International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 4, July-Aug-2026, ISSN (Online): 2395-566X

Artificial Intelligence and National Security Governance in Africa: A Comparative Study of Nigeria, South Africa, Kenya, Rwanda and Egypt

Paul 'Seun Sosina
PhD, fsi, mni
&
Odebiyi Olusola James, PhD

Abstract — Artificial intelligence is transforming national security governance by strengthening intelligence gathering, threat detection, border surveillance, cybersecurity, crime prevention and conflict early warning. However, its deployment across Africa raises concerns about privacy, algorithmic bias, accountability, misinformation, institutional readiness and technological dependence. This study examined artificial intelligence and national security governance in Africa through a comparative analysis of Nigeria, South Africa, Kenya, Rwanda and Egypt. Anchored in Technology Domestication Theory, the study adopted a qualitative multiple-case design. Data were obtained through documentary analysis of peer-reviewed studies, national policies, legislative frameworks, security strategies and African Union policy documents. The data were analysed using thematic synthesis and comparative policy analysis. Findings revealed that AI improves data processing, threat identification, surveillance capability and proactive security decision-making, although the scale of adoption varies across the five countries. Egypt and Rwanda demonstrate centralized policy arrangements, while Kenya and South Africa possess digital ecosystems but face implementation and regulatory challenges. Nigeria's adoption is constrained by infrastructure deficiencies, institutional responsibilities and technical capacity. Shared challenges include inadequate oversight, poor data quality, skills shortages, algorithmic bias, privacy risks and dependence on foreign technologies. The study concludes that effective AI-supported security requires context-sensitive governance grounded in human rights, democratic accountability, strategic autonomy and human oversight. It recommends risk-based regulation, oversight, impact assessments, indigenous capacity development, stronger data protection and harmonized standards.

Keywords— Artificial intelligence, national security governance, security governance, technology domestication, Africa.

I. INTRODUCTION

The creation of machines with in-built capacities to assess situations and make autonomous intelligent decisions represents a fundamental shift in how states approach security governance (Falode et al., 2025). As threats have become increasingly sophisticated and transnational, traditional security frameworks predicated on human intelligence, conventional surveillance, and reactive responses have proven inadequate in addressing the scale, speed, and complexity of modern security challenges (Donald et al., 2025). In Africa, AI is increasingly important in national security governance because the continent faces several security challenges, including terrorism, insurgency, banditry, cybercrime, maritime insecurity, and violent extremism (Donald et al., 2025; Rufus, 2024). These challenges are compounded by weak institutional capacity, porous borders, limited resources, and in some cases, authoritarian governance structures that exploit security narratives to consolidate power (Yelwa & Umar, 2025). The African Union has recognized AI's strategic importance, endorsing the Continental Artificial Intelligence Strategy in July 2024 as a framework for responsible AI adoption across the continent (African Union, 2024). This strategy emphasizes the potential of AI to contribute to Agenda 2063 and the Sustainable Development Goals, while acknowledging the governance challenges that accompany technological integration. Several African nations have developed national AI strategies or policies, including Egypt, Rwanda, South Africa, Kenya, Nigeria, and Mauritius, reflecting growing recognition of AI's importance for national development and security (OECD, 2026; Falode et al., 2025). The increasing deployment of AI-driven surveillance technologies, often sourced from authoritarian powers such as China and Russia, raises profound concerns about digital authoritarianism, civil liberties, and democratic accountability (Yelwa & Umar, 2025).

Across the continent, security architectures are actively experimenting with algorithmic tools to bridge operational deficits. Machine learning models, predictive analytics, natural language processing (NLP), and autonomous aerial systems are

being integrated into military logistics, intelligence synthesis, border control, and conflict early warning networks (Bor & Koech, 2023; Sayler, 2020; Zakari, 2024). In countries like Nigeria, South Africa, Kenya, Rwanda, and Egypt, AI systems are expanding institutional capabilities by enabling real-time metadata analysis, enhancing threat detection, automating tax and civil registries, and protecting critical digital infrastructure against cyber intrusions (Adedigba, 2026; Irambona et al., 2025; Nibigira et al., 2024; Zisengwe, 2025). However, these technological advances occur alongside acute vulnerabilities, including severe algorithmic bias, lack of human oversight, infrastructure gaps, and the unchecked proliferation of AI-generated deepfakes and political disinformation (Chinagorom et al., 2025; Effoduh et al., 2024; Ogbe et al., 2025). To capture these dynamic operational realities and governance tensions, this study provides a comprehensive analysis of artificial intelligence and national security governance in Africa. It investigates how state security apparatuses deploy AI tools across critical operational domains, critically evaluates the accompanying ethical and legal risks, and assesses the policy responses emerging at both continental and national levels. By grounding the inquiry in empirical evidence from five pivotal countries, namely Nigeria, South Africa, Kenya, Rwanda and Egypt, the study establishes a basis for understanding how African countries can balance technological modernization with democratic oversight, human rights protection and strategic data sovereignty.

II. STATEMENT OF THE PROBLEM

Artificial intelligence is increasingly being adopted within African security systems to support intelligence gathering, threat detection, border surveillance, cybersecurity, crime prevention and conflict early warning. Technologies such as predictive analytics, facial recognition, automated surveillance and unmanned aerial systems offer opportunities to strengthen responses to terrorism, insurgency, banditry, cybercrime and transnational organized crime (Adedigba, 2026; Donald et al., 2025; Falode et al., 2025). However, this adoption is occurring within institutional environments characterized by uneven regulatory capacity, inadequate infrastructure, technical skills shortages and weak accountability mechanisms (Jatau et al., 2025; Yilma & Wodajo, 2026). Consequently, AI-enabled security operations raise concerns about privacy, algorithmic bias, misinformation, transparency, human oversight and the protection of citizens' rights (Bor & Koech, 2023; Chinagorom et al., 2025; Ogbe et al., 2025). Existing studies have examined different aspects of AI and security governance. Donald et al. (2025) and Falode et al. (2025) investigated AI applications within Nigeria's national security architecture, while Nibigira et al. (2024) examined AI adoption for cybersecurity in Africa. Bor and Koech (2023) considered AI-enabled border surveillance and its human-rights implications. Similarly, Badawy (2025) assessed Egypt's national AI strategy, while Zisengwe (2025) examined AI governance and digital democracy in South Africa. Nevertheless, most existing studies focus on individual countries or specific technological applications. Limited comparative evidence explains how differences in institutional capacity, political systems, digital readiness, regulatory development and technological dependence influence the adoption and governance of AI across African national security institutions.

It therefore remains unclear how AI is being deployed across different security functions, what governance risks accompany its adoption and whether existing national and continental frameworks provide adequate safeguards. Dependence on foreign technologies also raises concerns about strategic autonomy, data sovereignty and the suitability of imported systems for African security environments (Nibigira et al., 2024; Yelwa & Umar, 2025). Against this background, the study comparatively examines Nigeria, South Africa, Kenya, Rwanda and Egypt. It seeks to address the gap between operational AI adoption and accountable governance and provide evidence for developing context-sensitive frameworks that promote security effectiveness while protecting human rights, democratic accountability and national data sovereignty.

Research Questions

The study is guided by the following research questions:

- How are AI technologies deployed across selected national security functions in Nigeria, South Africa, Kenya, Rwanda and Egypt?
- What ethical, legal, institutional and technical risks arise from the deployment of AI in national security operations?
- How do AI adoption, institutional readiness and governance approaches compare across the five selected countries?
- What continental and country-specific frameworks are required to ensure responsible, accountable and rights-based AI deployment in African national security governance?

Research Objectives

The general objective of the study is to examine artificial intelligence and national security governance in Africa through a comparative analysis of Nigeria, South Africa, Kenya, Rwanda and Egypt. The specific objectives are to:

- Examine the deployment of AI technologies across selected national security functions in Nigeria, South Africa, Kenya, Rwanda and Egypt.

- Assess the ethical, legal, institutional and technical risks associated with AI-enabled national security operations.
- Compare AI adoption, institutional readiness and governance approaches across the five selected countries.
- Propose continental and country-specific frameworks for responsible, accountable and rights-based AI deployment in African national security governance.

III. CONCEPTUAL FRAMEWORK

Concept of Artificial Intelligence

Artificial intelligence refers to the simulation of human intelligence processes by machines, particularly computer systems capable of learning, reasoning and decision-making without direct human input (Mannuru et al., 2023). The term was first coined by John McCarthy in 1956, who defined it as "the science and engineering of making intelligent machines" (Hoadley & Lucas, 2018). Since then, the concept has evolved to encompass a range of technologies and approaches. For the purposes of this study, AI is an artificial system developed in computer software, physical hardware, or other contexts that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action (Sayler, 2020). Key components of AI relevant to security governance include:

Machine Learning: A subset of AI that enables systems to learn and improve from experience without being explicitly programmed. Machine learning uses statistical techniques to allow computers to identify patterns in data and make predictions or decisions (Russell & Norvig, 2021).

Facial Recognition: AI systems that identify or verify individuals from digital images or video frames. These systems use deep learning algorithms to analyze facial features and match them against databases of known individuals (Nsude, 2022).

Predictive Analytics: The use of data, statistical algorithms and machine learning techniques to identify the likelihood of future outcomes based on historical data. In security governance, predictive analytics is used to forecast crime patterns, identify potential security threats and optimize resource allocation (Donald et al., 2025).

Natural Language Processing (NLP): AI systems that enable computers to understand, interpret and generate human language. NLP is used in security contexts for analyzing communications, detecting threats in textual data and enabling multilingual intelligence operations (Mannuru et al., 2023).

Automated Decision-Making: AI systems that make decisions or recommendations without direct human intervention. These systems are increasingly used in security contexts for threat assessment, resource allocation and operational planning (Sayler, 2020).

Concept of National Security Governance

National security governance refers to the institutions, policies, laws, processes and accountability mechanisms used to manage national security (Yilma & Wodajo, 2026). This concept encompasses the full range of state activities related to protecting national sovereignty, territorial integrity and the safety of citizens from internal and external threats. Security governance includes military operations, intelligence activities, law enforcement, border management and emergency response, as well as the legal and institutional frameworks that structure these activities (Jatau et al., 2025; van Eekelen, 2010). Many African states inherited centralized, authoritarian security systems from colonial powers, which were designed for control rather than democratic accountability (Olonisakin, 2008; Aning, 2015). These systems have often been modified to serve regime security rather than public safety, leading to opaque, unaccountable security institutions that prioritize regime survival over citizen welfare (Yelwa & Umar, 2025). Contemporary African security governance occurs within a complex landscape of threats, including terrorism, insurgency, organized crime, cybercrime, maritime insecurity and ethnic and religious violence. These threats are increasingly transnational in nature, requiring coordination across national borders and between different security institutions (Adedigba, 2026).

The concept of security governance has expanded beyond traditional state-centric approaches to encompass broader concerns about human security, including economic security, food security, health security and environmental security (Buzan, 1991). This expanded conception recognizes that security threats are multidimensional and require comprehensive responses that address root causes rather than merely symptoms. AI technologies have the potential to support this broader security agenda by enabling more effective monitoring, analysis and response to complex security challenges. However, the expansion of security governance to encompass AI technologies also raises concerns about accountability, transparency and democratic control. Security institutions have historically operated with limited public scrutiny and the introduction of AI systems may further complicate oversight and accountability (Yilma & Wodajo, 2026).

Relationship Between Artificial Intelligence and National Security Governance

AI significantly enhances security decision-making by enabling faster, more accurate threat assessments and more efficient resource allocation. AI systems can process vast amounts of data from diverse sources, identifying patterns and anomalies that human analysts might miss (Donald et al., 2025). This capability enables more proactive security approaches, where threats are identified and addressed before they escalate into crises. Predictive analytics is used to forecast terrorist activities, identify crime hotspots and optimize the deployment of security personnel (Boulanin & Verbruggen, 2017).

In terms of institutional coordination, AI can support integration across different security agencies by providing shared situational awareness and enabling real-time information sharing. AI-driven platforms can synthesize data from multiple sources, creating a common operating picture that enhances inter-agency coordination and reduces information silos (Sayler, 2020).

AI also affects threat identification by enabling more sophisticated surveillance, monitoring and analysis. AI-powered surveillance systems can continuously monitor vast geographic areas, detect suspicious activities and identify potential threats in real time (Nsude, 2022). This capability is particularly valuable in contexts where security forces are overstretched and unable to maintain constant vigilance. However, the expansion of AI-enabled surveillance raises concerns about privacy, civil liberties and the potential for abuse by authoritarian regimes (Yelwa & Umar, 2025).

Public accountability is a critical dimension of AI's relationship with security governance. The use of AI in security contexts creates new accountability challenges, as decisions made by algorithmic systems may be difficult to explain or challenge. Ensuring that AI systems are transparent, explainable and subject to oversight is essential for maintaining public trust and democratic accountability (Effoduh, Akpudo, & Kong, 2024). The protection of citizens' rights is another key consideration in the relationship between AI and security governance. AI systems can be used to monitor citizens, track their movements and analyze their behavior, potentially infringing on privacy and other fundamental rights. In authoritarian contexts, AI-enabled surveillance may be used to suppress dissent and consolidate political control (Yelwa & Umar, 2025).

Applications of Artificial Intelligence in National Security

Intelligence and Threat Detection

AI is changing intelligence gathering by enabling security institutions to process large volumes of data and identify emerging threats more efficiently. This represents a shift from traditional approaches based mainly on human intelligence, signals intelligence and manual analysis (Donald et al., 2025). Modern intelligence sources include satellite imagery, intercepted communications, radar signals, social media and open-source information. Machine learning, deep learning and natural language processing can classify, translate and analyse these diverse datasets more rapidly than manual methods (Sayler, 2020).

Donald et al. (2025) identify AI as an important means of addressing limitations in Nigeria's traditional intelligence methods and improving access to timely security information. Machine-learning systems can examine communication metadata, financial transactions and travel patterns to detect anomalies associated with security threats (Falode et al., 2025). AI also strengthens open-source intelligence through the analysis of social media, news reports and other digital platforms. Natural language processing facilitates the analysis of multilingual content across Africa's diverse linguistic environment (Mannuru et al., 2023). Nevertheless, limited training data, infrastructure deficiencies, technical skills shortages and difficulties in explaining AI-generated findings constrain effective adoption (Falode et al., 2025). Privacy, civil-liberty and accountability concerns also require careful attention.

Surveillance and Border Security

AI strengthens surveillance and border management through facial recognition, biometric identification, drones, smart cameras and automated monitoring systems (Bor & Koech, 2023). Nsude (2022) identifies AI-enabled facial recognition as a technology that can assist Nigerian law-enforcement and counterterrorism operations by improving the identification and monitoring of security threats. In South Africa, the growing application of facial recognition within policing and surveillance generates concerns about privacy and possible misuse (Zisengwe, 2025). When integrated with fingerprint and iris-scanning systems, AI can improve identity verification, reduce identity fraud and increase the efficiency of border-control processes (Bor & Koech, 2023).

AI-powered drones and smart cameras can monitor remote border areas and provide timely information about suspicious activities (Brundage et al., 2018). Falode et al. (2025) identify drone surveillance as an important tool for border monitoring and counterinsurgency operations in Nigeria. Foreign

technology companies, including Chinese firms such as Huawei and ZTE, facilitate access to advanced surveillance and biometric systems across Africa (Yelwa & Umar, 2025). Although these partnerships expand technological capacity, they also raise concerns about data sovereignty, foreign influence and technological dependence. Where legal safeguards are inadequate, AI-enabled surveillance may facilitate mass monitoring, unauthorized data collection and political repression (Bor & Koech, 2023; Yelwa & Umar, 2025).

Cybersecurity and Crime Prevention

AI strengthens cybersecurity by enabling governments and organizations to detect, prevent and respond to cyber threats more rapidly. Machine-learning systems analyse network traffic, identify unusual behaviour and adapt to evolving cyber risks more effectively than conventional rule-based systems (Nibigira et al., 2024). AI-powered tools can detect malware, phishing, ransomware and related threats before they cause extensive damage (Brundage et al., 2018). They can also identify abnormal data access, alert cybersecurity personnel and automate selected incident-response processes (Nibigira et al., 2024).

In Nigeria, AI offers important capabilities for strengthening cybersecurity and protecting critical infrastructure. In South Africa, machine-learning applications assist threat detection across government, finance and critical infrastructure, although institutional adoption remains uneven (Zisengwe, 2025). AI also contributes to crime prevention through predictive analysis of crime patterns and video analytics. Adedigba (2026) examines its application to security operations addressing banditry and insurgency in Nigeria. Similarly, AI-powered video analytics can identify suspicious activities and facilitate timely intervention (Chinagorom et al., 2025). However, limited technical expertise, poor infrastructure, inadequate training data and privacy concerns constrain adoption (Nibigira et al., 2024). The dual-use nature of AI also allows the same technologies to serve both defensive and harmful purposes.

Conflict Early-Warning Systems

AI can strengthen conflict early-warning systems through the analysis of social, political, economic, environmental and digital information. These systems identify warning signs and provide timely information to decision-makers (Falode et al., 2025). AI-assisted analysis can improve the Continental Early Warning System established under the African Peace and Security Architecture by detecting complex patterns associated with emerging conflicts (Oluyemi, 2025).

Machine-learning systems analyse satellite imagery, social media, news reports and economic indicators to detect patterns associated with rising tensions, military activity, instability and hate speech (Chinagorom et al., 2025). Natural language processing and sentiment analysis identify emerging narratives, disinformation and inflammatory content that may contribute to conflict escalation (Oluyemi, 2025). AI can also combine climate information, resource availability and demographic trends to assess conflict risks arising from environmental pressures and competition for scarce resources (Falode et al., 2025).

African security institutions integrate AI into conflict early-warning systems at different levels. Data scarcity, infrastructure deficiencies, technical complexity and limited institutional capacity continue to constrain its application (Oluyemi, 2025). Inaccurate predictions or missed warning signs may also create serious consequences. Therefore, AI-enabled early-warning systems require reliable data, transparent models, regular testing, institutional validation and meaningful human oversight (Chinagorom et al., 2025).

IV. ARTIFICIAL INTELLIGENCE GOVERNANCE CHALLENGES IN AFRICA

Privacy and Mass Surveillance

The deployment of AI-driven surveillance technologies across Africa has raised significant concerns about privacy, unlawful surveillance, consent, civil liberties, and the potential misuse of security technologies. AI-powered surveillance systems have the capacity to collect, store, and analyze vast amounts of data about individuals, enabling mass surveillance without individualized suspicion or consent (Bor & Koech, 2023). The deployment of these technologies has often occurred without robust legal frameworks or transparent oversight mechanisms. While many African countries have data protection laws, enforcement is often weak and legal frameworks inadequately address AI-specific risks (Effoduh et al., 2024). The use of AI-driven surveillance by authoritarian regimes raises particularly serious concerns. In countries such as Uganda, Ethiopia, and Zimbabwe, surveillance technologies have been used to monitor political opponents, suppress dissent, and consolidate political control (Yelwa & Umar, 2025). The acquisition of surveillance systems from authoritarian powers, such as China and Russia, has facilitated these practices (Yelwa & Umar, 2025).

Facial recognition technology is a particular source of concern because of its potential to facilitate mass surveillance and discriminatory outcomes. According to Bor and Koech (2023),

facial recognition systems may produce higher error rates for certain demographic groups, particularly individuals with darker skin tones. The collection and processing of biometric data without adequate public awareness or consent also undermine privacy and the principle of informed consent (Effoduh et al., 2024). Addressing these concerns requires clear legal safeguards, transparent data-processing procedures, independent oversight and effective accountability mechanisms to ensure that facial recognition technologies are used only for legitimate and lawful security purposes (Yelwa & Umar, 2025).
Algorithmic Bias and Accountability

Algorithmic bias represents a fundamental challenge to the responsible deployment of AI in security governance. AI systems trained on biased or incomplete data can produce discriminatory outcomes, perpetuating and amplifying existing inequalities (Bor & Koech, 2023). In many African contexts, training data may not adequately represent population diversity, leading to systems that perform poorly for certain demographic groups (Bor & Koech, 2023). The lack of transparency in AI systems is a significant barrier to identifying and addressing algorithmic bias, as many complex deep learning models operate as "black boxes" (Chinagorom, Chika, & Nwigwe, 2025).

Accountability for automated decisions is another critical challenge. When AI systems make decisions affecting individuals, determining responsibility and providing redress for harm is often difficult (Bor & Koech, 2023). Human oversight is widely recognized as essential for ensuring AI systems operate within ethical and legal boundaries and for preventing harmful outcomes (Effoduh et al., 2024). Addressing algorithmic bias requires diverse representation in AI development, transparent and explainable systems, regular auditing, and mechanisms for accountability and redress (Bor & Koech, 2023).

Deepfakes and Misinformation
The growth of AI-generated content, particularly deepfake audio, video and images, threatens political stability, national security and social cohesion in Africa. Deepfakes can impersonate political leaders, fabricate events and manipulate public opinion by presenting false information as authentic. Kharvi (2024) explained that their realistic appearance makes detection difficult and threatens political discourse, institutional trust and personal security. In South Africa, AI-generated deepfakes and political disinformation have weakened public confidence in political actors and democratic institutions (Zisengwe, 2025).

AI-driven social media algorithms intensify misinformation by prioritizing engagement and repeatedly exposing users to information that confirms existing beliefs. This encourages echo chambers, political polarization and the rapid circulation of misleading content (Ogbe et al., 2025). In societies affected by ethnic, religious or political tensions, deepfakes may provoke conflict, damage reputations and weaken trust in institutions. Addressing these risks requires stronger legal frameworks, effective detection and content-verification technologies, media literacy, public awareness and cooperation among governments, technology companies, civil society and researchers (Kharvi, 2024; Ogbe et al., 2025).

Regulatory and Technical Limitations
The governance of AI in African security contexts is constrained by weak regulation, inadequate infrastructure, limited funding, skills shortages, poor data quality, institutional fragmentation, and dependence on foreign technologies. While some countries have developed data protection laws or AI strategies, the regulatory environment remains fragmented and often inadequate (Yilma & Wodajo, 2026). Infrastructure deficits, including limited access to reliable electricity, broadband connectivity, and computing infrastructure, significantly constrain AI adoption (Falode et al., 2025). Funding limitations restrict investment in AI technologies and technical capacity, delaying implementation and limiting operational effectiveness (Chinagorom et al., 2025). In Nigeria, macroeconomic instability, inadequate infrastructure, regulatory complexity and governance weaknesses may further limit investment in the electricity, connectivity, technical expertise and computing systems required for effective AI-enabled national security operations (Okegbemi, 2024).

Skills shortages are a persistent challenge, with limited technical expertise in AI constraining the ability to develop, deploy, and maintain AI systems (Nibigira et al., 2024). Poor data quality and limited data availability constrain the development of accurate and reliable AI systems (Falode et al., 2025). Institutional fragmentation and weak inter-agency coordination limit the effectiveness of AI-driven intelligence and predictive analytics (Oluyemi, 2025). Dependence on foreign technologies compromises strategic autonomy, raises concerns about data sovereignty, and perpetuates unequal power relations (Yelwa & Umar, 2025).

Challenges
The governance of AI in African security contexts is constrained by numerous challenges that span regulatory, technical, institutional and ethical dimensions. These challenges are not uniform across the continent, but certain patterns emerge across the five case study countries.

Infrastructure Deficits
Inadequate physical and digital infrastructure represents a fundamental constraint on AI adoption across Africa. Limited access to reliable electricity, broadband connectivity, and computing infrastructure significantly restricts the development and deployment of AI systems (Falode et al., 2025). In Nigeria, macroeconomic instability, inadequate infrastructure, regulatory complexity and governance weaknesses limit investment in the electricity, connectivity, technical expertise and computing systems required for effective AI-enabled national security operations (Okegbemi, 2024).

Technical Skills Shortages
Limited technical expertise in AI constrains the ability to develop, deploy, operate, audit and maintain AI systems (Nibigira et al., 2024; Chinagorom et al., 2025). This skills gap affects all stages of the AI lifecycle, from system design to routine operations and oversight. The shortage is particularly acute in security institutions, where technical capacity is often limited and competition for skilled personnel with the private sector is intense.

Data Quality and Availability
Poor data quality and limited data availability constrain the development of accurate and reliable AI systems (Falode et al., 2025). Many African countries lack comprehensive, high-quality datasets for training AI systems. Data may be fragmented, incomplete, unrepresentative or outdated. The lack of interoperable data systems across security institutions further limits the effectiveness of AI-driven intelligence and predictive analytics.

Institutional Fragmentation
Weak inter-agency coordination and institutional fragmentation limit the effectiveness of AI-enabled security operations (Chinagorom et al., 2025; Oluyemi, 2025). Security institutions often operate in silos, with limited information sharing and coordination. This fragmentation undermines the development of integrated intelligence and predictive capabilities that require data from multiple sources.

Regulatory Weaknesses
Weak regulatory frameworks and inadequate enforcement mechanisms constrain responsible AI governance (Yilma & Wodajo, 2026). While some countries have developed data protection laws or AI strategies, the regulatory environment remains fragmented and often inadequate. Many frameworks lack specific provisions for AI-enabled security operations and enforcement is often weak.

Privacy and Civil Liberties Concerns
The deployment of AI-enabled surveillance raises significant concerns about privacy and civil liberties (Bor & Koech, 2023; Zisengwe, 2025). AI-powered surveillance systems can enable mass monitoring, unauthorized data collection and political repression. In authoritarian contexts, AI-enabled surveillance may be used to suppress dissent and consolidate political control (Yelwa & Umar, 2025).

Algorithmic Bias
AI systems trained on biased or incomplete data can produce discriminatory outcomes, perpetuating and amplifying existing inequalities (Bor & Koech, 2023). Facial recognition systems may produce higher error rates for certain demographic groups, particularly individuals with darker skin tones. The lack of transparency in AI systems is a significant barrier to identifying and addressing algorithmic bias.

Accountability Gaps
The use of AI in security contexts creates new accountability challenges, as decisions made by algorithmic systems may be difficult to explain or challenge (Bor & Koech, 2023). Determining responsibility for automated decisions and providing redress for harm is often difficult. Human oversight is widely recognized as essential for ensuring AI systems operate within ethical and legal boundaries and for preventing harmful outcomes (Effoduh et al., 2024).

Technological Dependence
Dependence on foreign technologies compromises strategic autonomy, raises concerns about data sovereignty, and perpetuates unequal power relations (Yelwa & Umar, 2025). African countries often rely on foreign vendors for AI technologies, including surveillance systems from countries such as China and Russia. This dependence creates vulnerabilities related to data sovereignty, system control, and foreign influence.

Deepfakes and Misinformation
The growth of AI-generated content, particularly deepfake audio, video and images, threatens political stability, national security and social cohesion (Kharvi, 2024; Zisengwe, 2025). Deepfakes can impersonate political leaders, fabricate events and manipulate public opinion. AI-driven social media algorithms intensify misinformation by prioritizing engagement and repeatedly exposing users to information that confirms existing beliefs.

Prospects

Short-Term Prospects (1-2 Years)

In the immediate term, African states will focus on standardizing policy frameworks, addressing baseline infrastructure gaps, and deploying low-complexity AI systems for crisis management. Key developments will include:

Formalizing National Strategies: Lagging states will move to establish official policy guidelines, such as South Africa formalizing its draft National AI Policy Framework and Nigeria developing dedicated operational directives to harmonize inter-agency AI procurement (Department of Communications and Digital Technologies, 2024; Falode et al., 2025).

Targeted Operational Deployment: AI adoption will concentrate on high-priority security needs, particularly automated threat detection in cybersecurity networks, basic facial recognition at major ports of entry, and predictive modeling for counter-banditry and counter-terrorism operations (Adedigba, 2026; Irambona et al., 2025).

Inter-Agency Standardization: Initial administrative efforts will focus on reducing institutional silos by establishing inter-agency committees to streamline intelligence sharing and metadata processing (Donald et al., 2025).

Medium-Term Prospects (3-5 Years)

Over the medium term, efforts will pivot toward institutionalizing regulatory oversight, building specialized human capital, and enforcing ethical compliance mechanisms:
Operationalizing Specialized AI Regulators: States will transition from high-level policy statements to enforcing risk-based compliance models. This includes scaling framework tools like Egypt's "Dual-Check" model (combining Ethical Impact Assessments with Technical Conformity Assessments) and establishing independent auditing bodies to monitor high-risk deployments in law enforcement (Badawy, 2025; Egypt National AI Governance Framework, 2026).

Addressing Technical Skills Shortages: Sustained investments in specialized technical education, military R&D partnerships, and public-sector digital training will begin to bridge technical expertise gaps and mitigate brain drain across the security sector (Chinagorom et al., 2025; Rwigema, 2026).

Mandatory Algorithmic Auditing: Governments will mandate regular audits of training datasets to detect and reduce demographic and algorithmic bias, ensuring that automated decision-making in defense and law enforcement adheres to statutory data protection standards (Effoduh et al., 2024).

Long-Term Prospects (6-10 Years)

In the long term, African security architectures will aim for strategic digital autonomy, indigenous technological innovation, and harmonized continental integration:

Developing Indigenous AI Capabilities: African states will actively reduce overreliance on foreign technology exporters by funding domestic tech ecosystems, creating localized training datasets tailored to African languages and cultural contexts, and establishing sovereign defense computing infrastructure (Nibigira et al., 2024; Ogbe et al., 2025).

Continental Regulatory Harmonization: Full alignment with the African Union Continental Artificial Intelligence Strategy (2024) will emerge as Regional Economic Communities (RECs) operationalize binding legal standards, shared technical norms, and cross-border data-sharing protocols (African Union, 2024; Yilma & Wodajo, 2026).

Integrated Early Warning Architecture: Advanced AI models will be fully integrated into regional security apparatuses such as an upgraded Continental Early Warning System (CEWS) combining real-time satellite imagery, NLP sentiment analysis, and climate-resource data to predict and mitigate conflicts before escalation, supported by robust judicial oversight and human-in-the-loop safeguards (Oluyemi, 2025).

Comparative Lessons

An analysis of the empirical evidence across Nigeria, South Africa, Kenya, Rwanda, and Egypt yields critical comparative insights into how national security architectures domesticate and govern artificial intelligence:

Institutional Centralization Accelerates Regulatory Maturity

A prominent lesson is that political leadership and dedicated institutional anchors are prerequisites for coherent AI governance. Egypt and Rwanda demonstrate that centralized administrative oversight such as Egypt's National Council for AI, Quantum Computing and Emerging Technologies alongside the Egyptian Center for Responsible AI (ECRAI), and Rwanda's Ministry of ICT and Innovation working with RURA, enables the establishment of formal risk classification systems, clear policy directives, and structured public-sector integration (Egypt National AI Governance Framework, 2026; Rwigema, 2026). Conversely, states like Nigeria exhibit severe policy fragmentation and inter-agency coordination deficits, where isolated deployments by defense and intelligence units occur without unified procurement standards or centralized ethical oversight (Donald et al., 2025; Falode et al., 2025).

Constitutional Safeguards and Civic Tech Mitigate Digital Authoritarianism

Comparative evidence highlights the necessity of balancing technological modernization with democratic checks. South Africa and Kenya showed that robust constitutional frameworks, data protection acts (e.g., POPIA 2020 and Kenya's Data Protection Act 2019), and active civil society ecosystems serve as essential counterweights against unchecked state surveillance and digital authoritarianism (Bor & Koech, 2023; Zisengwe, 2025). Where judicial and civic oversight are weak, AI-powered surveillance technologies risk being weaponized to monitor political dissent and consolidate regime security over citizen safety (Yelwa & Umar, 2025).

Infrastructure Adequacy Directly Moderates Operational Impact

The case studies establish that advanced AI algorithms cannot compensate for foundational physical and digital infrastructure deficits. In Rwanda and South Africa, relatively reliable broadband connectivity and power grids have enabled functional applications in public service automation, revenue systems, and threat monitoring (Rwigema, 2026; Zisengwe, 2025). In contrast, persistent energy deficits, limited computing power, and low data quality in Nigeria and rural Kenya severely constrain real-time predictive analytics, counter-insurgency processing, and early warning responsiveness (Adedigba, 2026; Falode et al., 2025; Kenya AI Strategy, 2025).

Strategic Reliance on Foreign Tech Exporters Imperils Data Sovereignty

Across all five nations, reliance on foreign technology vendors, particularly from China, Russia, and the Global North exposes a shared vulnerability (Bor & Koech, 2023; Yelwa & Umar, 2025). While foreign partnerships facilitate rapid access to biometric platforms, smart cameras, and autonomous drones, they compromise strategic autonomy, create long-term operational dependencies, and raise critical risks concerning data sovereignty, unrepresentative algorithmic bias, and foreign geopolitical influence (Badawy, 2025; Nibigira et al., 2024).

Policy Framework Development Does Not Guarantee Implementation

The presence of a national AI strategy or data protection law does not automatically ensure responsible deployment in security contexts. Egypt has developed comprehensive governance frameworks but faces implementation challenges and gaps in independent oversight (Badawy, 2025). Similarly, Kenya's AI Strategy (2025-2030) provides a broad framework, but data limitations, infrastructure gaps and technical capacity constrain implementation (Kenya AI Strategy, 2025). South Africa's draft National AI Policy Framework outlines important governance principles, but its draft status limits legal enforcement (Department of Communications and Digital Technologies, 2024). Nigeria's National AI Strategy (2024) and National Centre for Artificial Intelligence and Robotics exist, but funding limitations, infrastructure deficiencies and fragmented responsibilities constrain coordinated integration within its national security architecture (Donald et al., 2025; Falode et al., 2025).

Regional Coordination Remains Limited

The African Union Continental Artificial Intelligence Strategy provides an important foundation for regional coordination, but its effectiveness depends on national implementation, measurable standards, adequate funding and monitoring mechanisms (African Union, 2024; Yilma & Wodajo, 2026). Cross-border cooperation in AI governance remains limited, and significant challenges exist in harmonizing national approaches. The African Union and regional economic communities should promote the harmonization of AI governance standards across the continent.

Theoretical Framework

This study is anchored in Technology Domestication Theory, developed by Silverstone and Hirsch (1992) and later extended to institutional settings (Haddon, 2007; Harwood, 2011). The theory argues that technologies do not enter societies or institutions as neutral tools. Instead, users acquire, interpret, modify and integrate them according to social values, political interests, institutional arrangements and material conditions. Technology adoption is an active and context-dependent process rather than a uniform outcome of advancement.

Domestication occurs through four stages: appropriation, objectification, incorporation and conversion (Silverstone et al., 1992):

- Appropriation concerns how security institutions acquire AI technologies, including facial recognition systems, predictive algorithms, surveillance platforms and unmanned aerial systems. In this study, it explains procurement choices, foreign technological dependence and data-sovereignty concerns.
- Objectification describes how acquired technologies are positioned within security policies, laws, institutional structures and development priorities.
- Incorporation examines how AI becomes embedded in intelligence gathering, border surveillance, cybersecurity, crime prevention and conflict early-warning routines.
- Conversion concerns how governments use AI capabilities to demonstrate effective security, modernization, strategic autonomy or regional leadership.

- The theory is relevant because Nigeria, South Africa, Kenya, Rwanda and Egypt possess different political systems, digital capabilities, security challenges and regulatory arrangements. These differences influence how AI technologies are acquired, governed and operationalized. Technology Domestication Theory therefore helps explain why similar technologies produce different institutional practices and governance outcomes across the five countries. It also clarifies how infrastructure limitations, technical skills shortages, fragmented institutions, algorithmic bias, weak oversight and foreign dependence may hinder responsible adoption (Nibigira et al., 2024; Yelwa & Umar, 2025).
- Accordingly, the theory guides the comparative analysis of AI deployment, institutional readiness, governance risks and policy responses. It enables the study to assess whether AI is responsibly integrated into national security institutions or adapted in ways that weaken accountability, human rights and data sovereignty.

V. METHODOLOGY

This study adopts a qualitative, multi-case study research design to examine the intersection of artificial intelligence and national security governance across Africa. Utilizing purposive sampling, five state contexts (Nigeria, South Africa, Kenya, Rwanda and Egypt) were selected based on their regional strategic significance, digital ecosystem maturity, distinct national security threat profiles, and varying stages of regulatory development.

Data collection relies on documentary analysis of secondary sources, including peer-reviewed academic literature, national security strategies, legislative frameworks, official AI policy documents, and continental guidelines issued by the African Union. Data analysis is conducted through qualitative thematic synthesis and comparative policy analysis, structured through the analytical lens of Technology Domestication Theory. This approach enables a systematic evaluation of how foreign AI capabilities are appropriated, objectified, incorporated, and converted within diverse national security architectures, benchmarking operational realities against emerging governance structures across the selected cases.

VI. DISCUSSION OF FINDINGS

Common Applications and Benefits

The findings show that Nigeria, South Africa, Kenya, Rwanda and Egypt apply AI to similar national security functions, including intelligence gathering, surveillance, border management, cybersecurity, crime prevention and conflict early warning. AI improves the processing of large datasets, identification of threat patterns and allocation of security resources. It also automates routine activities and supports more proactive security decision-making (Adedigba, 2026; Donald et al., 2025; Zisengwe, 2025). Beyond security operations, AI contributes to public-sector productivity and data-driven service delivery (Mhlanga, 2026; Rwigema, 2026). In intelligence operations, AI assists analysts in identifying patterns and anomalies across diverse data sources (Donald et al., 2025; Nibigira et al., 2024). Machine-learning systems also strengthen cybersecurity by detecting unusual network activity and adapting to changing cyber threats (Nibigira et al., 2024). Facial recognition, biometric identification and drone surveillance contribute to identity verification and border monitoring, although their use raises privacy and accountability concerns (Bor & Koech, 2023). In conflict early warning, AI analyses social, political, environmental and digital information to identify emerging signs of insecurity and inform preventive responses (Chinagorom et al., 2025; Oluyemi, 2025). Nevertheless, the level of institutional integration differs across the five countries.

Differences in Governance Approaches

The comparative findings reveal differences in national AI strategies, data-protection systems, institutional arrangements and regulatory readiness. Rwanda's 2022 National AI Policy emphasizes skills development, infrastructure, data governance, responsible adoption and ethical implementation (Republic of Rwanda, Ministry of ICT and Innovation, 2022). Egypt's national AI strategy similarly promotes institutional coordination and responsible AI development, although implementation and independent oversight require further strengthening (Badawy, 2025).

Kenya's AI Strategy 2025–2030 presents a broad framework for infrastructure, data, research, innovation and ethical governance. However, data limitations, infrastructure gaps and technical capacity constrain implementation (Kenya AI Strategy, 2025). South Africa's draft National AI Policy Framework outlines important governance principles, but its draft status limits legal enforcement (Department of Communications and Digital Technologies, 2024). Nigeria has established AI-related policies and institutions, but funding limitations, infrastructure deficiencies and fragmented responsibilities constrain coordinated integration within its national security architecture (Donald et al., 2025; Falode et al., 2025).

Data-protection arrangements also differ across the selected countries. Egypt's Personal Data Protection Law, Kenya's Data

Protection Act and South Africa's Protection of Personal Information Act provide important legal safeguards, although enforcement capacity remains uneven. Rwanda maintains a coordinated policy approach, while Nigeria's responsibilities are distributed across several institutions. These differences show that the existence of an AI strategy or data-protection law does not automatically guarantee responsible security-sector implementation. Effective governance also requires institutional capacity, enforcement mechanisms, technical standards and independent oversight.

Shared Challenges and Identified Gaps

Despite differences in governance readiness, the five countries experience several common challenges. Infrastructure deficits, including unreliable electricity, inadequate broadband connectivity and limited computing facilities, restrict the development and deployment of AI systems (Falode et al., 2025; Kenya AI Strategy, 2025). Technical skills shortages also reduce the ability of security institutions to design, operate, audit and maintain AI applications (Chinagorom et al., 2025; Nibigira et al., 2024).

Poor, fragmented and unrepresentative data may reduce system accuracy and produce biased outcomes (Falode et al., 2025). Weak interagency coordination, overlapping responsibilities and limited information sharing also constrain AI-enabled intelligence and predictive analysis (Chinagorom et al., 2025; Oluyemi, 2025). Although national AI strategies and data-protection laws exist in several countries, many frameworks do not fully address the risks associated with surveillance, automated decisions and security applications (Yilma & Wodajo, 2026).

Privacy, algorithmic bias and accountability remain major ethical concerns. Without adequate safeguards, AI-enabled security systems may undermine civil liberties or discriminate against particular groups (Bor & Koech, 2023; Zisengwe, 2025). Dependence on foreign vendors further raises concerns about data sovereignty, system control and strategic autonomy (Yelwa & Umar, 2025). Limited public understanding of AI also reduces meaningful participation in policy development. These findings demonstrate that responsible AI adoption depends not only on technological investment but also on effective regulation, institutional coordination, human oversight, local capacity and public accountability.

Comparative Lessons across Case Studies

An analysis of the empirical evidence across Nigeria, South Africa, Kenya, Rwanda, and Egypt yields critical comparative insights into how national security architectures domesticate and govern artificial intelligence:

Institutional Centralization Accelerates Regulatory Maturity: A prominent lesson is that political leadership and dedicated institutional anchors are prerequisites for coherent AI governance. Egypt and Rwanda demonstrate that centralized administrative oversight such as Egypt's National Council for AI, Quantum Computing and Emerging Technologies alongside the Egyptian Center for Responsible AI (ECRAI), and Rwanda's Ministry of ICT and Innovation working with RURA, enables the establishment of formal risk classification systems, clear policy directives, and structured public-sector integration (Egypt National AI Governance Framework, 2026; Rwigema, 2026). Conversely, states like Nigeria exhibit severe policy fragmentation and inter-agency coordination deficits, where isolated deployments by defense and intelligence units occur without unified procurement standards or centralized ethical oversight (Donald et al., 2025; Falode et al., 2025).

Constitutional Safeguards and Civic Tech Mitigate Digital Authoritarianism: Comparative evidence highlights the necessity of balancing technological modernization with democratic checks. South Africa and Kenya showed that robust constitutional frameworks, data protection acts (e.g., POPIA 2020 and Kenya's Data Protection Act 2019), and active civil society ecosystems serve as essential counterweights against unchecked state surveillance and digital authoritarianism (Bor & Koech, 2023; Zisengwe, 2025). Where judicial and civic oversight are weak, AI-powered surveillance technologies risk being weaponized to monitor political dissent and consolidate regime security over citizen safety (Yelwa & Umar, 2025).

Infrastructure Adequacy Directly Moderates Operational Impact: The case studies establish that advanced AI algorithms cannot compensate for foundational physical and digital infrastructure deficits. In Rwanda and South Africa, relatively reliable broadband connectivity and power grids have enabled functional applications in public service automation, revenue systems, and threat monitoring (Rwigema, 2026; Zisengwe, 2025). In contrast, persistent energy deficits, limited computing power, and low data quality in Nigeria and rural Kenya severely constrain real-time predictive analytics, counter-insurgency processing, and early warning responsiveness (Adedigba, 2026; Falode et al., 2025; Kenya AI Strategy, 2025).

Strategic Reliance on Foreign Tech Exporters Imperils Data Sovereignty: Across all five nations, reliance on foreign technology vendors, particularly from China, Russia, and the Global North exposes a shared vulnerability (Bor & Koech, 2023; Yelwa & Umar, 2025). While foreign partnerships facilitate rapid access to biometric platforms, smart cameras, and autonomous drones, they compromise strategic autonomy, create long-term operational dependencies, and raise critical

risks concerning data sovereignty, unrepresentative algorithmic bias, and foreign geopolitical influence (Badawy, 2025; Nibigira et al., 2024).

Policy Framework Development Does Not Guarantee Implementation: The presence of a national AI strategy or data protection law does not automatically ensure responsible deployment in security contexts. Egypt has developed comprehensive governance frameworks but faces implementation challenges and gaps in independent oversight (Badawy, 2025). Similarly, Kenya's AI Strategy (2025-2030) provides a broad framework, but data limitations, infrastructure gaps and technical capacity constrain implementation (Kenya AI Strategy, 2025). South Africa's draft National AI Policy Framework outlines important governance principles, but its draft status limits legal enforcement (Department of Communications and Digital Technologies, 2024). Nigeria's National AI Strategy (2024) and National Centre for Artificial Intelligence and Robotics exist, but funding limitations, infrastructure deficiencies and fragmented responsibilities constrain coordinated integration within its national security architecture (Donald et al., 2025; Falode et al., 2025).

Regional Coordination Remains Limited: The African Union Continental Artificial Intelligence Strategy provides an important foundation for regional coordination, but its effectiveness depends on national implementation, measurable standards, adequate funding and monitoring mechanisms (African Union, 2024; Yilma & Wodajo, 2026). Cross-border cooperation in AI governance remains limited, and significant challenges exist in harmonizing national approaches. The African Union and regional economic communities should promote the harmonization of AI governance standards across the continent.

VII. CONCLUSION

This study examined the deployment and governance of artificial intelligence within the national security systems of Nigeria, South Africa, Kenya, Rwanda and Egypt. The findings show that AI strengthens intelligence analysis, threat detection, border surveillance, cybersecurity, crime prevention and conflict early warning by improving data processing, pattern identification and security decision-making (Adedigba, 2026; Donald et al., 2025). However, its adoption also creates ethical, legal and institutional risks relating to privacy, algorithmic bias, misinformation, accountability and civil liberties (Bor & Koech, 2023; Effoduh et al., 2024; Ogbe et al., 2025).

The comparative analysis reveals uneven AI adoption and governance across the five countries. Egypt and Rwanda maintain relatively coordinated policy arrangements, while Kenya and South Africa possess developed digital ecosystems but face implementation and enforcement challenges. Nigeria's growing AI capabilities remain constrained by infrastructure limitations, technical skills shortages and fragmented institutional responsibilities. Despite these differences, all five countries experience common challenges involving data protection, human oversight, institutional capacity and dependence on foreign technologies.

From the perspective of Technology Domestication Theory, these variations demonstrate that AI technologies do not produce uniform outcomes. Their adoption and effects depend on how national institutions acquire, interpret, regulate and integrate them into security practices. Political priorities, regulatory capacity and technological resources therefore shape the benefits and risks associated with AI-enabled security.

The African Union Continental Artificial Intelligence Strategy provides an important foundation for regional coordination and responsible AI adoption, but its effectiveness depends on national implementation, measurable standards, adequate funding and monitoring mechanisms (African Union, 2024; Yilma & Wodajo, 2026). The study concludes that AI can strengthen national security in Africa only when technological adoption is supported by context-sensitive governance, effective oversight, human-rights protection, institutional readiness and strategic data sovereignty. Technology should complement accountable human judgment and serve public security without undermining democratic values or the rule of law.

Recommendations

Based on the findings of the study, the following recommendations are proposed:

Develop Risk-Based AI Governance Frameworks

African governments should develop and implement risk-based AI governance frameworks that address the ethical, legal, institutional and technical risks associated with AI-enabled security operations. These frameworks should classify AI systems according to their level of risk and subject high-risk applications, including facial recognition, predictive policing and automated threat assessment, to stricter legal and technical requirements. The frameworks should be developed through inclusive processes involving security institutions, technical experts, civil society organizations, legal professionals and affected communities.

Establish Independent Oversight and Accountability Mechanisms

African governments should establish independent oversight and accountability mechanisms for AI systems deployed in national security. Such bodies should be empowered to review AI systems, conduct compliance audits, investigate complaints and provide remedies for individuals affected by unlawful or harmful automated decisions. Their membership should include security, legal, technical and human-rights experts. These mechanisms should operate with transparency and publish annual reports on AI system performance, audits and complaints.

Strengthen Data Protection and Privacy Laws

Existing data-protection and privacy laws should be strengthened and effectively applied to AI-enabled security operations. Clear rules should regulate the collection, processing, retention, sharing and deletion of personal data. Security institutions should also obtain appropriate legal authorization before conducting intrusive surveillance, except under clearly defined emergency circumstances. Independent data protection authorities should be empowered to oversee compliance and investigate violations.

Conduct Algorithmic and Human-Rights Impact Assessments

Security institutions should conduct algorithmic and human-rights impact assessments before deploying high-risk AI systems. These assessments should examine privacy risks, data quality, algorithmic bias, cybersecurity vulnerabilities and the possible effects of automated decisions on vulnerable groups. AI systems should also undergo regular independent auditing throughout their operational lifecycle. The results of these assessments and audits should be published to ensure transparency and public accountability.

Ensure Meaningful Human Oversight

African governments should ensure meaningful human oversight of AI-enabled security operations. AI should support rather than replace accountable human judgment in high-stakes decisions. Responsible officers should review automated recommendations, explain final decisions and remain legally accountable for the outcomes produced through AI-assisted processes. Human oversight should be supported by adequate training and clear protocols for intervention.

REFERENCES

1. Adedigba, T. A. (2026). Comparative assessment of artificial intelligence-supported security measures and conventional security approaches on banditry and insurgency activities in Nigeria. Zamfara International Journal of Education, 6(2), 258-267.
2. African Union. (2024). Continental artificial intelligence strategy: Harnessing AI for Africa's development and prosperity. African Union. https://au.int/sites/default/files/documents/44004-doc-EN-_Continental_AI_Strategy_July_2024.pdf
3. Aning, K. (2015). Security intelligence and democratic oversight in West Africa: Opportunities and challenges. Conflict, Security & Development, 15(1), 31-50.
4. Badawy, W. (2025). The ethical use and development of artificial intelligence (AI) strategy in Egypt: Identifying gaps and recommendations. AI and Ethics, 5, 3579-3591.
5. Bor, S., & Koech, N. C. (2023). Balancing human rights and the use of artificial intelligence in border security in Africa. Journal of Intellectual Property and Information Technology Law, 3(1), 77-122.
6. Boulanin, V., & Verbruggen, M. (2017). Mapping the development of autonomy in weapon systems. Stockholm International Peace Research Institute. https://www.sipri.org/sites/default/files/Mapping-development-autonomy-in-weapon-systems.pdf
7. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention and mitigation. Future of Humanity Institute. https://arxiv.org/pdf/1802.07228
8. Buzan, B. (1991). People, states and fear: An agenda for international security studies in the post-Cold War era. Lynne Rienner Publishers.
9. Chinagorom, A. E., Chika, A. J., & Nwigwe, C. (2025). Artificial intelligence and counter-terrorism in Nigeria: Prospects, pitfalls and the future of security strategy. Jalingo Journal of Social and Management Sciences, 6(3), 154-165.
10. Department of Communications and Digital Technologies. (2024). South Africa national artificial intelligence policy framework. Republic of South Africa. https://www.africadataprotection.org/South-Africa-AI.pdf
11. Donald, D., Mustapha, A., & Imam, A. S. (2025). Role of artificial intelligence (AI) in intelligence gathering and management of Nigeria national security. International Journal of Sub-Saharan African Research, 3(3), 206-225.
12. Effoduh, J. O., Akpudo, U. E., & Kong, J. D. (2024). Toward a trustworthy and inclusive data governance policy for the use of artificial intelligence in Africa. Data & Policy, 6, e34.
13. Egypt National AI Governance Framework. (2026). Guide to Egypt's national AI governance framework. National Council for Artificial Intelligence, Quantum Computing and Emerging Technologies.

https://ai.gov.eg/SynchedFiles/ar/Resources/Guide%20to%20Egypt%E2%80%99s%20National%20AI%20Governance%20Framework%2015-3-2026.pdf
14. Elokaby, M. A. (2024). Development of cybersecurity laws in Egypt and its impact on the judicial system (Opportunities and challenges). International Cybersecurity Law Review, 5, 563-584.
15. Falode, J. A., Murtala, W., Dovoeke, D., Manoah, K., & Ajayi-Segun, B. M. (2025). Harnessing artificial intelligence for national security in Nigeria: Strategic prospects and limitations. LASU Journal of Peace & Security Studies, 1(1), 269-284.
16. Gikunda, P., Kituku, B., Moso, J., Wai, L. W., & Wang, P. (2025). Kenya's AI ethics and governance framework 2025. Dedan Kimathi University of Technology and Northumbria University. https://repository.dkut.ac.ke:8080/xmlui/handle/123456789/21478
17. Haddon, L. (2007). Roger Silverstone's legacies: Domestication. New Media & Society, 9(1), 25–32. https://doi.org/10.1177/1461444807075201
18. Harwood, S. A. (2011). The domestication of online technologies by smaller businesses and the "busy day." Information and Organization, 21(2), 84–106. https://doi.org/10.1016/j.infoandorg.2011.03.002
19. Hashem, S. (2019). Towards a national cybersecurity strategy: The Egyptian case. Systemics, Cybernetics and Informatics, 17(3), 88-94.
20. Hoadley, D. S., & Lucas, N. J. (2018). Artificial intelligence and national security. Congressional Research Service. https://digital.library.unt.edu/ark:/67531/metadc1157028/
21. Irambona, E., Bugingo, E., & Tunezerwe, E. (2025). Implementation of AI-powered cybersecurity solutions in Rwanda's government institutions: Case study RISA institution. International Journal of Innovative Science and Research Technology, 10(4), 1583-1592.
22. Jatau, P. M., Lenshie, N. E., & Okoli, A. C. (2025). Security governance and the necessity for community-led approaches in Nigeria. African Solutions Journal, 6(1), 1–29.
23. Kenya AI Strategy. (2025). Kenya artificial intelligence strategy 2025-2030. Ministry of Information, Communications and the Digital Economy. https://ict.go.ke/sites/default/files/2025-03/Kenya%20AI%20Strategy%202025%20-%202030.pdf
24. Kenya Cybersecurity Strategy. (2025). Kenya cybersecurity strategy, 2025-2029. National Computer and Cybercrimes Coordination Committee. https://ict.go.ke/sites/default/files/2025-03/Kenya%20AI%20Strategy%202025%20-%202030.pdf
25. Kharvi, P. L. (2024). Understanding the impact of AI-generated deepfakes on public opinion, political discourse, and personal security in social media. IEEE Security & Privacy, 22(4), 115–122. https://doi.org/10.1109/MSEC.2024.3405963
26. Mannuru, N. R., Shahriar, S., Teel, Z. A., Wang, T., Lund, B. D., Tijani, S., ... & Vaidya, P. (2023). Artificial intelligence in developing countries: The impact of generative artificial intelligence (AI) technologies for development. Information Development, 02666669231200628.
27. Mhlanga, D. (2026). Using artificial intelligence to improve governance and public services in Africa. Frontiers in Big Data, 9, Article 1835663. https://doi.org/10.3389/fdata.2026.1835663
28. Nibigira, N., Havyarimana, V., & Xiao, Z. (2024). Artificial intelligence adoption for cybersecurity in Africa. Journal of Information Security, 15, 134-147.
29. Nsude, I. (2022). Artificial intelligence (AI), the media and security challenges in Nigeria. Communication, Technologies et Développement, 11.
30. OECD. (2026). AI governance in Africa: Insights from a policy dialogue with 12 countries. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/04/oecd-artificial-intelligence-case-studies_71322177/strengthening-ai-governance-in-africa_812bb149/1ff55135-en.pdf
31. Ogbe, S. J., Jiboyewa, J. M., & Ekwem, N. (2025). Influence of artificial intelligence-enabled social media communication on national security in Nigeria. Social & Digital Media Discourse, 6(1), 49-67.
32. Okegbemi, A. C. (2024). Economic environment factors and how they suppress growth and development in Nigeria. African Journal of Economic Review, 11(4), 256–278.
33. Olonisakin, F. (2008). Peacekeeping in Sierra Leone: The story of UNAMSIL. Lynne Rienner Publishers.
34. Oluyemi, O. A. (2025). Emerging technologies and their implications on Africa's security architecture. SADI Journal of Interdisciplinary Research, 12(2), 7-25.
35. Republic of Rwanda, Ministry of ICT and Innovation. (2022). The National AI Policy: To leverage AI to power economic growth, improve quality of life and position Rwanda as a global innovator for responsible and inclusive AI. Ministry of ICT and Innovation. https://www.minict.gov.rw/index.php?eID=dumpFile&t=f&f=67550&token=6195a53203e197efa47592f40ff4aaf24579640e

36. Rufus, A. I. (2024). Ungoverned Spaces and the Challenges of Terrorism in Africa. Kashere Journal of Politics and International Relations, 2(2), 490–503.
37. Russell, S., & Norvig, P. (2021). Artificial intelligence: A modern approach (3rd ed.). Prentice Hall Series.
38. Rwigema, P. C. (2026). Effects of artificial intelligence adoption on productivity and service delivery in Rwanda's public sector. International Journal of Innovation Studies, 10(1), 340-365.
39. Sayler, K. M. (2020). Artificial intelligence and national security (CRS Report No. R45178). Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R45178
40. Silverstone, R., and Hirsch, E. (Eds.). (1992). Consuming technologies: Media and information in domestic spaces. Routledge.
41. Silverstone, R., Hirsch, E., and Morley, D. (1992). Information and communication technologies and the moral economy of the household. In R. Silverstone and E. Hirsch (Eds.), Consuming technologies: Media and information in domestic spaces (pp. 15–31). Routledge.
42. Van Eekelen, W. F. (2010). The legal framework of security sector governance. Geneva, Switzerland: Geneva Centre for the Democratic Control of Armed Forces. Retrieved from https://www.dcaf.ch/sites/default/files/publications/documents/The%2520Legal%2520Framework%2520of%2520Security%2520LOW.pdf
43. Yelwa, M. A., & Umar, I. (2025). Intelligence and influence: The rise of digital authoritarianism in African security governance. African Journal of Politics and Administrative Studies, 18(3), 188-207.
44. Yilma, K., & Wodajo, K. (2026). Strategy as governance: The governance of AI in Africa. Science and Public Policy, 53(2), 236-244.
45. Zakari, M. (2024). Implication of artificial intelligence on national security for the Nigeria security agencies. Journal of Terrorism Studies, 6(1), 1-15.
46. Zisengwe, M. (2025). Exploring the implications of AI on digital democracy in South Africa. In State of Internet Freedom in Africa 2025. Collaboration on International ICT Policy for East and Southern Africa (CIPESA). https://cipesa.org/wp-content/files/reports/State_of_Internet_Freedom_in_Africa_2025__Exploring_the_Implications_of_Artificial_Intelligence_on_Digital_Democracy_in_South_Africa_.pdf