Center of Artificial Intelligence

CENTER OF SCIENCE

REVIEW ARTICLE

Artificial Intelligence and the Future of Knowledge Preservation: Implications for National Security and Strategic Decision-Making in Nigeria

Olalekan Idowu JIMOH [1] *, Adeolu Oluwaseun ADEJOBI [2]

[1] Department of Political Science and Defence Studies, Nigerian Defence Academy, Kaduna, Kaduna State, Nigeria

[2] Department of Library, Archival and Information Studies, University of Ibadan, Ibadan, Oyo State, Nigeria

* Corresponding Author's E-mail: jimohoijoseph@gmail.com

Article Info.

Article history:

Received: 29/12/2025

Accepted: 17/01/2025

Published: 27/01/2026

Abstract

The rapid advancement of Artificial Intelligence (AI) has transformed how nations create, store, and utilise knowledge, with profound implications for national security and strategic decision-making. In Nigeria, weak institutional memory, inadequate knowledge management systems, and fragmented data infrastructures have created significant vulnerabilities in national security operations and policy formulation. This study examines how AI-driven technologies can enhance knowledge preservation and strengthen strategic decision-making frameworks within Nigeria's security architecture. Guided by the Knowledge Management Theory and Information Warfare Theory, the research adopts a qualitative approach, drawing on content analysis of policy documents, scholarly publications, and institutional reports from the Nigerian Defence Academy, NITDA, and global AI frameworks. Findings reveal that while AI presents immense opportunities for improving intelligence analysis, data preservation, and evidence-based policy formulation, Nigeria faces critical challenges, including poor digital infrastructure, limited AI literacy, and weak policy coordination. The study underscores the urgent need for a National AI and Knowledge Preservation Policy to safeguard institutional memory, promote data sovereignty, and strengthen national resilience against emerging cyber and information threats. It concludes that integrating AI into Nigeria's strategic systems can serve as a catalyst for sustainable national security, improved governance, and informed decision-making, provided that ethical, infrastructural, and policy frameworks are effectively implemented.

Keywords: Artificial Intelligence; Knowledge Preservation; National Security; Strategic Decision-Making; Digital Sovereignty; Nigeria.

Introduction

The twenty-first century has witnessed a profound transformation in the global knowledge ecosystem, driven by rapid advances in Artificial Intelligence (AI), machine learning (ML), and digital technologies. These innovations have revolutionised how knowledge is created, stored, and transmitted, blurring traditional boundaries between human cognition and automated intelligence [1]. In today's interconnected world, knowledge has become a strategic resource; a critical determinant of national power, competitiveness, and security. As AI systems increasingly automate the collection, analysis, and storage of information, the concept of knowledge preservation the systematic safeguarding of institutional and national intelligence has assumed new significance. However, alongside these opportunities lie deep-seated vulnerabilities: algorithmic bias, data obsolescence, cyber espionage, and the erosion of human institutional memory [2]. Understanding how AI reshapes knowledge preservation is, therefore, central to the debate on national security and strategic decision-making, particularly in developing countries such as Nigeria.

Knowledge preservation has historically served as the foundation for statecraft, intelligence continuity, and policy planning. Nations that effectively manage and preserve institutional knowledge are better equipped to anticipate security threats, formulate evidence-based policies, and respond to crises. The growing integration of AI in intelligence and defence infrastructures from predictive analytics and surveillance to cyber threat detection has amplified both the capacity and the complexity of knowledge systems [3]. In this emerging landscape, the preservation of digital knowledge is no longer merely an archival concern; it is a strategic imperative. The loss, manipulation, or inaccessibility of critical data whether through cyberattacks, system failures, or poor data governance can severely undermine a nation's security posture and its ability to make timely, informed decisions.

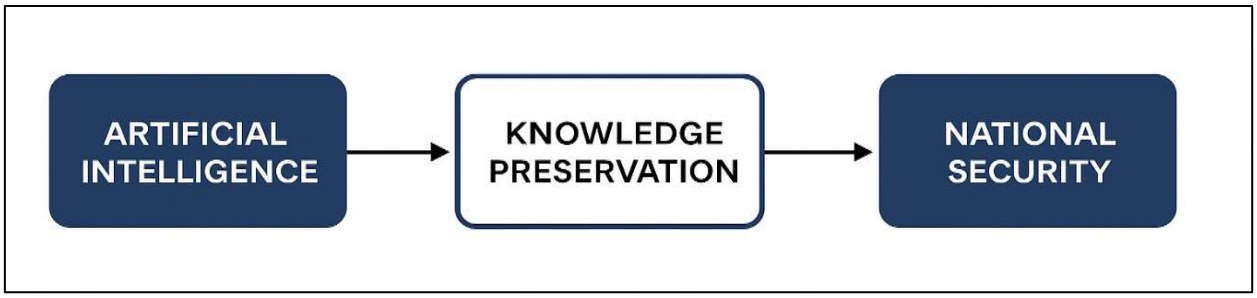

Fig. 1: *Conceptual diagram showing the link between AI, Knowledge Preservation, and National Security*

In the Nigerian context, these challenges are particularly pronounced. Despite growing digital adoption across government institutions, the country faces chronic problems of data insecurity, cyber vulnerability, and institutional memory loss [4]. Many national databases ranging from population and financial records to intelligence archives remain fragmented, poorly digitised, or exposed to cyber risks. Moreover, weak inter-agency coordination, poor data governance frameworks, and inadequate investment in AI-driven knowledge management have compounded the threat of information decay and loss of strategic memory [5]. For Nigeria's security and defence sectors, the implications are profound: intelligence gaps, duplication of effort, and slow response to evolving threats such as terrorism, cyber warfare, and disinformation.

Furthermore, AI introduces both promise and peril in the preservation of knowledge. On the one hand, intelligent systems can automate document classification, ensure long-term digital storage, and enhance retrieval efficiency through semantic search technologies [6]. On the other hand, reliance on AI-driven platforms without robust cybersecurity or ethical oversight can expose critical data to adversarial attacks, algorithmic manipulation, and unauthorised access. The Nigerian government's increasing adoption of digital governance tools, including biometric systems, defence surveillance platforms, and AI-based policy analytics, underscores the urgency of developing secure, ethical, and resilient knowledge preservation strategies [7].

In essence, this study explores how Artificial Intelligence is reshaping the landscape of knowledge preservation and its implications for national security and strategic decision-making in Nigeria. It interrogates the intersection of technology, policy, and security asking how the country can safeguard its digital heritage while harnessing AI for innovation and resilience. By situating Nigeria within global debates on AI governance, cybersecurity, and strategic knowledge management, the study aims to contribute to a deeper understanding of how emerging technologies can either fortify or fracture the very foundations of national security.

Literature Review

The emergence of Artificial Intelligence (AI) has redefined the landscape of knowledge creation, preservation, and utilisation in contemporary governance and security. AI, encompassing technologies such as machine learning, deep learning, and natural language processing, refers to systems capable of performing cognitive functions traditionally associated with human intelligence [8]. In the context of national security, AI's relevance lies in its ability to automate intelligence analysis, predict threats, and preserve vast institutional data through algorithmic processing and advanced storage mechanisms. Machine learning, a subset of AI, enables systems to learn from data patterns and improve decision accuracy over time critical for detecting cyber threats, managing classified information, and enhancing real-time situational awareness [9].

Knowledge preservation refers to the systematic process of capturing, organising, and safeguarding information to ensure its longevity and accessibility for future use. It goes beyond archiving documents to include codifying tacit knowledge, securing digital databases, and maintaining institutional memory [10]. Models such as the SECI framework (Socialisation, Externalisation, Combination, Internalisation) developed by [11] highlight how knowledge is created, shared, and institutionalised across organisations. In national security, knowledge preservation ensures continuity in strategic planning, intelligence gathering, and intergenerational transfer of expertise especially in bureaucratic institutions prone to data loss or political turnover.

Strategic decision-making in the security domain involves the integration of intelligence, foresight, and technological tools to formulate policies that safeguard national interests [12]. AI enhances this process through predictive analytics, real-time threat detection, and cognitive decision-support systems, reducing reliance on fragmented or outdated information. However, in Nigeria, weak institutional data systems, poor cyber governance, and infrastructural deficits threaten the sustainability of digital knowledge preservation, increasing vulnerability to misinformation and data loss [13].

Theoretical Review

This study draws upon two interrelated theoretical frameworks to conceptualise the relationship between AI, knowledge preservation, and national security namely, the Knowledge Management Theory and Information Warfare Theory.

The Knowledge Management Theory by [11] posits that organisational knowledge is a key source of innovation and competitive advantage. Knowledge is created through dynamic interactions between tacit and explicit knowledge forms, requiring supportive technologies and institutional culture. In the context of AI, this theory underscores how intelligent systems facilitate knowledge retention and retrieval, particularly in sensitive security environments where institutional continuity is vital.

The Information Warfare Theory developed by [14] focuses on the strategic use and control of information as a weapon in modern conflicts. It argues that dominance over information systems equates to power in the digital age, where states and non-state actors compete to control narratives, data, and cyber networks. Applying this to Nigeria, the integration of AI in intelligence operations enhances national resilience against cyberattacks, espionage, and disinformation campaigns that threaten state stability.

Methodology

This study adopts a descriptive and analytical research design, aimed at exploring how Artificial Intelligence (AI) influences knowledge preservation and its implications for national security and strategic decision-making in Nigeria. The research employed qualitative content analysis combined with an extensive secondary data review. Policy documents published between 2015 and 2025 were examined, and this period was selected to capture Nigeria's contemporary security and digital governance landscape, particularly following the expansion of counterterrorism operations, the rise of digital governance initiatives, and increased discourse on data-driven national security.

The selection criteria for policy documents were refined to include: official federal government policies, white papers, and strategic frameworks related to national security, intelligence coordination, ICT, and digital governance; documents issued by core security and policy institutions such as the Office of the National Security Adviser (ONSA), National Intelligence Agency (NIA), Defence Intelligence Agency (DIA), Nigerian Police Force, and relevant ministries; Nigerian Defence Academy (NDA), the Federal Ministry of Communications, Innovation and Digital Economy, and the National Information Technology Development Agency (NITDA), which oversees Nigeria's AI and digital policy frameworks. International sources include the World Economic Forum (WEF), United Nations Educational, Scientific and Cultural Organisation (UNESCO), and Organisation for Economic Co-operation and Development (OECD) policy papers on AI ethics, digital transformation, and knowledge governance. Additional secondary sources were drawn from peer-reviewed journals, books, and global policy databases that discuss AI-driven knowledge systems, cybersecurity, and strategic intelligence. The study employs a thematic and comparative analytical framework.

The Nexus between Artificial Intelligence and Knowledge Preservation

The emergence of Artificial Intelligence (AI) has transformed the landscape of knowledge creation, preservation, and utilization across sectors, marking a paradigm shift in how societies store, secure, and retrieve information. Knowledge preservation traditionally dependent on manual archiving and static repositories has evolved into a dynamic, data-driven ecosystem underpinned by intelligent systems capable of processing vast datasets, detecting patterns, and ensuring institutional continuity. In the context of national security, where knowledge equates to power and strategic foresight, AI has become indispensable for managing complex intelligence archives, enhancing data accessibility, and safeguarding institutional memory.

AI enhances knowledge preservation through its capacity to automate data archiving, retrieval, and curation processes. Machine learning (ML) algorithms can identify, categorize, and store critical information efficiently, minimizing human error and bias in knowledge systems [15]. For instance, supervised learning models are employed to classify intelligence reports, policy documents, and operational data based on content, metadata, and context. Similarly, unsupervised learning supports anomaly detection and trend analysis, critical for identifying gaps in institutional knowledge or potential security vulnerabilities.

Moreover, Natural Language Processing (NLP) has revolutionized text preservation and retrieval by enabling machines to understand, interpret, and generate human language. NLP tools are increasingly used to digitize and structure historical documents, declassify intelligence materials, and facilitate multilingual information access within government and defence archives [16]. In Nigeria's intelligence and policy ecosystem, integrating NLP-powered systems could enhance institutional efficiency by converting vast unstructured archives ranging from debriefing reports to legislative records into searchable, actionable intelligence.

In addition, predictive analytics, a branch of AI, aids in forecasting information needs and identifying critical knowledge assets at risk of loss or obsolescence. By analysing historical patterns, AI systems can recommend proactive measures to safeguard vital data repositories, predict future trends in strategic domains, and support evidence-based decision-making. This predictive capability has been applied in military intelligence forecasting, cyber threat detection, and strategic risk assessment [17].

Table 1: AI Tools for Knowledge Preservation and Their Applications

AI Tool	Primary Function	Application in Knowledge Preservation	Example/Use Case
Machine Learning (ML)	Pattern recognition and data classification	Automates categorization of archives and intelligence reports	Defence archives in the U.S. Department of Defense (JAIC)
Natural Language Processing (NLP)	Text comprehension and translation	Digitizes and analyses textual data from unstructured sources	UN AI Ethics Repository for multilingual data
Predictive Analytics	Forecasting and trend analysis	Identifies at-risk knowledge repositories; predicts data needs	Cyber threat intelligence and risk management systems
Neural Networks	Deep learning for unstructured data	Enhances image, video, and document recognition	AI-powered document scanning in digital heritage projects

Cloud AI Services	Data storage and intelligent retrieval	Provides scalable, secure storage for large datasets	Amazon S3 Intelligent-Tiering, Google Cloud AI
Blockchain-Integrated AI	Secure data integrity and traceability	Ensures authenticity and non-repudiation of stored knowledge	National Archives using blockchain for document verification

Source: Compiled by the Author from [18, 19, 20, 21, 22, 23].

AI thus represents a transformative force in modern knowledge preservation one that not only digitizes history but also safeguards the future. In the Nigerian national security context, its adoption could mitigate institutional memory loss, enhance data-driven decision-making, and foster strategic resilience in an era of information warfare.

Knowledge Preservation, Institutional Memory, and National Security

Knowledge preservation and institutional memory form the backbone of national resilience, particularly within the realms of intelligence, diplomacy, and defence. For any nation, the ability to retain, retrieve, and utilise accumulated knowledge determines not only policy coherence but also the continuity of strategic vision across changing administrations. In the context of national security, institutional memory ensures that lessons from past operations, negotiations, and policy frameworks are not lost to political transitions or bureaucratic inefficiencies. Modern security institutions thrive on the systematic preservation of knowledge to sustain both operational efficiency and strategic foresight.

Importance of Knowledge Continuity in Intelligence, Diplomacy, and Defence

In intelligence and defence establishments, knowledge continuity guarantees that security operations are informed by cumulative experience and situational awareness. The loss of critical data or classified archives can result in repeated operational failures and strategic blind spots. For instance, continuity of intelligence knowledge allows for pattern recognition in counterterrorism operations, trend analysis in cyber defence, and accurate threat forecasting [24]. Similarly, in diplomacy, access to historical records enables negotiators to maintain consistent foreign policy positions and uphold national credibility.

In advanced nations, institutional memory is considered an asset embedded in secure, AI-driven knowledge systems that integrate human expertise with digital intelligence. These systems found in the U.S. National Security Agency (NSA), the UK's Government Communications Headquarters (GCHQ), and Israel's Directorate of Military Intelligence ensure continuity through knowledge retention frameworks, periodic data audits, and digital redundancy. AI technologies, especially those based on machine learning and semantic data analysis, are increasingly used to manage the life cycle of classified knowledge from creation to archival and retrieval [25].

Nigeria's Institutional Challenges: Loss of Records, Poor Digital Infrastructure, and Bureaucratic Fragmentation

Nigeria, by contrast, continues to grapple with systemic weaknesses in knowledge management across its defence, intelligence, and diplomatic institutions. The lack of a unified digital archiving policy, coupled with poor infrastructure and fragmented bureaucracies, has resulted in significant loss of institutional memory. Vital intelligence and defence data are often stored manually or inconsistently across ministries and agencies, exposing them to risks of misplacement, manipulation, or physical damage [26].

Furthermore, frequent leadership changes and weak inter-agency coordination impede knowledge transfer. Each administrative cycle often begins anew, disregarding prior insights a phenomenon [27] terms "policy amnesia." This discontinuity undermines Nigeria's capacity to learn from past counterinsurgency efforts, diplomatic negotiations, and strategic security assessments. Additionally, the limited adoption of AI-driven document management systems and inadequate cybersecurity frameworks make Nigeria's national archives highly vulnerable to data loss and cyber intrusions.

Table 2: Comparative Analysis of Knowledge Preservation Maturity Levels (Nigeria vs. Global Benchmarks)

Dimension	Nigeria	Global Benchmarks (e.g., USA, UK, Israel)	Remarks
Policy Framework	Fragmented and reactive; limited digital policies	Integrated national digital archiving and security strategies	Nigeria lacks a unified digital knowledge framework
Technology Adoption	Low; manual and inconsistent digital systems	Advanced AI, cloud computing, and automated archives	Technological gap undermines efficiency
Cybersecurity Infrastructure	Weak enforcement and outdated protection systems	Robust cyber defence and real-time threat detection	Nigeria's archives remain vulnerable to breaches
Institutional Coordination	Poor inter-agency collaboration and knowledge transfer	Cross-agency integration and shared intelligence platforms	Bureaucratic silos weaken institutional memory
Data Sovereignty	Reliance on foreign storage and cloud systems	Strong local data governance and sovereignty laws	Risk of external access to national intelligence data
Human Capacity	Limited digital literacy and AI expertise	Skilled workforce and continuous professional training	Nigeria must invest in AI literacy and digital governance

Source: Compiled by the Author from [18, 19, 20, 21, 22, 23].

Artificial Intelligence and Strategic Decision-Making

Artificial Intelligence (AI) has emerged as a transformative force in strategic decision-making, reshaping the processes through which intelligence is gathered, analysed, and utilised for national security and defence operations. In an era characterised by complex and rapidly evolving threats from cyberattacks and terrorism to geopolitical instability AI systems are increasingly used to enhance analytical precision, risk forecasting, and operational efficiency. Strategic decision-making, particularly in the security and defence sectors, depends on the timely synthesis of vast data streams into actionable insights a task AI performs with unparalleled speed and accuracy [15].

AI in Intelligence Analysis and Decision Support Systems: AI's integration into intelligence analysis and decision support systems has revolutionised how governments and defence institutions interpret information and make policy or tactical decisions. AI-powered decision support systems (DSS) leverage machine learning algorithms to detect hidden patterns within large datasets, providing intelligence analysts with deeper situational awareness and predictive insights. For instance, natural language processing (NLP) enables the automated extraction of critical intelligence from text, communications, and open-source data, while computer vision aids in the analysis of satellite and surveillance imagery [28].

In the national security context, AI's analytical capabilities allow agencies to process data at scales beyond human capacity, improving the precision of counterterrorism, cyber defence, and border security operations. Within Nigeria, AI-enabled systems could be utilised by the Defence Intelligence Agency (DIA) and the Office of the National Security Adviser (ONSA) to improve intelligence fusion, early warning mechanisms, and strategic coordination. These systems enhance decision superiority, enabling national leaders to respond effectively to emerging threats [29].

Predictive Analytics for Risk Assessment and Crisis Management: Predictive analytics, one of AI's most critical applications in strategic decision-making, helps anticipate potential risks and inform proactive responses. Machine learning models trained on historical data can forecast conflict escalation, insurgency hotspots, or cyber intrusion attempts with high accuracy. For instance, neural networks and Bayesian models have been successfully used in global defence systems to predict troop movements, assess geopolitical risks, and model crisis scenarios [30].

In Nigeria, predictive analytics can be deployed to improve national risk assessment frameworks such as identifying flashpoints of insecurity in the North-West or forecasting economic instability linked to political unrest. These insights can inform the National Security Council's strategic planning and enhance inter-agency coordination during crises. Moreover, AI's ability to simulate multiple decision outcomes under uncertainty supports adaptive and data-driven policymaking.

Enhancing Real-Time Situational Awareness in Defence and Internal Security: Another significant contribution of AI is its capacity to enhance real-time situational awareness in defence and internal security operations. AI-driven command and control systems integrate multiple data sources from sensors, surveillance drones, and social media to provide a unified operational picture [31]. This enables commanders and policymakers to make informed, timely, and precise decisions.

For example, AI-based geospatial intelligence (GEOINT) systems process satellite imagery to monitor conflict zones, detect troop mobilizations, or assess environmental threats. In internal security, AI tools can detect anomalies in network communications or crowd behaviour, assisting agencies such as the Department of State Services (DSS) and Nigerian Police Force (NPF) in identifying early signs of unrest. These systems strengthen Nigeria's national situational awareness architecture, which is essential for both proactive defence and disaster response management.

Furthermore, AI's integration into cybersecurity operations enables automated detection of malicious activity, pattern recognition of attack vectors, and incident response coordination. When linked to national threat databases, such systems enhance the efficiency of real-time threat intelligence and cyber resilience.

Table 3: AI-Enabled Strategic Decision-Making Models

Model	AI Techniques Used	Core Function	Applications in National Security	Relevance to Nigeria
Intelligent Decision Support Systems (IDSS)	Machine Learning, NLP, Expert Systems	Integrates data from multiple sources for decision-making	Intelligence analysis, crisis response, policy modelling	Supports data-driven defence planning
Predictive Risk Analytics (PRA)	Neural Networks, Bayesian Inference	Forecasts future events and threat probabilities	Conflict prediction, cyber threat detection, economic security	Enables proactive crisis management
Geospatial Intelligence Systems (GEOINT)	Computer Vision, Deep Learning	Analyses spatial and satellite imagery	Border surveillance, troop movement tracking	Enhances situational awareness in conflict zones
Autonomous Decision Simulation (ADS)	Reinforcement Learning, Multi-Agent Systems	Simulates alternative decision outcomes	Military scenario modelling, policy testing	Assists in evaluating national security strategies
Cognitive Analytics Platforms (CAP)	NLP, Knowledge Graphs	Synthesizes unstructured text data into insights	Intelligence synthesis, diplomatic briefings	Strengthens strategic analysis and knowledge retrieval

Source: Compiled by the Author from [1, 30, 32, 20].

Implications for Nigeria's National Security and Strategic Studies

The integration of Artificial Intelligence (AI) into Nigeria's national security and strategic decision-making architecture carries transformative potential for intelligence operations, defence management, and national governance. As the nature of conflict evolves from conventional warfare to hybrid and information-based threats, AI serves as a force multiplier, enhancing the efficiency, speed, and precision of decision-making in complex and volatile environments. The implications of AI transcend military applications, extending into cyber defence, governance, and the preservation of institutional knowledge essential for long-term strategic planning.

AI as a Force Multiplier in Intelligence Gathering and Defence Operations: AI operates as a strategic enabler within modern intelligence and defence ecosystems by augmenting human capabilities and expanding the reach of national security institutions. Through machine learning (ML), natural language processing (NLP), and computer vision, AI systems can process and interpret vast amounts of data from satellite imagery and intercepted communications to social media activity faster and more accurately than human analysts [31].

For Nigeria, where security challenges range from insurgency in the North-East to banditry and cyber threats, AI can provide actionable intelligence through automated data fusion and pattern recognition. For instance, AI-powered surveillance drones and geospatial mapping tools can monitor conflict-prone zones, identify patterns of terrorist movement, and predict ambush points. Similarly, sentiment analysis tools can track online radicalisation trends or disinformation campaigns targeting national stability [29].

Digital Sovereignty and Cyber Defence Imperatives: The increasing digitisation of Nigeria's defence and intelligence systems underscores the urgency of digital sovereignty the capacity of a nation to control and protect its data infrastructure and cyber ecosystem. AI, while a strategic asset, also introduces new vulnerabilities. The reliance on external technologies, foreign cloud infrastructure, and imported algorithms creates dependencies that may compromise national autonomy [20].

AI-powered cybersecurity tools such as anomaly detection algorithms, threat intelligence platforms, and automated response systems are critical for identifying and neutralising cyberattacks in real time. These systems can detect deviations in network behaviour, trace digital footprints of adversaries, and prevent data exfiltration from sensitive institutions. However, building indigenous AI capacity is essential to avoid external manipulation of national data streams.

Nigeria must therefore invest in AI sovereignty, which entails developing domestic AI models, secure data centres, and encryption standards aligned with national defence priorities. This approach will not only strengthen cyber resilience but also ensure the protection of sensitive intelligence and governance records that form the backbone of strategic continuity.

Challenges and Policy Gaps

Despite the transformative potential of Artificial Intelligence (AI) for knowledge preservation and national security in Nigeria, several institutional, technical, and policy-related challenges undermine its effective integration into the country's strategic architecture. These challenges cut across governance deficiencies, infrastructural inadequacies, ethical ambiguities, and human capital constraints, all of which weaken Nigeria's capacity to harness AI for sustainable national development and security enhancement.

a) **Absence of a Comprehensive AI Policy Framework:** Nigeria currently lacks a nationally coordinated AI policy that clearly defines objectives, ethical standards, and accountability mechanisms for AI deployment in security and governance [20]. While initiatives such as the National Digital Economy Policy and Strategy 2020-2030 and National Artificial Intelligence Policy Draft 2023 exist, they remain fragmented and largely unimplemented. The absence of a robust legislative and institutional framework leaves critical gaps in data governance, algorithmic transparency, and civilian oversight of AI use within security institutions.

b) **Inadequate Digital and Data Infrastructure:** AI technologies rely heavily on data quality, availability, and storage capacity, yet Nigeria's digital infrastructure remains underdeveloped. Limited broadband penetration, unstable power supply, and insufficient high-performance computing facilities constrain real-time data processing and secure storage of classified information [10]. Moreover, weak cyber resilience exposes critical data to breaches, manipulation, or loss, thereby threatening national intelligence continuity and institutional memory [33].

c) **Human Capital Deficit and Skill Gaps:** There is a significant shortage of skilled professionals in AI engineering, data science, and cybersecurity within Nigeria's defence, intelligence, and academic sectors. Most security personnel lack the technical expertise to operate, interpret, or maintain AI systems effectively [26]. This human capital deficit limits local innovation and deepens dependence on foreign technology providers, raising national sovereignty concerns.

d) **Ethical, Legal, and Privacy Concerns:** The integration of AI into security operations raises profound ethical and privacy dilemmas. Issues such as algorithmic bias, mass surveillance, and data misuse could erode civil liberties and public trust if not properly regulated [1]. Nigeria lacks specific legislation governing AI ethics, data protection, and accountability mechanisms for misuse by state actors, despite adopting the Nigeria Data Protection Act 2023. Without ethical safeguards, the risk of abuse in intelligence gathering and surveillance remains high.

e) **Fragmented Institutional Coordination:** The lack of inter-agency coordination among the Ministry of Defence, Office of the National Security Adviser (ONSA), National Information Technology Development Agency (NITDA), and National Intelligence Agency (NIA) results in duplication of efforts and fragmented knowledge management systems. This institutional fragmentation prevents the establishment of unified AI-driven intelligence repositories and undermines the creation of a national security data-sharing ecosystem.

Conclusion and Recommendations

This study examined the intersection of Artificial Intelligence (AI), knowledge preservation, and national security in Nigeria, emphasising how AI technologies can transform strategic decision-making and strengthen institutional memory. The findings reveal that AI possesses immense potential to revolutionise how states collect, store, process, and utilise knowledge for national defence and governance.

The study therefore made these strategic recommendations that would enhance Nigeria's capacity to leverage Artificial Intelligence (AI) for knowledge preservation and national security:

a) Develop a National AI and Knowledge Preservation Strategy: For a more concrete development and implementation plan for a national AI and knowledge preservation policy, there should be: (i) the establishment of a central coordinating body under the Office of the National Security Adviser, (ii) digitisation and standardisation of legacy archives across security agencies, (iii) capacity development through targeted training in data science and knowledge management for intelligence personnel, and (iv) inter-agency data-sharing protocols supported by secure AI-enabled platforms.
b) Strengthen Digital Infrastructure and Data Sovereignty: To safeguard sensitive intelligence and national data, Nigeria must invest in secure data centres, cloud architecture, and sovereign digital infrastructure. This includes local data hosting and encryption technologies that prevent overreliance on foreign AI systems and ensure national control over digital assets. The study clarifies that AI deployment in Nigeria's security sector need not rely exclusively on high-bandwidth, cloud-dependent systems. Specifically, the paper discusses the feasibility of hybrid and low-resource AI architectures, including offline-first systems, edge computing, and localised data centres that can operate with intermittent connectivity. It further recommends the use of energy-efficient AI models, scheduled batch processing during periods of power availability, and deployment within already secured facilities with alternative power sources (such as military bases and intelligence headquarters).
c) Institutionalise AI Ethics and Governance Frameworks: The adoption of AI in national security must be guided by ethical standards, transparency, and human oversight. Nigeria should establish an AI Ethics and Oversight Commission to regulate usage, prevent algorithmic bias, and promote accountability in military, intelligence, and public governance systems [20]. The study proposes specific legislative and regulatory measures, including the enactment of a National Data Protection and Algorithmic Accountability Framework tailored to security institutions. Proposed safeguards include mandatory algorithmic audits, independent oversight mechanisms involving the judiciary and legislature, clearly defined limits on surveillance use, and strict penalties for unauthorised data exploitation. The paper also recommends embedding human-in-the-loop decision-making structures to ensure that AI systems augment rather than replace human judgment in security operations.
d) Capacity Building and Research Collaboration: The Nigerian Defence Academy (NDA), universities, and research institutes should collaborate with global AI hubs to train experts in AI for defence, data science, and cybersecurity. Promoting indigenous AI research and development (R&D) will enhance local innovation and reduce dependency on imported technologies.
e) Policy Integration and Inter-Agency Coordination: National security institutions should integrate AI into existing knowledge management systems, promoting collaboration between agencies such as the Defence Headquarters, the National Intelligence Agency (NIA), and the Office of the National Security Adviser (ONSA). Shared intelligence frameworks would improve decision speed and operational effectiveness.

References

[1] L. Floridi, *The Logic of Information: A Theory of Philosophy as Conceptual Design*. Oxford University Press, 2018.
[2] M. J. Bates, "Preserving digital knowledge in the age of artificial intelligence," *Information Research*, vol. 26, no. 1, pp. 1–15, 2021.
[3] M. Taddeo and L. Floridi, "How AI can be a force for good," *Science*, vol. 361, no. 6404, pp. 751–752, 2018.
[4] B. A. Omodunbi, S. O. Esan, and A. Olaniyan, "Cybersecurity and data protection in Nigeria: Policy gaps and implementation challenges," *African Security Review*, vol. 31, no. 1, pp. 45–63, 2022.
[5] A. Oluwafemi and B. Olayinka, "Institutional memory and data governance in Nigeria's public sector," *African Journal of Governance and Development*, vol. 10, no. 2, pp. 101–120, 2021.
[6] R. Kapoor, P. Singh, and G. Kaur, "AI-based archival preservation: Opportunities and risks," *Journal of Digital Heritage*, vol. 12, no. 4, pp. 55–72, 2023.
[7] T. Adeleke, "Digital governance and cybersecurity in Nigeria: Challenges and opportunities," *Journal of African Digital Policy*, vol. 6, no. 2, pp. 34–52, 2022.
[8] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed. Pearson, 2020.
[9] V. C. Muller, "Ethics of Artificial Intelligence," in *The Stanford Encyclopedia of Philosophy*, 2021.
[10] K. Wiig, *Knowledge Management Foundations: Thinking about Thinking*. Arlington, TX: Schema Press, 1999.
[11] I. Nonaka and H. Takeuchi, *The Knowledge-Creating Company*. Oxford University Press, 1995.
[12] G. Allison and P. Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis*. New York: Longman, 1999.
[13] T. Adejumo, *Cybersecurity and Data Governance in Nigeria: Emerging Trends and Challenges*. Lagos: Spectrum Books, 2023.
[14] M. Libicki, *What is Information Warfare?* National Defense University Press, 1995.
[15] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed. Pearson, 2021.
[16] D. Jurafsky and J. H. Martin, *Speech and Language Processing*, 3rd ed. Pearson, 2023.
[17] M. Taddeo and L. Floridi, "How AI can be a force for good," *Science*, vol. 361, no. 6404, pp. 751–752, 2018.
[18] NITDA, *National Artificial Intelligence Strategy for Nigeria*. Federal Ministry of Communications, Innovation and Digital Economy, 2023.
[19] UNESCO, *Recommendation on the Ethics of Artificial Intelligence*. Paris: UNESCO, 2021.
[20] UNESCO, *AI and the Future of Knowledge: Towards Sustainable Digital Infrastructures*. Paris, 2023.
[21] World Economic Forum, *AI Governance and the Future of Digital Sovereignty*. Geneva: WEF, 2022.
[22] World Economic Forum, *Global Cybersecurity Outlook*. Geneva, 2022.
[23] World Economic Forum, *Harnessing Artificial Intelligence Responsibly for the Fourth Industrial Revolution*. Geneva: WEF, 2022.
[24] M. Lowenthal, *Intelligence: From Secrets to Policy*, 8th ed. CQ Press, 2019.
[25] J. J. Bryson, *The Ethics of Artificial Intelligence*. Oxford University Press, 2021.
[26] T. Adebayo, *Digital Governance and Institutional Memory in Nigeria's Public Sector*. Lagos: Centre for Policy Studies, 2022.
[27] B. Omitola, "Policy Amnesia and Governance Failure in Nigeria," *African Journal of Public Policy*, vol. 12, no. 3, pp. 45–58, 2021.
[28] J. Clark, *Artificial Intelligence and National Security Decision-Making*. RAND Corporation, 2020.

[29] T. Adebayo, *Artificial Intelligence and Defence Modernisation in Africa: Challenges and Opportunities*. Abuja: Defence Policy Review Series, 2023.
[30] H. Hassani, X. Huang, and E. Silva, "Big Data and Artificial Intelligence in National Security," *Technological Forecasting & Social Change*, vol. 155, p. 119988, 2020.
[31] M. C. Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," *Texas National Security Review*, vol. 1, no. 3, pp. 36–57, 2018.
[32] UNESCO, *Recommendation on the Ethics of Artificial Intelligence*. Paris: UNESCO Publications, 2023.
[33] C. Eze, "Institutional Memory and Knowledge Preservation in African Public Institutions," *African Governance Review*, vol. 5, no. 2, pp. 45–62, 2022.