over long-term investments in AI. To overcome these challenges, Nigeria can foster partnerships with private sectors, international organisations, and AI-focused start-ups to pool resources and share costs. The Samyukta Electronic Warfare System is a prominent example of collaboration between India's Defence Research and Development Organisation (DRDO) and Tata Power Strategic Engineering Division (SED).[128] This integrated mobile electronic warfare system was jointly developed by DRDO, Bharat Electronics Limited, Electronics Corporation of India Limited, and the Indian Army's Corps of Signals to support tactical battlefield operations.[129] Tata Power SED played a significant role in the development of the Command and Control Software for the Samyukta system, contributing to its capabilities in surveillance, analysis, interception, direction finding, and position fixing, prioritizing, and jamming of communication and radar signals from HF to MMW frequencies.[130] Another avenue for addressing resource constraints lies in regional collaboration. Establishing cost-sharing agreements with neighbouring countries can facilitate the development of shared AI infrastructure, such as data centres and research hubs, for security purposes. The African Union's Continental AI Strategy provides a framework for

'Artificial Intelligence in Africa: Challenges and Opportunities' <https://researchportal.northumbria.ac.uk/ws/portalfiles/portal/31309999/AI_in_Africa_Opportunities_and_Challenges_Paper_68_Manuscript.pdf> accessed 16 January 2025.

[128] Defence Research and Development Organisation 'Programme Samyukta' <https://www.drdo.gov.in/drdo/programme-samyukta>

[129] The system's capabilities include Electronic Intelligence (ELINT), Communications Intelligence (COMINT), and electronic countermeasures (ECM), enabling activities such as signal interception, analysis, direction finding, and jamming. The system operates on 145 ground mobile vehicles, covering an area of 150 km by 70 km, enhancing the Indian Army's electronic warfare capabilities. See Indian Defence Analysis, 'Himshakti: India's Most Lethal Electronic Warfare System' <https://indiandefenseanalysis.wordpress.com/2023/03/25/himshakti-indian-armys-most-lethal-electronic-warfare-system/> accessed 16 January 2024.

[130] Ibid.

regional cooperation to harness AI's transformative potential while addressing ethical, legal, and societal challenges.[131] The strategy emphasizes the development of shared AI infrastructure, such as data centres and research hubs, and prioritizes collaboration among member states to stimulate investment, build capabilities, and foster innovation.[132] By pooling resources and aligning efforts, AU member countries can collectively address critical issues, including national and regional security, through scalable and inclusive AI solutions.[133] This approach underscores the importance of a unified effort in leveraging AI to strengthen security frameworks across Africa. It focuses on key areas such as building AI capabilities, minimizing risks, stimulating investment, and fostering regional cooperation. In the context of national security, this strategy highlights the importance of pooling resources through regional partnerships to develop shared AI infrastructure, such as data centres and research hubs.[134] These facilities can support AI-driven solutions to address security challenges across multiple countries, promoting collaborative frameworks and leveraging Africa's young, tech-savvy population for sustainable and secure growth.[135] Nigeria can leverage the African Union's Continental AI Strategy by collaborating with regional partners to establish shared AI infrastructure, such as data centres and research hubs, for addressing security challenges. By aligning with the strategy, Nigeria can attract funding, build local AI expertise, and utilise its young, tech-savvy population to drive AI-driven national security solutions. The Federal Ministry of

[131] African Union, 'Continental Artificial Intelligence Strategy: Harnessing AI for Africa's Development and Prosperity' (July 2024) <https://au.int/sites/default/files/documents/44004-doc-EN-_Continental_AI_Strategy_July_2024.pdf> accessed 17 January 2024.
[132] Ibid.
[133] Ibid.
[134] Ibid.
[135] Ibid.

Communications, Innovation, and Digital Economy’s partnership with Google.org, which provided a ₦2.8 billion grant to Data Science Nigeria, illustrates the importance of nurturing AI expertise.[136] A positive implication of this is that a larger pool of Nigerians with AI skills can strengthen Nigeria's ability to develop and implement AI-based security solutions. In conclusion, addressing resource constraints requires Nigeria to embrace collaboration at both national and regional levels, leverage existing frameworks, and invest in its human capital. By adopting these strategies, Nigeria can overcome financial and technological barriers and harness AI's transformative potential to bolster national security and drive sustainable development.

4. Lack of Expertise: A study published notes that Nigerian policymakers and decision-makers often lack awareness and understanding of AI's potential in the security sector, hindering its integration into existing systems.[137] The same study highlights that Nigeria faces a shortage of skilled AI professionals, stressing the need for expertise in machine learning, data analysis, and cybersecurity to implement AI solutions effectively for national security.[138] This gap affects both the quality and reliability of AI applications in national security. To address the shortage of AI expertise and awareness for national security in Nigeria, the country can implement several strategies. These include initiating training programs in partnership with local universities and global tech firms, fostering public-private collaborations with companies like

[136] Federal Ministry of Communication, Innovation, and Digital Economy, ‘Ministry Announce N2.8billion Google Support to Advance AI Talent Development in Nigeria’ (October 31 2024) <https://fmcide.gov.ng/ministry-announce-n2-8billion-google-support-to-advance-ai-talent-development-in-nigeria/> accessed 17 January 2025.

[137] Musa Zakari, Implication of Artificial Intelligence on National Security for the Nigerian Security Agencies’ (2024) 6(1) *Journal of Terrorism Studies,* 11.

[138] Ibid.

Google and Microsoft, and organizing workshops to raise AI awareness among policymakers. Additionally, Nigeria should invest in AI research and development, possibly by collaborating with regional and international partners, and support the establishment of shared AI infrastructure through regional cooperation. Nigeria can take a cue from Kenya. Kenya's National AI Strategy 2025-2030 aims to position the country as Africa's leading AI innovation hub by focusing on sustainable development, economic growth, and social inclusion.[139] The strategy highlights the importance of building AI digital infrastructure, developing a robust data ecosystem, and fostering AI research and innovation tailored to Kenya's unique needs.[140] It places a strong emphasis on creating a talent pipeline by collaborating with educational institutions and the private sector to cultivate a skilled workforce, ensuring Kenya has the experts needed to drive AI adoption and innovation. The strategy outlines key enablers such as governance frameworks, investment mobilization, and ethical AI practices, all crucial to achieving these ambitious goals.[141] By focusing on the development of skilled AI professionals, Kenya is taking significant steps to leverage AI for sectors including security, further enhancing its role as a leader in Africa's AI revolution.

5. AI-powered tools for creating deepfakes (realistic forgeries) could erode trust in institutions and media.[142] Deepfakes are a

[139] ITedgenews, 'Kenya Unveils National AI Strategy 2025-2030, Aiming to Lead Africa's AI Revolution' <https://www.itedgenews.africa/kenya-unveils-national-ai-strategy-2025-2030-aiming-to-lead-africas-ai-revolution/#:~:text=AI%20revolution%20%2D%20ITEdgeNews-,Kenya%20unveils%20National%20AI%20Strategy%202025%2D2030%2C%20aiming,to%20lead%20Africa's%20AI%20revolution&text=Kenya's%20Ministry%20of%20ICT%20and,AI)%20Strategy%202025%2D2030.> accessed 17 January 2025.

[140] Ibid.

[141] Ibid.

[142] R Chesney and D Citron, 'Deepfakes: A Looming Crisis for National Security, Democracy and Privacy?' *(Lawfare,* Wednesday, February 2018), <https://www.house.mn.gov/comm/docs/d9e1f352-ce1b-46d1-b4e3-2807437b571e.pdf> accessed 15 May 2024.

form of synthetic media, generated by AI-powered or closely related digital tools, which diverge from capturing reality and instead rely on training data. [143] Deepfakes can significantly affect Nigeria's national security efforts when combined with AI use. It can create fake news and propaganda targeting government officials, security forces, or ethnic groups.[144] This can sow discord, incite violence, and undermine public trust in legitimate institutions. Deepfakes depicting fabricated events or statements from leaders can create confusion and demoralize the population.[145] This can make it harder for the government to maintain order and combat threats. Deepfakes can create fake social media profiles or manipulate existing ones to gather intelligence or spread misinformation.[146] This can complicate efforts by Nigerian security forces to identify legitimate threats. Deepfakes have the potential to portray security operations in a negative light, discouraging cooperation from the public. This can make it harder for security forces to gather information and apprehend criminals.

6. Errors or biases in AI algorithms used for intelligence gathering or decision-making could lead to misinterpretations of threats or faulty military actions.[147] AI algorithms are prone to biases, theft, and manipulation, particularly when the training dataset lacks proper curation or protection. [148] For instance, researchers have found racial biases in AI facial recognition systems due to limited diversity in training images, and gender biases in some

[143] I Kalpokas and J Kalpokiene, *Deepfakes: A Realistic Assessment of Potentials, Risks and Policy Regulation* (Springer, 2022) 1.

[144] K M Sayler and L A Harris, 'Deepfakes and National Security' <https://apps.dtic.mil/sti/pdfs/AD1117081.pdf> accessed n 13 May 2024.

[145] Ibid.

[146] Ibid.

[147] Ibid.

[148] D S Hoadley and K M Sayler, 'Artificial Intelligence and National Security' <https://apps.dtic.mil/sti/trecms/pdf/AD1107549.pdf > accessed 13 May 2024.

natural language processing programs.[149] These issues could have significant implications for AI applications in the military, especially if biases are undetected and are incorporated into systems with lethal consequences.[150] Some argue that predictive policing which relies on data-driven analysis to allocate law enforcement resources based on predictions of future crimes, including the identification of potential perpetrators, victims, or target locations should not be employed in Nigeria as a substitute for community involvement and comprehensive crime prevention strategies.[151] The reason is that using past and present crime data, which may include social media content and communication records, can result in biases related to race, ethnicity, and discrimination.[152] Additionally, some opine that any AI system intended to profile Nigerians or designate individuals as potential perpetrators of terrorist activities, or to flag individuals based on their travel history or religious beliefs, could be prejudicial and undermine the constitutional principle of the presumption of innocence.[153] This study submits that while concerns about bias and discrimination in predictive policing are valid, completely rejecting it might overlook potential benefits. However, studies have not conclusively proven a decrease in crime due to predictive policing.[154] Nigeria may consider investing in building trust and collaboration between law enforcement and communities. This can improve information sharing, leading to more effective crime prevention and solving.

[149] Ibid.

[150] Ibid.

[151] Effoduh (n 27) 10.

[152] Ibid.

[153] Ibid.

[154] A Meijer and M Wessels, 'Predictive Policing: Review of Benefits and Drawbacks' (2019) 42(1) *International Journal of Public Administration* 1-9.

7. Accountability Gap: Current legal systems struggle to hold AI accountable for its actions because they are designed for humans and companies with human decision-makers.[155] Nigeria faces similar challenges. The issue is whether AI can ever be truly liable for its own decisions, this issue becomes even more complex when AI systems communicate and coordinate decisions, making it difficult to pinpoint who is responsible (e.g., algorithmic collusion)[156]. While most AI currently relies on human input, there is anticipation of an increase in autonomous AI systems, like care robots.[157] This raises new questions about legal liability. A looming challenge for legal systems is apparent: how to hold AI accountable for its actions in a fair and effective way.[158] Some argue that the accountability gap for AI can be a significant issue, requiring new legal solutions, but it is not always insurmountable.[159] Courts can sometimes address minor accountability gaps by creatively interpreting existing laws.[160] For example, courts in Nigeria could creatively interpret laws related to data privacy (Nigeria Data Protection Act 2023) and cybersecurity (Cybercrimes Act 2015) to address some AI-related issues. Some acknowledge that gaps that are more significant exist.[161] Simply stretching existing laws to cover AI would not work.[162] It would be a doctrinal overreach (trying to apply a law beyond its intended scope) and lead to bad legal outcomes.[163] Legal systems need to be prepared for significant changes to hold AI

[155] K Heine and A Quintavalla, 'Bridging the Accountability Gap of Artificial Intelligence – What can be Learned from Roman law?' (2024) 44 *Legal Studies* 66.
[156] Ibid.
[157] Ibid, 66.
[158] Ibid.
[159] Ibid.
[160] Ibid.
[161] Ibid.
[162] Ibid.
[163] Ibid.

accountable.[164] While there might be ways to adapt existing laws for minor issues, substantial challenges require entirely new legal tools and approaches.[165] Nigeria could develop regulations that address issues like algorithmic bias, data privacy for AI applications, and clear guidelines for AI use in national security. The Nigerian legal system can adapt and introduce new solutions as new challenges arise. It has been argued that Roman law offers a blueprint for creating a legal framework for AI.[166] This could serve as a model for creating a legal framework for AI in Nigeria. Thus, a system can be designed with:

a. Differentiated Liability: The extent of an AI owner's liability would depend on the level of autonomy granted to the AI (similar to praepositio & iussum).

b. Limited Liability Schemes: A "digital peculium" can be established to limit the owner's liability for the AI's actions.

This study submits that overall, the potential dangers of AI in warfare can create a cautious environment for AI deployment in Nigeria. This could lead to missed opportunities for utilising AI for defensive purposes and improving national security.

OVERSIGHT OVER DEPLOYMENT OF AI FOR NATIONAL SECURITY IN NIGERIA

Oversight regarding the deployment of AI for national security purposes is crucial. This involves monitoring adherence to established AI security standards through routine audits and assessments, as well as implementing certification procedures for AI systems and components.[167] This ensures that they meet safety and security criteria before being deployed. While Nigerian law mandates warrants for

[164] Ibid.
[165] Ibid.
[166] Ibid.
[167] C Yu, 'AI as Critical Infrastructure: Safeguarding National Security in the Age of Artificial Intelligence' <https://osf.io/preprints/osf/u4kdq> accessed15 May 2024.

processing personal data in national security cases, the legal framework lacks clear guidelines for courts to assess such warrant requests.[168] This creates an opaque system with inadequate judicial and legislative oversight of intelligence activities. For instance, judicial oversight is limited to the initial stages of surveillance, and there is no requirement for public reports on intelligence agency activities or oversight body actions.[169] These shortcomings are particularly concerning in the context of AI-powered surveillance in Nigeria. AI algorithms can analyse vast amounts of data to identify patterns and predict behaviour, raising significant privacy concerns. Without clear oversight mechanisms, the use of AI in national security could lead to discriminatory profiling, biased decision-making, and potential violations of civil liberties.

A common approach to oversight of AI is to employ human oversight, however, a study has shown that the assumption that humans can effectively oversee these algorithms is questionable and evidence suggests humans may not be able to understand or analyse complex algorithms properly.[170] There have been proposals for a shift from human oversight to institutional oversight.[171] This would involve the justification stage, where government agencies need to prove the algorithm is necessary and that any oversight methods are effective.[172] It also includes the democratic review stage, where public approval should be required before implementing the algorithm with oversight.[173] Currently, Nigeria lacks an oversight authority for AI national security systems. This is worrisome, especially considering the functions of an oversight authority, which include:[174]

[168] Cybercrimes Act 2015, s 39, Terrorism (Prevention and Prohibition) Act Federal Republic of Nigeria Official Gazette No.91 Vol. 109 (16 May 2022), s 68; the Lawful Interception of Communications Regulations 2019 Federal Republic of Nigeria Official Gazette No.12 Vol.106 (23 January 2019), regs 12 and 13, among others.

[169] Lawful Interception of Communications Regulations 2019, reg 13.

[170] B Green, 'The Flaws of Policies Requiring Human Oversight of Government Algorithms' (2022) *Computer Law & Security Review* 1.

[171] Ibid.

[172] Ibid.

[173] Ibid.

[174] F Patel and PC Tommey, 'An Oversight Model for AI in National Security: The Privacy and Civil Liberties Oversight Board' <https://www.brennancenter.org/our-work/analysis-opinion/oversight-model-ai-national-security-privacy-and-civil-liberties> accessed 20 May 2024.

1. Reviewing national security systems and this includes everything from domestic intelligence programs to autonomous weapons systems.
2. Ensuring compliance with legal and ethical standards, which includes making sure AI use follows privacy, civil rights, and civil liberties guidelines
3. Identifying and mitigating risks: This includes assessing the potential for bias, and algorithmic errors, and ensuring proper data security.
4. Recommending a course of action: The oversight body should be able to suggest stopping the use of a system if the risks outweigh the benefits.
5. Providing transparency and accountability: The public must be informed about the use of AI in national security and the oversight body should work to declassify information where possible.
6. Staying informed of evolving technologies

Such a body must be independent of the agencies being overseen and have sufficient resources to carry out its work effectively.

INTERNATIONAL COMPARISONS

This study compares the United Kingdom with Nigeria, exploring their approaches to AI in national security and highlighting key strengths and weaknesses. While both Nigeria and the UK recognise the potential of Artificial Intelligence (AI) to bolster national security, their approaches and challenges, differ due to varying levels of development and policy frameworks.

Overall, Nigeria can learn from the UK's approach by focusing on adapting and strengthening existing regulatory frameworks to address the challenges and opportunities presented by AI. This can provide a more efficient and effective path for fostering responsible AI development and ensuring public trust. Research shows AI has significant potential to streamline current processes within the UK's national security apparatus, leading to both faster and more impactful results.[175]

[175] A Babuta, M O Oswald and A Janjeva, 'Artificial Intelligence and UK National Security Policy Considerations' (*RUSI Occasional Paper*, April 2020) <https://static.rusi.org/ai-national-security-final-web-version.pdf> accessed 14 May 2024.

The UK intelligence agencies' legal responsibilities are outlined in the Security Service Act of 1989 for the Security Service and the Intelligence Services Act of 1994 for the Secret Intelligence Service and GCHQ.

These laws limit their authority to collect and share information to what is necessary for their operations. Regarding digital investigative powers, such as intercepting communications and accessing data, the Investigatory Powers Act of 2016, (IPA) provides the primary framework.[176] Under the Investigatory Powers Act 2016, the agencies are subject to a large level of scrutiny and oversight. Section 2 of the Investigatory Powers Act 2016 emphasizes the importance of privacy, requiring authorities to explore less intrusive methods before resorting to more invasive measures. Surveillance activities and the use of covert human intelligence sources are governed by the Regulation of Investigatory Powers Act of 2000.[177] The Human Rights Act 1998, which adopts the principles of the European Convention on Human Rights (ECHR) into UK law, safeguards essential human rights and political liberties with certain limitations.[178]

Under Article 8 of the right to privacy can only be restricted on the condition that it is lawful and deemed necessary in a democratic society.[179] On the other hand, the state has obligations under the ECHR to prevent risks to individuals or society, requiring it to take reasonable measures within its powers to do so.[180] The Investigatory Powers Act 2016 reinforced the already-existing safeguards that applied to the use of investigatory powers by introducing ground-breaking oversight systems.[181] It gave these powers a clear legal basis and, ensured that they

[176] The UK Investigatory Powers Act 2016 (IPA 2016) available at <https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted/data.htm> accessed 13 May 2024,

[177] The Regulation of Investigatory Powers Act 2000, available at <http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf> accessed 13 May 2024.

[178] United Kingdom: Human Rights Act 1998, 9 November 1998, <https://www.refworld.org/legal/legislation/natlegbod/1998/en/48641> accessed 14 May 2024.

[179] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, ETS 5, 4 November 1950, <https://www.refworld.org/legal/agreements/coe/1950/en/18688> accessed May 2024.

[180] European Convention on Human Right, art 2 and 3.

[181] Gov. UK, 'Explanatory Framework for Adequacy Discussions Section H: National Security Data Protection and Investigatory Powers Framework' 18

are only used when necessary for a legitimate purpose and in a manner that is proportionate to that purpose.[182] This test of necessity and proportionality offers national security agencies a set of criteria to evaluate the validity of implementing new technologies, including AI.[183] Under Regulation 7(3) of Nigeria's Lawful Interception of Communications Regulation 2019, a warrant is required to intercept communications in cases involving national security, crime prevention or investigation, the protection of Nigerians' economic well-being, public emergency or safety, or compliance with international mutual assistance agreements.

This paper submits that the Lawful Interception of Communications Regulations 2019 provisions outlined offer some level of protection, but they do not fully match the comprehensiveness of the human rights proportionality test. The Regulation focuses on specific justifications: It outlines five reasons (national security, crime prevention, economic well-being, public safety, and international cooperation) for obtaining a warrant to intercept communication. It is also limited in scope, as it only applies to the interception of communication, not other privacy-invasive measures related to AI use.

The Human Rights Proportionality test is more comprehensive as it goes beyond specific justifications, requiring a balancing act between the importance of the objective (e.g., national security) and the limitations placed on individual rights (e.g., privacy). It considers less intrusive alternatives and encourages exploring options that achieve the objective with less impact on privacy. The test involves weighing the severity of the privacy restriction against the importance of the objective achieved. The Lawful Interception of Communications Regulation 2019 offers a starting point but the human rights proportionality test provides a more robust framework for safeguarding privacy when using AI for national security. Overall, the human rights proportionality test can provide a framework for Nigeria to ensure AI use for national security is necessary and proportionate to the threat and minimize privacy intrusions while achieving security goals. It will also foster

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf 13 May 2024.

[182] Ibid. Also, see the work of Yin on Harmonious AI law in Ghana.

[183] Babuta, Oswald and Janjeva, (n 175) 23.

public trust by demonstrating a commitment to balancing security and rights. By applying this test, Nigeria can develop a responsible and effective approach to AI that strengthens national security while safeguarding the fundamental rights of its citizens.

Currently, authorisation processes for agencies in the UK often focus on approving the initial collection of data. The position is the same in Nigeria in the laws that provide for warrants for the interception of information.[184] It has been argued that with AI, the data can be analysed later for new purposes and this creates a gap because the initial approval might not have considered all the potential uses of AI on that data.[185] Therefore emphasising the need for AI use to be demonstrably necessary and proportionate, balancing effectiveness with minimal intrusion on individual rights.[186]

Additionally, transparency and accountability are crucial, ensuring the public understands how these systems work and who bears responsibility for their decisions.[187] There is a need for the Nigerian government to be transparent about the specific AI tools used for national security and the justification behind their deployment. This transparency can help address public concerns about privacy and potential misuse. Human rights law offers a valuable framework for states to guide their decisions on deploying AI technologies.[188] This framework emphasises the need for transparency in justifying the deployment and ensuring it meets a pressing social need.[189] Additionally, it highlights the importance of proportionality, meaning the chosen AI solution should be the least intrusive option that achieves the desired outcome.[190]

[184] Terrorism (Prevention and Prohibition) Act 2022 Federal Republic of Nigeria Official Gazette No.91 Vol. 109 (16 May 2022), s 68; Cybercrimes Act 2015, s 39; Lawful Interception of Communications Regulations 2019, reg 7.
[185] Babuta, Oswald and Janjeva, (n 175) 23.
[186] Ibid.
[187] Ibid.
[188] D Murray, 'Symposium: How Will Artificial Intelligence Affect International Law? Using Human Rights Law To Inform States' Decisions to Deploy AI' [2020] 114 *American Journal of International Law Unbound* 158-162.
[189] Ibid, 160.
[190] Ibid.

In the UK, there are existing guidance and standards relating to the use of AI for national security purposes. They include the Data Ethics Frameworks issued by the Department for Digital, Culture, Media and Sport UK that sets overarching principles for the use of data such as transparency, accountability and fairness.[191] There is also the Guidance for Secure AI System Development issued by the National Security Agency, National Cyber Security Centre-UK, Cybersecurity and Infrastructure Security Agency, and Partners, which provides guidelines to ensure the secure design, development, deployment, operation and maintenance of AI systems.[192] Notably, in the UK, several organisations are involved in guiding the ethical and responsible utilization of AI.[193] These include the Centre for Data Ethics and Innovation,[194] the Information Commissioner's Office,[195] the Office for AI,[196] and parliamentary and independent committees,[197] among others. Nigeria can draw valuable lessons from the UK's approach to deploying AI for national security by adopting a robust framework that balances security needs with human rights. This includes using a human rights proportionality test to justify AI technologies, developing a unified national AI policy that prioritizes transparency, accountability, necessity, and proportionality, and instituting ongoing reviews to reassess AI's use on collected data. By adapting existing legal frameworks and

[191] Government Digital Service 'Data Ethics Framework' https://assets.publishing.service.gov.uk/media/5f74a4958fa8f5188dad0e99/Data_Ethics_Framework_2020.pdf 13 May 2024.

[192] The National Security Agency (NSA), UK National Cyber Security Centre (NCSC-UK), U.S Cybersecurity and Infrastructure Security Agency (CISA), and other partners 'Guidelines for Secure AI System Development' https://media.defense.gov/2023/Nov/27/2003346994/-1/-1/0/GUIDELINES-FOR-SECURE-AI-SYSTEM-DEVELOPMENT.PDF 14 May 2024. There is also the Government Digital Service and Office for Artificial Intelligence, 'Understanding Artificial Intelligence Ethics and Safety', 10 June 2019 https://www.gov.uk/guidance/understanding-artificial-intelligence-ethics-and-safety 8 May 2024.

[193] Babuta, Oswald and Janjeva, (n 175) 35.

[194] See UK Government, 'Centre for Data Ethics and Innovation', <https://www.gov.uk/government/> accessed 14 May 2024.

[195] ICO <https://ico.org.uk/> accessed 14 May 2024.

[196] Gov. UK, 'Office for Artificial Intelligence' <https://www.gov.uk/government/organisations/office-for-artificial-intelligence> accessed 14 May 2024.

[197] UK Parliament, 'Artificial Intelligence Committee' <https://committees.parliament.uk/committee/376/artificial-intelligence-committee> accesssed 14 May 2024.

clearly defining stakeholder roles, Nigeria can ensure ethical AI deployment that protects individual rights while fostering public trust.

CONCLUSION

This article has explored the challenges and opportunities of using Artificial Intelligence (AI) for national security in Nigeria. It compared Nigeria's approach to AI in national security with the United Kingdom identifying key lessons that Nigeria can learn from these countries. AI can be a valuable tool for national security, but it is important to develop and use AI responsibly. It also discussed existing AI projects in Nigeria as well as other technologies the country can leverage.

The multilingual large language model (LLM) project earlier discussed has received an initial funding of US$3.5 million from both local and international partners.[198] This includes a direct contribution of $1.5 million, with an additional $2 million invested by 21st Century Technologies.[199] Key supporters of the project include the UNDP, UNESCO, and major global tech companies such as Meta, Google, and Microsoft.[200] These funds will support pilot projects and contribute to the advancement of AI systems in Nigeria. Minister Bosun Tijani also highlighted other several key developments in Nigeria's artificial intelligence (AI) landscape, demonstrating the government's ongoing efforts to enhance AI capacity and infrastructure.[201] He reported that Nigeria's government, through partnerships with 21st Century Technologies and the National Centre for Artificial Intelligence and Robotics (NCAIR), is advancing its AI capabilities.[202] The collaboration involves funding the acquisition of GPUs to build the country’s national computing capacity, which will be accessible to local researchers, startups, and government entities for critical AI projects.[203] The GBB data centre in the Federal Capital

[198] Murithi, (n 60).
[199] Ibid.
[200] Ibid.
[201] Inclusion Times, ‘Nigeria Launches First Multilingual AI-Language Model’ (<https://www.inclusiontimes.com/nigeria-launches-first-multilingual-ai-language/> accessed 24 January 2025.
[202] Ibid.
[203] Ibid.

Territory (FCT) will house these resources.[204] Additionally, NCAIR has been relaunched with enhanced capacity, supported by CISCO, to strengthen AI research and development. These initiatives highlight Nigeria's commitment to fostering a robust AI ecosystem through public-private partnerships.

This study submits that Nigeria's growing AI ecosystem reflects promising strides, particularly in fostering public-private partnerships, building infrastructure, and gaining international recognition, but significant gaps remain that could hinder its potential, especially in national security applications. While the $3.5 million funding and partnerships with global tech companies demonstrate a commitment to AI development, the investment scale is modest compared to the vast resources needed for large-scale, security-focused AI projects. The investment scale for large-scale, security-focused AI projects for national security uses can range from hundreds of millions to several billion dollars, depending on the project's complexity, scope, data requirements, research and development needs, and the level of integration with existing infrastructure. For instance, the U.S. Department of Defence and the Department of Homeland Security have collectively invested approximately $700 million in AI projects for over two years.[205]

A comprehensive national AI policy is critical to addressing ethical challenges, data privacy, and algorithmic accountability, especially for applications in surveillance, border control, and counter-terrorism. Workforce development also lags, limiting Nigeria's ability to harness AI effectively in critical areas like intelligence analysis or predictive threat modelling. Additionally, the maturity of Nigeria's data ecosystem is insufficient for advanced AI models, which rely on high quality, representative datasets to support national security applications like identifying extremist activities or misinformation campaigns.[206] While initiatives

[204] Ibid.

[205] K Hays, 'The U.S. Defense and Homeland Security Departments have Paid $700 Million for AI projects since ChatGPT's Launch' *(Fortune*, October 15 2024) <https://fortune.com/2024/10/14/us-dod-dhs-700-million-ai-projects-past-two-years-increase-since-chatgpt-launch/> accessed 22 January 2025.

[206] According to a report by the GSMA, challenges in fostering AI-enabled solutions in Africa include a lack of open data ecosystems and local, quality data necessary for truly localized AI models. See Tanvi Deshpande, 'Understanding AI for Sustainable Development in Africa' (*GSMA*, 9 February 2024) https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/blog/understanding-ai-for-sustainable-development-in-africa/

like the NCAIR and GBB data centre aim to bolster computational capacity, ensuring their operational efficiency and scalability is crucial for supporting continuous advancements in security technologies. However, without a robust data infrastructure, these efforts may not reach their full potential. Therefore, to leverage AI for national security purposes, Nigeria must prioritize the development of a comprehensive data ecosystem alongside its investments in computational infrastructure. With a well-designed national AI strategy, Nigeria can strike a crucial balance: protecting its people while ensuring a secure future. Nigeria needs to address the challenges and risks of AI use, and it needs to develop a clear legal framework for AI. By doing so, Nigeria can ensure that AI is used for good and that it does not undermine human rights or national security. Below are some recommendations:

1. Increase Investment in AI Research and Development: Allocate significantly more funding for large-scale, security-focused AI projects, comparable to investments made by other nations. This could involve increased government funding, leveraging private sector investment, and exploring international collaborations in the context of AI deployment for national security purposes. The National Centre for Artificial Intelligence and Robotics (NCAIR) should include research efforts on areas with high national security relevance, such as cybersecurity, counter-terrorism, border security, and disaster response.
2. Enhance AI Talent Development: With AI-specific knowledge still in its infancy, the majority of Nigeria's tech talent concentrates on web development, mobile apps, and general IT. Although many of these programs are still in their infancy, universities are starting to offer AI-related courses.[207] Nigerian colleges and international organizations are working together to bridge the AI skills gap, but these initiatives still need to be scaled up.[208] Organizations like Data Science Nigeria (DSN),

[207] Baruwa, (n 121).

[208] Ibid.

the Nigerian Centre for Artificial Intelligence and Robotics (NCAIR), and AI Saturdays are promoting AI capabilities through training and workshops, and there is little doubt that Nigeria has a growing tech community.[209] Nonetheless, there is still a shortage of highly qualified data scientists and AI experts. There is a scarcity of qualified AI and data science specialists in Nigeria. Despite the increased interest, it will take time and money to develop local competence.[210] In Nigeria, instead of roles specialized in AI, a large portion of the talent is concentrated on general software development. Nigeria can expand AI education and training programs at all levels, from primary and secondary education to university and professional training. This includes supporting the development of AI curricula, providing scholarships and fellowships, and establishing AI research centres of excellence. The country can also create incentives to attract and retain top AI talent within Nigeria, such as competitive salaries, research opportunities, and supportive research environments.

3. Develop a Comprehensive National AI Strategy: This can be achieved by establishing and implementing clear ethical guidelines for the development and use of AI in national security, to address issues such as bias, fairness, accountability, transparency, and human oversight. It is also imperative that Nigeria establishes mechanisms for human oversight and control over AI systems used in national security, ensuring that human decision-making remains central. There is also a need to conduct regular reviews and assessments of AI systems used in national security to evaluate their effectiveness, identify potential risks, and ensure compliance with ethical guidelines and legal frameworks.

[209] Ibid.

[210] Ibid.

4. Foster Public Trust and Transparency: This can be done by promoting public awareness and education through engaging in public outreach and education programs to raise awareness about the potential benefits and risks of AI in national security. Nigeria can ensure transparency and accountability in the development and deployment of AI systems for national security.

5. Strengthen Data Infrastructure and Governance: Nigeria should develop a comprehensive national data strategy that addresses data collection, storage, sharing, and use for national security purposes. This should include guidelines for data quality, security, privacy, and ethical considerations. Investing in robust data infrastructure to facilitate efficient data collection, storage and management is imperative. Nigeria can invest in high-performance computing infrastructure by expanding and upgrading existing computing infrastructure, including high-performance computing clusters and cloud platforms, to support the development and deployment of advanced AI models. Finally, Nigeria must develop and implement clear data governance frameworks, including regulations, standards, and best practices for the ethical and responsible use of data in national security applications.

By following these recommendations, Nigeria can develop a robust framework for ethical and effective AI use in national security. This will allow the nation to reap the benefits of AI while safeguarding its citizens' fundamental rights and fostering public trust.

REFERENCES

Abiodun A, 'A Comparative Analysis of the Legal Framework for the Criminalization of Cyberterrorism in Nigeria, England, and the United States' (2021) 12(1) *Nnamdi Azikiwe University Journal of International Law and Jurisprudence* 99-112.

Adigun A, 'BREAKING: Nigerian Military Bans Drone Operation in North Eas' (*Nigerian Tribune*, 15 January 2025) https://tribuneonlineng.com/breaking-nigerian-military-bans-drone-operation-in-north-eas/> accessed 21 January 2025.

African Defence Forum, 'Nigerian Navy to Harness AI' (July 9 2024) <https://adf-magazine.com/2024/07/nigerian-navy-to-harness-ai/#:~:text=Emmanuel%20Ogalla%20made%20the%20announcement,are%20used%20in%20ship%20construction.> accessed 16 January 2025.

African Union, 'Continental Artificial Intelligence Strategy: Harnessing AI for Africa's Development and Prosperity' (July 2024) <https://au.int/sites/default/files/documents/44004-doc-EN-_Continental_AI_Strategy_July_2024.pdf> accessed 17 January 2024.

Afsah E, 'Artificial Intelligence, Law and National Security' in S. Voeneky *et al* (eds), *The Cambridge Handbook of Responsible Artificial Intelligence*, (Cambridge University Press, 2022)

Agency Reporter, 'Nigerian Navy Adopts AI to Enhance Operational Effectiveness – Ogalla' (*Nation Newspaper*, August 11 2023) <https://thenationonlineng.net/nigerian-navy-adopts-ai-to-enhance-operational-effectiveness-ogalla/> accessed 16 January 2025.

Ajose T, 'Nigeria to Deploy AI for Tackling Insecurity in 2025' (News Central, December 18, 2024) <https://newscentral.africa/nigeria-to-deploy-ai-for-tackling-insecurity-in-2025/> accessed 23 January 2025.

Allen G and Chan T, 'Artificial Intelligence and National Security' 18 <https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf> accessed 14 May 2024.

Al-Onyanabo T, 'Harnessing AI for Financial Inclusion in Nigeria: Opportunities and Challenges' (2024) <://www.researchgate.net/publication/381161690_Title_Page_Title_Harnessing_AI_for_Financial_Inclusion_in_Nigeria_Opportunities_and_Challenges> accessed 16 January 2025.

Amalu NS, 'Impact of Boko Haram Insurgency on Human Security in Nigeria' (2015) 14 *Global Journal of Social Sciences* 33-42.

Appel D and Black A, 'Generative AI for National Security' <https://www.thecipherbrief.com/column_article/generative-ai-for-national-security> accessed 16 January 2025.

Arakpogun EO and others 'Artificial Intelligence in Africa: Challenges and Opportunities' <https://researchportal.northumbria.ac.uk/ws/portalfiles/portal/31309999/AI_in_Africa_Opportunities_and_Challenges_Paper_68_Manuscript.pdf> accessed 16 January 2025.

Awotayo OO and others, ' Intelligence System and National Security in Nigeria: The Challenges of Data Gathering' (November 2023-April 2024) 4(2) *Janus.net e-journal of International Relations* 193-211.

Babalola O, 'The (Draft) National Artificial Intelligence (AI) Strategy: A Diminution of Privacy and Data Protection?' (*Itedgenews,* 7 August 2024) <https://www.itedgenews.africa/the-draft-national-artificial-intelligence-ai-strategy-a-diminution-of-privacy-and-data protection/#:~:text=By%20Olumide%20Babalola.%20On%20the%203rd%20day,make%20'input'%20and%20'further%20dissect%20its%20contents.'.> accessed 23 January 2025.

Babuta A, Oswald MO and Janjeva A, 'Artificial Intelligence and UK National Security Policy Considerations' (*RUSI Occasional Paper*, April 2020) <https://static.rusi.org/ai-national-security-final-web-version.pdf> accessed 14 May 2024.

Baruwa O, 'Nigeria: Is Nigeria Ready for Artificial Intelligence (Ai)?' (*allafrica*, 9 October 2024)

<https://allafrica.com/stories/202410100476.html#:~:text=AI%20thrives%20on%20high%2Dquality, currently%20lack%20sufficient%20data%20infrastructure> accessed 23 January 2025.

Black J and Murray AD, 'Regulating AI and Machine Learning: Setting the Regulatory Agenda', (2010) 10(3) *European Journal of Law and Technology* <https://www.ejlt.org/index.php/ejlt/article/view/722> accessed 2 May 2024.

Blasch E and others, 'Artificial Intelligence Strategies for National Security and Safety Standards' <https://arxiv.org/pdf/1911.05727> accessed January 21 2025.

Chesney R and Citron D, 'Deepfakes: A Looming Crisis for National Security, Democracy and Privacy?' *(Lawfare,* Wednesday, February 2018), <https://www.house.mn.gov/comm/docs/d9e1f352-ce1b-46d1-b4e3-2807437b571e.pdf> accessed 15 May 2024.

Congressional Research Service 'Artificial Intelligence and National Security' <https://sgp.fas.org/crs/natsec/R45178.pdf> accessed 9 May 2024.

Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, ETS 5, 4 November 1950, <https://www.refworld.org/legal/agreements/coe/1950/en/18688> accessed May 2024.

De Zúñiga H, and others, 'A Scholarly Definition of Artificial Intelligence (AI): Advancing AI as a Conceptual Framework in Communication Research' (2023) 4(2) *Political Communication* 317-344.

Defence Research and Development Organisation 'Programme Samyukta' <https://www.drdo.gov.in/drdo/programme-samyukta> accessed 12 May 2024.

Deshpande T, 'Understanding AI for Sustainable Development in Africa' (*GSMA*, 9 February 2024) <https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/blog/understanding-ai-for-sustainable-development-in-africa/ > accessed May 4 2024

Devineni SD, 'AI in Data Privacy and Security' (2024) *International Journal of Artificial Intelligence and Machine Learning* 35-49.

Dohrman D, CEO of Tangram Flex, Mihai Filip, CEO of Oves Enterprises, and Sean Moriarty, CEO of Primer AI discuss the future of AI in the national security and defense sector. 'Putting AI to work for National Security' Atlantic Council, 14 November 2024, Washington DC https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqbGRCTmt6c0J1Z2d6WEhmSU5DUURmSkkxaHBQQXxBQ3Jtc0tteFZQMXNZQ2pfSU10bUZZc2ZYb0kybUc5LXJTYUFtUXVZUm9XU2lYeEIwMTVTSXdpM2dwWk5TU0Z2Qy1tRUdxbFIwSHV5TUdudGRFWVNLbmtYbWVvQ3FDc2hOTS1WUlkwYnd2bHVpcHl5bDFqWGFTcw&q=https%3A%2F%2Fwww.atlanticcouncil.org%2Fevent%2Fputting-ai-to-work-for-national-security%2F&v=dXs7tQiGQaI accessed 9 May 2023.

Ebeh JI, 'National Security and National Development: A Critique' (2015) 4 IJCR 1-14.

Effoduh JO, 'Towards a Rights Respecting Artificial Intelligence Policy in Nigeria' <https://paradigmhq.org/wp-content/uploads/2021/11/Towards-A-Rights-Respecting-Artificial-Intelligence-Policy-for-Nigeria.pdf> accessed 23 April 2024.

Elimian G, 'Nigeria has only 8,352 Cybersecurity Professionals as Global Demand Rises to 4 Million' <https://leadership.ng/nigeria-has-only-8352-cybersecurity-professionals-report/> accessed 13 May 2024.

Eme OI and Oyinshi TO, 'Boko Haram and Security Challenges in Nigeria' (2014) 2 (11) *Kuwait Chapter of Arabian Journal of Business and Management Review*, 1-18.

Eme OI and Oyinshi TO, 'Boko Haram Insurgency in Nigeria: Implications for National Security and Restorative Justice' (2019) 19 *African Journal on Conflict Resolution* 1-17.

EU 'Artificial Intelligence Act Final Draft (2024)' https://artificialintelligenceact.eu/the-act/ on 15 May 2024 The EU AI Act is a proposed regulation by the EU to establish uniform rules for using AI. For details on China's AI regulations see, Sheehan M, 'Tracing the Roots of China's AI Regulations' <https://carnegieendowment.org/2024/02/27/tracing-roots-of-china-s-ai-regulations-pub-91815> accessed 15 May 2024.

Federal Ministry of Communication, Innovation, and Digital Economy, 'Ministry Announce N2.8billion Google Support to Advance AI Talent Development in Nigeria' (October 31 2024) <https://fmcide.gov.ng/ministry-announce-n2-8billion-google-support-to-advance-ai-talent-development-in-nigeria/> accessed 17 January 2025.

Gov. UK, 'Explanatory Framework for Adequacy Discussions Section H: National Security Data Protection and Investigatory Powers Framework' 18 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf 13 May 2024.

Gov. UK, 'Office for Artificial Intelligence' <https://www.gov.uk/government/organisations/office-for-artificial-intelligence> accessed 14 May 2024.

Government Digital Service 'Data Ethics Framework' https://assets.publishing.service.gov.uk/media/5f74a4958fa8f5188dad0e99/Data_Ethics_Framework_2020.pdf 13 May 2024.

Green B, 'The Flaws of Policies Requiring Human Oversight of Government Algorithms' (2022) *Computer Law & Security Review* 1-22 https://doi.org/10.1016/j.clsr.2022.105681.(https://www.sciencedirect.com/science/article/pii/S0267364922000292).

Gubak HD and Bulus K, 'National Security Challenges and Sustainable Development in Nigeria: A Critical Analysis of the Niger Delta Region' (2018) 4 *Global Journal of Political Science and Administration,* 32-50.

Guinn Center for Policy Priorities, 'Introduction Artificial Intelligence Defined' <https://guinncenter.org/wp-content/uploads/2024/04/AI-General-Overview-KBC-Edit-V2-040424.pdf > accessed 23 May 2024.

Hawkes S,'Mantra Embraces Artificial Intelligence in Security' (*Mantra Protection Solutions Limited,* November 25 2024) <https://www.mantraoperations.com/blog/2024/11/25/mantra-embraces-

artificial-intelligence-in-security?utm_source=chatgpt.com> accessed 17 January 2025.

Hays K, 'The U.S. Defense and Homeland Security Departments have Paid $700 Million for AI projects since ChatGPT's Launch' *(Fortune*, October 15 2024) <https://fortune.com/2024/10/14/us-dod-dhs-700-million-ai-projects-past-two-years-increase-since-chatgpt-launch/> accessed 22 January 2025.

Heine K and Quintavalla A, 'Bridging the Accountability Gap of Artificial Intelligence – What Can Be Learned from Roman Law?' (2024) 44 *Legal Studies* 65-80.

Hoadley DS and Sayler KM, 'Artificial Intelligence and National Security' <https://apps.dtic.mil/sti/trecms/pdf/AD1107549.pdf > accessed 13 May 2024.

Hu M, Behar E and Ottenheimer D, 'National Security and Federalizing Data Privacy Infrastructure for AI Governance' (2024) 92(5) *Fordharm Law Review* 1829-1853.

Iashvili G and Iavich M, 'Enhancing Cyber Intelligence Capabilities through Process Automation: Advantages and Opportunities' in A Lopata *et al Advanced Information Networking and Applications, the 36th International Conference on Advanced Information Networking and Applications* (AINA-2022), Sydney, NSW, Australia, 13-15 April 2022, 92-101.

Iashvili G and Iavich M, 'Enhancing Cyber Intelligence Capabilities through Process Automation: Advantages and Opportunities' in A Lopata *et al Advanced Information Networking and Applications, the 36th International Conference on Advanced Information Networking and Applications* (AINA-2022), Sydney, NSW, Australia, 13-15 April 2022, 92-101.

Ibeh R, 'Deploying Artificial Intelligence To Tackle Nigeria's Security Challenges' (*National Economy*) <https://nationaleconomy.com/deploying-artificial-intelligence-to-tackle-nigerias-security-challenges/#:~:text=In%20line%20with%20this%2C%20the,and%20information%20and%20communication%20security> accessed 9 May 2024.

ICO <https://ico.org.uk/> accessed 14 May 2024.

Inclusion Times, 'Nigeria Launches First Multilingual AI-Language Model' (April 22 2024) <https://www.inclusiontimes.com/nigeria-launches-first-multilingual-ai-language/#:~:text=The%20Federal%20Government%20has%20launched,relaunch%20in%20partnership%20with%20Cisco.> accessed 17 January 2025.

Inclusion Times, 'Nigeria Launches First Multilingual AI-Language Model' <https://www.inclusiontimes.com/nigeria-launches-first-multilingual-ai-language/> accessed 24 January 2025.

Indian Defence Analysis, 'Himshakti: India's Most Lethal Electronic Warfare System' <https://indiandefenseanalysis.wordpress.com/2023/03/25/himshakti-indian-armys-most-lethal-electronic-warfare-system/> accessed 16 January 2024.

International Committee of the Red Cross (ICRC), A Guide to the Legal Review of New Weapons, Means and Methods of Warfare (2006) 23 <https://www.icrc.org/en/doc/assets/files/other/icrc_002_0902.pdf> accessed 13 May 2024.

ITedgenews, 'Kenya Unveils National AI Strategy 2025-2030, Aiming to Lead Africa's AI Revolution' <https://www.itedgenews.africa/kenya-unveils-national-ai-strategy-2025-2030-aiming-to-lead-africas-ai-revolution/#:~:text=AI%20revolution%20%2D%20ITEdgeNews-,Kenya%20unveils%20National%20AI%20Strategy%202025%2D2030%2C%20aiming,to%20lead%20Africa's%20AI%20revolution&text=Kenya's%20Ministry%20of%20ICT%20and,AI)%20Strategy%202025%2D2030.> accessed 17 January 2025.

Jaiyeola J, 'Cyberattacks on Nigerian Govt Agencies Rise — Report' <https://punchng.com/cyberattacks-on-nigerian-govt-agencies-rise-report/> accessed 13 May 2024.

Joshi MA, 'The Security Risks of Generative Artificial Intelligence' (2024) 7(2) *International Journal on Integrated Education (IJIE)* 91-95.

Kalpokas I and Kalpokiene J, *Deepfakes: A Realistic Assessment of Potentials, Risks and Policy Regulation* (Springer, 2022) .

Lyons-Cunha J, 'What is AI Infrastructure?' (11 December 2024) <https://builtin.com/artificial-intelligence/ai-infrastructure> accessed 16 January 2024.

Maisha KF, 'AI & Arms Race: The Rivalry between the U.S. & China in the Field of Tech Supremacy' (BIPSS Commentary) <https://bipss.org.bd/pdf/AI%20&%20Arms%20Race%20The%20Rivalry%20Between%20the%20U.S.%20&.pdf> accessed 13 May 2024.

Martins MR, 'From On-Premise to Cloud: Evolving IT Infrastructure for the AI Age' (2023) 20(03), *World Journal of Advanced Research and Reviews,* 1898-1934.

Meijer A and Wessels M, 'Predictive Policing: Review of Benefits and Drawbacks' (2019) 42(1) *International Journal of Public Administration* 1-9.

Murithi KM, 'AI News: Nigerian Government Debuts AI Tool with Multilingual Capabilities' (*Coingape,* April 20 2024) <https://coingape.com/ai-news-nigerian-government-debuts-ai-tool-with-multilingual-capabilities/> accessed 17 January 2025.

Murray D, 'Symposium: How Will Artificial Intelligence Affect International Law? Using Human Rights Law To Inform States' Decisions to Deploy AI' (2020) 114 *American Journal of International Law Unbound* 158-162

NCAIR and NITDA, 'National AI Strategy 2024' <https://ncair.nitda.gov.ng/wp-content/uploads/2024/08/National-AI-Strategy_01082024-copy.pdf> accessed 23 January 2025.

NCAIR, <https://ncair.nitda.gov.ng/> accessed 22 January 2025.

Nsude, I 'Artificial Intelligence (AI), The Media and Security Challenges In Nigeria' (2022) 11 *Communication, technologies et développement* 1-16.

Nwosu CC and others, 'Artificial Intelligence in Public Service and Governance in Nigeria' (2024) 4(2) *Journal of Governance and Accountability Studies,* 109-120.

Olaoluwa F and Potter K, 'Natural Language Processing (NLP) for Social Media Threat Intelligence' *Preprints* (2024) https://doi.org/10.20944/preprints202409.0488.v1

Oliver D, 'Pioneering Unmanned Fleet in Sub-Saharan Africa' (*Times Aerospace*, 20 March 2024) <https://www.timesaerospace.aero/features/defence/pioneering-unmanned-fleet-in-sub-saharan-africa#:~:text=Nigeria%20is%20the%20only%20country,have%20used%20them%20in%20combat.> accessed 21 January 2025.

Olokor F, 'Nigeria Can Fight Boko Haram, insecurity with AI, Says Borno's Chief Judge' <https://www.arise.tv/nigeria-can-fight-boko-haram-insecurity-with-ai-says-bornos-chief-judge/> accessed 15 May 2024.

Olubusoye OE, Korter GO, and Keshinro O, 'Nigerian Statistical System: the Evolution, Progress and Challenges' <http://doi/10.13140/RG.2.1.3136.4569> accessed 22 January 2024.

Oluda OF and Josephs CG, 'The Causes of Digital Divide in Nigeria: The Context of the Nigerian Law Reform Commission' Master Thesis, Lund University School of Economics and Management 2023, <https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9123699&fileOId=9123921> accessed 23 January 2025.

Park SH, 'Ethics for Artificial Intelligence: Focus on the Use of Radiology Images' (2022) 83(4) *Journal of the Korean Society of Radiology* 759-770. DOI: 10.3348/jksr.2022.0036.

Patel F and Tommey PC, 'An Oversight Model for AI in National Security: The Privacy and Civil Liberties Oversight Board' <https://www.brennancenter.org/our-work/analysis-opinion/oversight-model-ai-national-security-privacy-and-civil-liberties> accessed 20 May 2024.

Raimi L, Akhemonkhan I, and Ogunjirin OD, 'Corporate Social Responsibility and Entrepreneurship (CSRE): Antidotes to Poverty, Insecurity and Underdevelopment in Nigeria' 6th International Conference held in Universiti de Lome, Togo) from 1st to 2nd November 2012). [1] A Akubo and BI Okolo, ‘Boko Haram Insurgency in Nigeria’ 1-17 < https://www.accord.org.za/ajcr-issues/boko-haram-insurgency-in-nigeria/> accessed 26 August 2024.

Sayler KM and Harris LM, ‘Deepfakes and National Security’ <https://apps.dtic.mil/sti/pdfs/AD1117081.pdf> accessed n 13 May 2024.

Schmitt MN and Thurnher JS, ‘’Out of the Loop’: Autonomous Weapons Systems and the Law of Armed Conflict’ (2013) 4 *Harvard National Security Journal* 231-281.

Srivastava K, ‘Artificial Intelligence and National Security: Perspective of the Global South’ (2023) 2(2) *International Journal of Law in Changing World* 77-87.

Swire P and Sacks S, ‘Limiting Data Broker Sales in the Name of U.S. National Security: Questions on Substance and Messaging’ https://www.lawfaremedia.org/article/limiting-data-broker-sales-in-the-name-of-u.s.- national-security-questions-on-substance-and-messaging [https://perma.cc/UA98-94Q2 on 15 May 2024,

Szabadföldi, I, ‘Artificial Intelligence in Military Application - Opportunities and Challenges’ (2021) XXVI *Land Forces Academic* Review 157-165.

The National Security Agency (NSA), UK National Cyber Security Centre (NCSC-UK), U.S Cybersecurity and Infrastructure Security Agency (CISA), and other partners ‘Guidelines for Secure AI System Development’ https://media.defense.gov/2023/Nov/27/2003346994/-1/-1/0/GUIDELINES-FOR-SECURE-AI-SYSTEM-DEVELOPMENT.PDF 14 May 2024. There is also the Government Digital Service and Office for Artificial Intelligence, ‘Understanding Artificial Intelligence Ethics and Safety’, 10 June 2019 https://www.gov.uk/guidance/understanding-artificial-intelligence-ethics-and-safety 8 May 2024. UK Government, ‘Centre for Data Ethics and Innovation’, <https://www.gov.uk/government/> accessed 14 May 2024.

The Regulation of Investigatory Powers Act 2000, available at <http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf> accessed 13 May 2024.

The UK Investigatory Powers Act 2016 (IPA 2016) available at <https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted/data.htm> accessed 13 May 2024.

Timi-Koleolu S and Atanda O, 'Artificial Intelligence In Nigeria: Legal and Regulatory Guidance' <https://pavestoneslegal.com/newsletters/ > accessed 9 May 2023.

Uba J, 'Nigeria: Artificial Intelligence (AI) Regulation In Nigeria: Key Considerations, Recommendations, Legal Framework, And Policy Development For Artificial Intelligence (AI) In Nigeria' <https://www.mondaq.com/nigeria/new-technology/1373830/artificial-intelligence-ai-regulation-in-nigeria-key-considerations-recommendations-legal-framework-and-policy-development-for-artificial-intelligence-ai-in-nigeria> accessed 9 May 2023.

UK Parliament, 'Artificial Intelligence Committee' <https://committees.parliament.uk/committee/376/artificial-intelligence-committee> accessed 14 May 2024.

United Kingdom: Human Rights Act 1998, 9 November 1998, <https://www.refworld.org/legal/legislation/natlegbod/1998/en/48641> accessed 14 May 2024.

US Government Accountability Office 'How Artificial Intelligence Is Transforming National Security' (*GOA Watchblog,* 19 April 2023) <https://www.gao.gov/blog/how-artificial-intelligence-transforming-national-security#:~:text=AI%20in%20national%20security%2C%20on,integrate%20AI%20into%20defense%20systemson> accessed 9 May 2024.

Yin, Elijah Tukwariba. "Regulation and Ethical Issues of Artificial Intelligence in Ghana: Towards a Harmonious AI Law." *Exploring AI Implications on Law, Governance, and Industry*. IGI Global Scientific Publishing, 2025. 119-156.

Yu C, 'AI as Critical Infrastructure: Safeguarding National Security in the Age of Artificial Intelligence' <https://osf.io/preprints/osf/u4kdq> accessed15 May 2024.

Zakari M, Implication of Artificial Intelligence on National Security for the Nigerian Security Agencies' (2024) 6(1) *Journal of Terrorism Studies,* 1-15.

Zimmermann A, Vredenburgh K, and Lazar S, 'The Political Philosophy of Data and AI' (2022) 52(1) *Canadian Journal of Philosophy* 1–5.

STATUTES

Cybercrimes (Prohibition, Prevention, etc.) Act, 2015

European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights)

Human Rights Act 1998 (United Kingdom)

Nigeria Data Protection Act 2023 (Nigeria)

Protection of Personal Information Act 4 of 2013 (POPI Act) (South Africa)

Regulation of Investigatory Powers Act 2000 (United Kingdom)

Terrorism (Prevention and Prohibition) Act 2022 Federal Republic of Nigeria Official Gazette No.91 Vol. 109 (16 May 2022) UK Investigatory Powers Act 2016 (IPA 2016) (United Kingdom)