Published by

British Journal of Contemporary Research

BEXFORD PUBLISHING

Artificial Intelligence and the Transformation of Digital Security Governance in the Global South: Evidence from Nigeria and Implications for the International Order

Original Research Article | Volume 1 | Issue 6 | 2026 | Article Number: 021

Accepted: 03 October 2026 | Published: 10 November 2026 | ISSN: 2979-8582 (Online)

Crossref : **https://doi.org/10.67693/BJCR-UUIR2MG2**

Ojuawo Olakunle Olaniyi[1], Adetunberu Oludotun (PhD)[2]

[1]Department of Peace and Security Studies, Faculty of Multidisciplinary Studies, Ekiti State University, Ado-Ekiti, Nigeria,

[2]Department of Intelligence and Security Studies, Faculty of Multidisciplinary Studies, Ekiti State University, Ado-Ekiti, Nigeria

OOO 0009-0004-4899-9279, **AO** 0009-0007-4469-6416

Correspondence: Ojuawo Olakunle Olaniyi, ojuawoolakunle@gmail.com

Abstract

The rapid development of artificial intelligence (AI) is transforming digital security governance by changing how states detect, analyze, and respond to emerging security threats. This transformation has implications beyond national security, particularly for state capacity, digital sovereignty, regional cooperation, and the evolving international order. This study examines how AI is transforming digital security governance in Nigeria and assesses the implications for state capacity, digital sovereignty, regional security cooperation, and the international order. The study adopts a qualitative case study design based on documentary analysis of Nigerian government policies and institutional documents, regional frameworks, peer-reviewed literature, and relevant reports. Securitization Theory and Complex Interdependence Theory guide the analysis, while the study uses digital sovereignty as an analytical concept. Findings indicate that Nigeria is gradually incorporating AI into digital security governance through cybersecurity policies, emerging AI institutions, technological capacity-building initiatives, and the development of AI-related security applications. However, the transformation remains constrained by limitations in digital infrastructure, technical expertise, institutional capacity, regulatory implementation, and technological dependence. The study further finds that AI creates a dual dynamic for Nigeria: it offers opportunities to strengthen threat detection, intelligence analysis, cybersecurity, and other security capabilities, while dependence on external technologies and infrastructure may constrain digital sovereignty. Regional and international cooperation provides opportunities for Nigeria to strengthen its digital security capacity, but also reflects the complex interdependencies surrounding emerging technologies. The study concludes that AI is not merely a technological innovation but an emerging force reshaping digital security governance

© 2026 The Authors. Published by Bexford Publishing Ltd

and international relations. It recommends stronger integration of AI and cybersecurity governance, investment in indigenous technological capacity, enhanced regional cooperation, and greater Nigerian participation in global AI governance to promote a more secure and inclusive international digital order.

Keywords: Artificial Intelligence, Digital Security Governance, Cybersecurity, Digital Sovereignty, State Capacity, International Order, Regional Security Cooperation

1. Introduction

The rapid advancement of digital technologies has fundamentally transformed governance, economic development, and international security. The Fourth Industrial Revolution, driven by the convergence of artificial intelligence (AI), big data analytics, cloud computing, blockchain technology, and the Internet of Things (IoT), has reshaped how governments deliver public services, formulate policies, and respond to increasingly complex security challenges. While digital transformation has accelerated innovation and global connectivity, it has also intensified cyber threats, including cybercrime, cyber espionage, ransomware attacks, digital terrorism, misinformation campaigns, and attacks on critical national infrastructure. These developments have exposed the limitations of traditional security approaches and elevated digital security governance as a strategic priority for protecting cyberspace, digital infrastructure, and national information assets (Maleh et al., 2021; Huang et al., 2021; Gilbert & Gilbert, 2024).

Digital security governance has consequently emerged as a multidimensional framework for managing digital risks by integrating cybersecurity, regulatory oversight, intelligence coordination, data protection, institutional accountability, and international cooperation. Unlike conventional cybersecurity, which focuses primarily on protecting networks and information systems, digital security governance provides broader institutional and policy mechanisms for safeguarding national digital ecosystems. Existing studies emphasize that effective digital security governance depends on adaptive governance structures that can respond to rapidly evolving technological threats while balancing innovation, national security, economic development, and democratic accountability (Maleh et al., 2021; Zukis, 2022; Gilbert & Gilbert, 2024). Within this framework, AI has become a transformative technology that enhances intelligence gathering, predictive analytics, cyber threat detection, surveillance, border management, financial intelligence, and early warning systems. However, integrating AI into security governance has also raised concerns about algorithmic bias, transparency, accountability, privacy, and ethical regulation, highlighting the need for robust AI governance frameworks (Horvitz et al., 2021; Deeks, 2023; Meleouni & Efthymiou, 2024).

Beyond domestic governance, AI is increasingly influencing international security governance and the evolving international order. Technological capability has become a strategic determinant of national competitiveness and geopolitical influence as states compete for leadership in artificial intelligence, advanced computing, digital infrastructure, and data governance (Posey et al., 2026). Consequently, debates surrounding AI now extend beyond technological innovation to encompass digital sovereignty, technological dependence, cyber diplomacy, and global governance. Calderaro and Blumfelde (2022) argue that digital sovereignty has become central to contemporary international politics, while Srivastava and Bullock (2024) contend that AI governance constitutes an emerging arena for negotiating international authority and cooperation. Similarly, Costa-Barbosa et al. (2024) observe that AI governance increasingly shapes the global distribution of power through technological competitiveness, regulatory standards, and strategic alliances.

These transformations are particularly significant for developing countries where digital transformation is progressing alongside institutional and technological constraints. Nigeria provides an appropriate empirical

© 2026 The Authors. Published by Bexford Publishing Ltd

context because of its expanding digital economy, increasing investment in AI, and policy initiatives to strengthen digital transformation and cybersecurity, including the National Artificial Intelligence Strategy and the National Digital Economy Policy and Strategy (National Artificial Intelligence Strategy, 2026). Nevertheless, persistent cybercrime, inadequate digital infrastructure, fragmented regulatory frameworks, limited institutional capacity, and dependence on foreign digital technologies continue to constrain effective digital security governance (Akujobi et al., 2026). These challenges underscore the importance of understanding how AI can strengthen digital security governance while simultaneously creating new governance and sovereignty concerns.

Despite growing scholarship on AI, cybersecurity, digital governance, and digital sovereignty, limited attention has examined how AI transforms digital security governance in developing countries and how these transformations influence state capacity, digital sovereignty, regional security cooperation, and the evolving international order. Furthermore, existing studies often examine AI, digital security governance, and international relations separately, overlooking their interconnected dynamics, particularly within African contexts. Against this background, this study examines how artificial intelligence is transforming digital security governance in Nigeria and its implications for state capacity, digital sovereignty, regional security cooperation, and the evolving international order. Specifically, the study seeks to (i) analyze how artificial intelligence is transforming digital security governance in Nigeria; (ii) evaluate the implications of AI-enabled digital security governance for state capacity and digital sovereignty; (iii) examine the influence of AI-driven digital security governance on regional security cooperation and the evolving international order; and (iv) propose policy measures for strengthening responsible and inclusive AI governance in Nigeria and other developing countries. To achieve these objectives, the study adopts a qualitative case study approach based on documentary and thematic analysis, guided by Securitization Theory, Complex Interdependence Theory, and Digital Sovereignty. By integrating perspectives from artificial intelligence, digital security governance, and international relations, the study contributes to the growing scholarship on technology-driven security governance. It provides empirical evidence to inform policy and governance debates across the Global South.

2. Literature Review

2.1 Artificial Intelligence and Digital Security Governance

The literature increasingly identifies artificial intelligence (AI) as a transformative technology in contemporary security governance. AI's capacity to process large volumes of data, identify patterns, and support rapid decision-making has expanded its application in cybersecurity, intelligence analysis, surveillance, predictive policing, border management, and defense. Horvitz et al. (2021) emphasize the importance of responsible AI development within national security institutions, while Deeks (2023) examines the growing incorporation of AI into national security decision-making. Meleouni and Efthymiou (2024) similarly identify cybersecurity, intelligence, and defense as key areas of AI application, while highlighting the need for appropriate governance and international standards. These studies establish that AI is increasingly becoming embedded in security institutions rather than remaining solely a commercial or technological innovation.

Empirical developments reinforce this argument. Governments are increasingly experimenting with AI-assisted cyber defense and threat detection. The United Kingdom, for example, has been testing frontier AI models for public-sector cyber defense through the Government Cyber Coordination Center and the National Cyber Security Center. Such developments illustrate a shift toward predictive and automated security governance. At the same time, AI creates new security vulnerabilities because the technology can also be exploited to improve cyberattacks, discover vulnerabilities, and generate sophisticated malicious

© 2026 The Authors. Published by Bexford Publishing Ltd

content. This dual-use character means that AI simultaneously strengthens and complicates digital security governance.

The governance literature consequently moves beyond AI's technological benefits to consider accountability, transparency, privacy, bias, and institutional oversight. Ndrejaj and Ali (2022) identify governance deficits as a key risk of rapid AI integration, while Chesterman et al. (2024) examine emerging AI principles and governance frameworks intended to promote responsible deployment. The central issue emerging from this literature is therefore not simply whether AI can improve security, but whether institutions possess the capacity to govern AI-enabled security systems effectively.

2.2 Digital Security Governance and State Capacity

The literature on cybersecurity governance provides an important foundation for understanding this institutional question. Maleh et al. (2021) emphasize that effective cybersecurity requires governance structures that integrate technical capabilities with risk management, organizational processes, policies, and standards. Huang et al. (2021) further demonstrate that cybersecurity risks increasingly transcend organizational and national boundaries, requiring cooperation between governments and private-sector actors. These perspectives indicate that digital security governance is broader than conventional cybersecurity because it encompasses institutional coordination, regulatory oversight, risk management, data governance, infrastructure protection, and cooperation.

This distinction matters especially when AI is incorporated into security systems. AI may increase the operational capacity of security institutions by enabling faster analysis and automated threat detection, but its effectiveness depends on infrastructure, data quality, technical expertise, and regulatory institutions. Consequently, technological acquisition does not automatically translate into stronger state capacity.

African scholarship illustrates this challenge. Arakpogun et al. (2021) identify institutional and governance constraints affecting AI development in African countries, while Wakunuma et al. (2022) highlight the limited development of appropriate AI governance structures. Njoroge (2024) similarly identifies weaknesses in infrastructure, technical capacity, policy implementation, and ethical integration. These findings are significant for Nigeria because they suggest that the effectiveness of AI-enabled security governance depends on institutions' ability to translate technological possibilities into sustainable governance capabilities.

Recent Nigerian research reinforces this concern. Falade and Osho's analysis of Nigeria's cybersecurity legislation and policy framework identifies ongoing problems with enforcement, institutional coordination, skills retention, and implementation, despite improvements in the country's cybersecurity architecture. Similarly, recent research on AI governance in Nigeria identifies concerns about regulatory gaps, data privacy, and institutional readiness, and calls for locally appropriate governance frameworks rather than simply adopting external models.

The literature therefore suggests an important paradox: AI can strengthen operational state capacity while simultaneously exposing weaknesses in governance capacity. This paradox is central to understanding Nigeria's experience.

2.3 AI, Digital Sovereignty and Technological Dependence

A third body of literature links AI governance to digital sovereignty. Digital sovereignty concerns states' and societies' capacity to exercise meaningful control over digital infrastructure, data, algorithms, and technological systems. Calderaro and Blumfelde (2022) argue that AI increasingly affects strategic autonomy because control over data, algorithms, and computational resources has become an important source of power. Srivastava and Bullock (2024) further demonstrate that AI-enabled global governance

© 2026 The Authors. Published by Bexford Publishing Ltd

involves complex relationships between state authority and private technological power.

Costa-Barbosa et al. (2024) similarly broaden the sovereignty debate to include computing capacity, databases, data, algorithms and AI models. This is particularly significant for developing countries because access to advanced AI frequently depends on foreign infrastructure, cloud services, computing resources and technology companies. Digital sovereignty therefore cannot be reduced to having a national AI policy; it also involves the ability to control, or meaningfully participate in, the technological infrastructure on which AI systems depend.

Recent African scholarship makes this issue increasingly explicit. Effoduh (2026) argues that African AI governance frameworks can reproduce external technological and normative dependencies when international models are adopted without sufficient adaptation to African contexts. His analysis of the African Union and national initiatives, including Nigeria, connects AI governance to questions of epistemic and technological sovereignty. Similarly, recent research on African AI sovereignty argues that access to AI models alone does not guarantee autonomy because computing infrastructure, localized data, and indigenous technical capacity remain critical constraints.

Nigeria therefore presents an important case for examining the sovereignty implications of AI adoption. The country is developing domestic AI institutions and policy capacity, but this occurs within a global technological environment dominated by foreign platforms, advanced computing infrastructure, and transnational technology firms. The central question is consequently whether AI adoption strengthens Nigeria's strategic autonomy or creates new forms of technological dependence.

2.4 AI, Regional Security Cooperation and the International Order

The international-relations literature increasingly treats AI as a factor influencing global power, diplomacy, security cooperation and the international order. Arsenault and Kreps (2022) argue that AI has implications for defense, diplomacy, trade, warfare and the distribution of international power. Kļaviņš (2021) similarly highlights the growing relationship between AI and diplomacy, while Tzimas (2021) draws attention to the governance challenges associated with autonomous weapons and collective security.

AI creates a particularly important tension between interdependence and strategic competition. Digital infrastructure, data, semiconductor technologies, cloud computing, and AI research networks operate across national borders, making international cooperation unavoidable. At the same time, governments increasingly regard AI capabilities as strategic assets. Control over advanced computing and AI technologies can provide economic and security advantages, encouraging states to protect technological capabilities and restrict strategic technologies.

This tension is increasingly visible in competing approaches to AI governance and technological sovereignty. States are developing domestic AI strategies while also pursuing international partnerships, technology controls, and strategic arrangements designed to protect their technological interests. Recent scholarship describes this development as the emergence of technologically differentiated blocs in which states seek greater control over critical digital and AI infrastructures. This development has implications for developing countries because technological competition among major powers may create new opportunities for cooperation while also deepening dependence on external technology providers.

The international-order literature therefore suggests that AI should not be treated merely as another emerging technology. It is increasingly becoming a component of geopolitical power and international governance. However, existing scholarship tends to focus on major technological powers, leaving comparatively less attention to how developing countries such as Nigeria experience and respond to these transformations.

© 2026 The Authors. Published by Bexford Publishing Ltd

2.5 AI Governance in Africa and Nigeria

African scholarship provides an important counterbalance to the dominant focus on technologically advanced countries. Arakpogun et al. (2021), Wakunuma et al. (2022) and Njoroge (2024) identify challenges involving institutional capacity, infrastructure, skills, regulatory development and implementation. Gagliardone (2024) adds a critical sovereignty perspective by situating AI governance within Africa's broader history of technological dependence and external influence.

At the continental level, the African Union's Continental Artificial Intelligence Strategy represents an important attempt to establish an Africa-centered approach to AI governance. The strategy emphasizes responsible AI, African development priorities, and continental cooperation. This indicates that African states are increasingly seeking to shape AI governance collectively rather than simply adopting external models.

Nigeria is particularly significant within this emerging African landscape. The establishment of the National Center for Artificial Intelligence and Robotics and the development of national AI policy demonstrate growing efforts to build domestic AI capacity. Recent Nigerian scholarship, however, continues to identify regulatory, institutional, and implementation challenges. The emerging Nigerian experience therefore demonstrates both policy ambition and implementation constraints.

However, the existing literature has a significant limitation. African studies frequently examine AI through the perspectives of development, ethics, governance readiness, or digital sovereignty. In contrast, relatively fewer studies examine how AI specifically transforms digital security governance and how that transformation affects state capacity, regional security cooperation, and the international order.

2.6 Synthesis and Research Gap

The literature establishes four important conclusions. First, AI is increasingly embedded in security governance through cybersecurity, intelligence, surveillance, predictive analytics, and decision support. Second, effective digital security governance depends on institutional capacity, regulation, infrastructure, coordination, and accountability. Third, AI adoption increasingly raises questions of digital sovereignty because control over data, algorithms, computing infrastructure, and technological supply chains has become strategically important. Fourth, AI is reshaping international security cooperation and geopolitical competition.

Nevertheless, these strands of scholarship remain insufficiently integrated. AI-security studies generally focus on technological capabilities and risks; cybersecurity-governance studies emphasize institutional and regulatory arrangements; digital-sovereignty literature focuses on autonomy and technological control; and international-relations scholarship concentrates on geopolitical competition and global governance. African scholarship has begun to address AI governance and sovereignty, but comparatively little research connects these dimensions to the transformation of digital security governance.

This study therefore addresses the principal gap: the limited integrated analysis of how AI-driven changes in digital security governance affect state capacity, digital sovereignty, regional security cooperation, and Nigeria's position within the evolving international order. The study addresses this gap by treating Nigeria not merely as an illustration of global AI adoption but as an empirical case through which the broader relationship between technology, security governance, sovereignty, and international order can be examined.

© 2026 The Authors. Published by Bexford Publishing Ltd

3. Theoretical Framework

3.1 Securitization Theory

Securitization Theory, developed by the Copenhagen School, serves as the primary theoretical lens for this study. The theory explains how issues are framed as security threats and subsequently receive increased political and institutional attention (Buzan et al., 1998). Rather than treating threats as inherent, securitization examines how political actors construct specific issues as matters requiring urgent security responses.

The theory is particularly relevant to the increasing securitization of cyberspace and emerging technologies. Cybercrime, cyber espionage, attacks on critical infrastructure, data breaches, and AI-enabled threats have been progressively incorporated into national security agendas (Madubuko & Chitsungo, 2024, pp. 25–50). AI therefore constitutes both a potential security threat and a tool for addressing emerging threats through intelligence analysis, surveillance, threat detection, predictive analytics, and early-warning systems. In the Nigerian context, Securitization Theory helps explain how digital threats acquire national security significance and how their securitization shapes digital security governance and the adoption of AI-enabled security capabilities.

3.2 Complex Interdependence Theory

Complex Interdependence Theory, formulated by Keohane and Nye (1977), emphasizes the multiple and interconnected relationships among states, international organizations, corporations, and other non-state actors. The theory challenges a purely state-centric perspective of international relations by recognizing that economic, technological, and security relationships increasingly transcend national borders.

The theory is particularly relevant to AI and digital security because AI systems rely on cross-border data flows, cloud infrastructure, computing resources, semiconductor technologies, technology companies, and international knowledge networks. Cyber threats also transcend national boundaries, necessitating increased cooperation among states and non-state actors. In Nigeria, digital security governance cannot be understood solely through domestic institutions, as the country's security environment is linked to international technology providers, regional organizations, transnational cyber threats, and global digital infrastructures (Jude, 2025). Complex Interdependence Theory therefore helps explain how AI creates opportunities for regional and international cooperation while simultaneously generating technological dependencies that may constrain national autonomy.

3.3 Application of the Theoretical Framework

The two theories provide complementary perspectives for this study. Securitization Theory explains how AI and digital threats acquire security significance and influence Nigeria's domestic digital security governance, while Complex Interdependence Theory clarifies the transnational technological relationships, dependencies, and cooperative arrangements that shape this governance.

Digital sovereignty serves as an analytical concept rather than a third theoretical framework. It provides a basis for assessing whether AI adoption enhances Nigeria's control over its data, digital infrastructure, technological capabilities, and security systems or increases reliance on external technologies. The combined framework therefore enables the study to analyze how AI transforms digital security governance, influences state capacity and digital sovereignty, and connects Nigeria's domestic security transformation to regional cooperation and the evolving international order.

4. Research Methodology

This qualitative case study investigates how artificial intelligence is transforming digital security

© 2026 The Authors. Published by Bexford Publishing Ltd

governance in Nigeria and its broader implications for state capacity, digital sovereignty, regional security cooperation, and the international order. Nigeria is selected as the case study because of its expanding digital economy, evolving AI governance framework, cybersecurity challenges, and growing involvement in regional and international digital governance initiatives.

The study relies primarily on documentary data, including Nigerian government policies and legislation, institutional documents, reports from relevant national agencies, African Union and ECOWAS policy documents, peer-reviewed academic literature, and selected reports from reputable international organizations. Particular emphasis is given to documents addressing artificial intelligence, cybersecurity, digital governance, data protection, digital infrastructure, and regional and international cooperation. The analysis focuses on developments between 2016 and 2024, a period characterized by significant expansion in Nigeria's digital governance and AI policy environment.

Documents are purposively selected based on their relevance to the research objectives, institutional authority, credibility, and contribution to understanding AI and digital security governance in Nigeria. To strengthen the analysis, the study compares evidence across source categories, including government documents, scholarly studies, and international and regional reports. This approach distinguishes policy intentions, institutional initiatives, and demonstrable implementation, reducing the risk of interpreting proposed AI applications as established practices.

The data are analyzed using thematic analysis, structured around four interconnected themes derived from the study's objectives: AI and digital security governance, state capacity and digital sovereignty, regional security cooperation, and implications for the international order. This study examines documentary evidence through these themes. It interprets it through the frameworks of Securitization Theory and Complex Interdependence Theory, with digital sovereignty as a central analytical concept. This methodological approach connects Nigeria's domestic AI and security developments to broader patterns of technological interdependence and international security governance.

This study is limited by its reliance on documentary evidence and the availability of publicly accessible information regarding specific AI applications within Nigerian security institutions. When evidence indicates policy intentions rather than operational deployment, the study maintains a clear distinction. This limitation is addressed by triangulating available sources and carefully interpreting the evidence.

4.1 Artificial Intelligence and the Transformation of Digital Security Governance in Nigeria

Nigeria's digital security governance has expanded beyond conventional cybersecurity to incorporate emerging technologies and data-driven approaches to national security. The National Cybersecurity Policy and Strategy (NCPS) 2021 recognizes the increasing sophistication of cyber threats and promotes real-time information sharing among government, the private sector, and other stakeholders. Significantly, the policy identifies artificial intelligence and machine learning as technologies that can support cybersecurity data analysis and identify potential cyber risks (Federal Republic of Nigeria, 2021).

This development has significant security implications. AI-enabled analysis can support cyber-threat detection, intelligence processing, surveillance, predictive assessment, and early warning, potentially shifting security governance from predominantly reactive responses to more data-driven approaches. The National Center for Artificial Intelligence and Robotics (NCAIR) identifies automated threat detection, facial recognition, predictive analytics, AI-enabled drones, and cybersecurity among potential applications of AI and robotics in Nigeria's security sector (NCAIR, n.d.). These developments indicate that AI is increasingly being incorporated into Nigeria's national-security discourse and emerging digital security architecture.

© 2026 The Authors. Published by Bexford Publishing Ltd

The establishment of NCAIR further reflects efforts to develop domestic capacity in AI and other emerging technologies. Its activities in machine learning, intelligent robotics and related technologies, together with its reported support for pilot AI projects using national cloud infrastructure, provide an institutional foundation for technology-enabled security capabilities (NCAIR, n.d.). However, the available evidence does not establish widespread operational deployment of all the security applications NCAIR identifies. It is therefore more appropriate to describe these capabilities as emerging rather than as evidence of a fully transformed security system.

From the perspective of Securitization Theory, incorporating AI into cybersecurity policy and national-security planning reflects the increasing treatment of cyber threats and digital vulnerabilities as security priorities. AI consequently has a dual character: it shapes the emerging digital threat environment while also providing tools to detect, analyze, and manage such threats. This is particularly relevant to Nigeria, where cybercrime, digital fraud, attacks on information systems, and other technology-enabled threats have increased the demand for more sophisticated security capabilities.

Overall, the evidence indicates a gradual transformation of Nigeria's digital security governance rather than a complete transition to AI-driven security. Policy commitments, institutional initiatives, and emerging technological capabilities demonstrate growing recognition of AI's security value. Nevertheless, limitations in infrastructure, technical expertise, implementation capacity, and regulatory oversight may constrain the effective deployment of AI-enabled security systems. Nigeria's experience therefore reflects an ongoing transition in which AI is increasingly incorporated into national security governance, while its practical contribution remains dependent on the country's institutional and technological capacity.

4.2 AI, State Capacity and Digital Sovereignty in Nigeria

Artificial intelligence can strengthen Nigeria's state capacity by improving public institutions' ability to process information, detect threats, support decision-making, and manage increasingly complex digital risks. However, the effectiveness of AI-enabled governance depends on digital infrastructure, technical expertise, reliable data, and institutional capacity. Nigerian scholarship similarly identifies weaknesses in infrastructure, skills, institutional coordination, and policy implementation as key constraints on developing effective AI and cybersecurity capabilities (Arakpogun et al., 2021; Njoroge, 2024).

Nigeria has taken steps to strengthen domestic AI capacity through institutions such as the National Center for Artificial Intelligence and Robotics (NCAIR). Its research and development in machine learning, robotics, and related technologies, along with initiatives involving national cloud infrastructure and locally developed AI models, show efforts to reduce dependence on externally developed technological capabilities (NCAIR, n.d.). These initiatives are significant from a digital-sovereignty perspective because technological autonomy increasingly depends not only on access to AI but also on the capacity to develop, manage, and adapt critical digital technologies locally.

Nevertheless, developing domestic capacity does not eliminate technological dependence. AI-enabled security governance requires access to computing infrastructure, specialized software, data, cloud services, advanced hardware, and technical expertise, many of which are embedded within global technology networks. Nigeria therefore faces a dual challenge: strengthening indigenous technological capabilities while operating within an international digital environment in which foreign states and multinational technology companies often control critical technologies and infrastructures. This creates a tension between AI-enabled state capacity and technological dependence.

From a digital sovereignty perspective, the issue is not whether Nigeria adopts AI, but how much it can meaningfully control the technologies, data, and infrastructure that underpin AI-enabled security

© 2026 The Authors. Published by Bexford Publishing Ltd

governance. Greater domestic capacity can strengthen strategic autonomy, while excessive dependence on external technologies may create vulnerabilities and limit policy choices. Complex Interdependence Theory helps explain this tension because Nigeria's technological development necessarily involves relationships with foreign technology providers, international institutions and regional partners.

The evidence therefore suggests that AI offers Nigeria an opportunity to strengthen state capacity and improve digital security governance, but institutional, infrastructural and technological constraints condition its benefits. Nigeria's emerging AI initiatives represent an important step toward greater technological capability, yet they also show that digital sovereignty remains an ongoing process rather than an achieved condition. This tension between capacity-building and dependence has broader implications for Nigeria's participation in regional digital-security cooperation and the evolving international order.

4.3 AI, Regional Security Cooperation and Nigeria's International Security Engagement

Nigeria's digital security governance is increasingly embedded within regional and international cooperation mechanisms. The National Cybersecurity Policy and Strategy (NCPS) 2021 recognizes that cyber threats transcend national borders and therefore calls for stronger cooperation with ECOWAS and the African Union. It specifically identifies cross-border law-enforcement cooperation, information sharing on cyber threats, technology transfer, and regional cybersecurity coordination as important components of Nigeria's cybersecurity strategy (Federal Republic of Nigeria, 2021).

This regional orientation is also evident in Nigeria's participation in ECOWAS cybersecurity mechanisms. Nigeria's national Computer Emergency Response Team (ngCERT), operating under the National Cybersecurity Coordination Center, is a member of the ECOWAS Information Sharing and Analysis Center (ISAC) and cooperates with other entities to exchange information on vulnerabilities and security incidents. These arrangements show that Nigeria cannot manage digital security effectively through domestic institutions alone. Cyber threats, digital infrastructure, and security information increasingly require cross-border coordination.

The regional framework has also expanded beyond information sharing towards coordinated capacity building. The ECOWAS Regional Cybersecurity and Cybercrime Strategy calls for cooperation among national cybersecurity institutions, sharing of alerts and cybersecurity information, joint responses to cyber threats, capacity building and mechanisms for regional coordination. In September 2023, ECOWAS and its partners launched the Joint Platform for the Advancement of Cybersecurity in West Africa in Abuja, focusing on regional cyber resilience, cyber diplomacy, capacity building and cooperation.

The African Union's development of the Continental Artificial Intelligence Strategy in 2024 further expands this regional context. The strategy seeks an Africa-centered approach to AI while promoting ethical and responsible use, national coordination, and stronger regional and global cooperation. For Nigeria, participation in these emerging frameworks creates opportunities to share expertise, strengthen cybersecurity capacity, and contribute to regional approaches to AI governance.

From the perspective of Complex Interdependence Theory, these developments show that Nigeria's digital security is increasingly shaped by multiple relationships involving states, regional organizations, technology actors, and international partners. AI intensifies this interdependence because its development and security applications depend on data, infrastructure, technical expertise, and information networks that extend beyond national borders. Regional cooperation can therefore strengthen Nigeria's ability to respond to cyber and AI-related threats while also creating dependencies on external institutions, technologies, and expertise.

The evidence suggests that Nigeria's regional engagement is becoming an important component of its

© 2026 The Authors. Published by Bexford Publishing Ltd

digital security governance. However, the extent to which regional cooperation can translate into effective AI-enabled security capabilities depends on institutional capacity, information-sharing mechanisms, technical expertise, and participating states' ability to coordinate their policies. Nigeria's experience therefore illustrates the dual character of technological interdependence: cooperation can strengthen security capacity, but dependence can also constrain strategic autonomy. This provides the basis for examining the broader implications of Nigeria's AI and digital security transformation for the evolving international order.

4.4 AI, Nigeria and the Evolving International Order

Nigeria's experience shows that the transformation of digital security governance is increasingly linked to broader changes in the international technological and security environment. The growing use and development of AI occur within a system characterized by cross-border data flows, technological dependence, international cooperation, and competition over advanced digital technologies. Consequently, Nigeria's efforts to strengthen AI-enabled security capabilities cannot be separated from the international structures within which these technologies are developed and accessed.

From the perspective of Complex Interdependence Theory, Nigeria's digital security environment involves multiple relationships with regional organizations, international institutions, technology providers, and other states. These relationships give Nigeria opportunities to access technological expertise, strengthen cybersecurity cooperation, and participate in emerging AI-governance initiatives. However, they can also create dependencies in which external actors control critical technologies, infrastructure, computing resources, or expertise.

The implications for digital sovereignty are therefore significant. Nigeria's development of domestic AI institutions and capabilities represents an effort to strengthen technological autonomy, but continued participation in global technology networks means that complete independence is neither realistic nor necessarily desirable. The more important question is whether Nigeria can control critical digital resources sufficiently while benefiting from international cooperation.

At the international level, AI is increasingly linked to technological power and geopolitical influence. Competition over advanced computing, AI systems, digital infrastructure, and technological standards is creating new forms of strategic competition alongside existing patterns of international cooperation. Nigeria's participation in African and international AI-governance initiatives therefore provides an opportunity to influence emerging norms while also navigating the interests of technologically advanced states.

The Nigerian case consequently suggests that AI is contributing to a gradual transformation rather than a complete replacement of the existing international order. The transformation is occurring through changing patterns of technological dependence, digital sovereignty, security cooperation, and access to strategic technologies. Nigeria's experience demonstrates that developing countries are not merely passive recipients of this transformation; they are increasingly negotiating their own interests, building domestic capabilities, and participating in regional and global governance arrangements.

5. Discussion

The findings demonstrate that artificial intelligence is beginning to reshape digital security governance in Nigeria, but the transformation remains gradual and constrained by institutional and technological limitations. Nigeria has moved beyond a purely conventional cybersecurity approach by incorporating AI and machine learning into national cybersecurity policy, establishing institutions for AI development, and exploring AI applications relevant to threat detection, intelligence, and surveillance. This aligns with the

© 2026 The Authors. Published by Bexford Publishing Ltd

broader literature identifying AI as increasingly important to contemporary security governance (Horvitz et al., 2021; Deeks, 2023; Meleouni & Efthymiou, 2024). However, the Nigerian case also shows that AI-related policies and institutional initiatives do not necessarily translate into widespread operational deployment.

From the perspective of Securitization Theory, the findings indicate that cyberspace and emerging digital threats have taken on greater national-security significance in Nigeria. Incorporating AI into cybersecurity policy reflects an attempt to develop more sophisticated mechanisms for identifying and responding to threats. However, securitization also raises governance concerns, particularly where increased surveillance and automated decision-making may affect privacy, accountability, and individual rights. Nigeria's experience therefore demonstrates that strengthening digital security through AI requires not only technological investment but also appropriate institutional and regulatory safeguards.

The findings also support the relevance of Complex Interdependence Theory. Nigeria's digital security environment is connected to regional organizations, international technology providers, transnational cyber threats, and global digital infrastructure. Regional cooperation through ECOWAS and the African Union provides opportunities for information sharing, capacity building, and coordinated responses to cyber threats. At the same time, dependence on external technologies and infrastructure creates vulnerabilities that may constrain Nigeria's strategic autonomy. This confirms that digital security in the contemporary international system cannot be managed exclusively through national mechanisms.

The findings further demonstrate the importance of digital sovereignty as an analytical concept. Nigeria's efforts to develop domestic AI institutions and technological capabilities suggest an attempt to strengthen technological autonomy. Nevertheless, sovereignty in the digital environment does not necessarily require complete technological independence. Rather, it involves the capacity to exercise meaningful control over critical data, infrastructure, technologies, and security decisions while participating in international technological networks. Nigeria's challenge is therefore to balance the benefits of technological interdependence with the need to protect national security and strategic autonomy.

Taken together, the findings suggest that AI is gradually transforming the international order. This transformation is reflected not simply in the emergence of new technologies but in changing patterns of technological power, security cooperation, dependence and sovereignty. Nigeria's experience shows that developing countries actively participate in this process, though technological and institutional inequalities shape their capacity to influence it. The Nigerian case therefore extends existing scholarship by linking AI adoption to digital security governance, state capacity, digital sovereignty, and international cooperation in a developing-country context.

5.1 Implications of the Findings

The findings have three major implications. First, AI governance should be integrated with digital security governance rather than treated solely as an economic or innovation policy issue. Second, Nigeria's security capacity will increasingly depend on investment in infrastructure, technical expertise, data governance, and institutional coordination. Third, regional and international cooperation remains essential, but such cooperation should be structured in ways that strengthen rather than undermine Nigeria's technological agency.

Overall, the evidence supports the argument that AI is not simply changing the tools available to security institutions; it is changing the governance structures, dependencies, and relationships through which security is organized. This provides the basis for the policy recommendations and conclusion that follow.

© 2026 The Authors. Published by Bexford Publishing Ltd

5.2 Policy Recommendations

Based on the findings, the study recommends the following:

1. **Integrate AI governance with national digital-security policy.** Nigeria should better align its AI governance framework with existing cybersecurity and national-security policies. AI-related security applications should follow clear standards for risk assessment, accountability, transparency, data protection, and human oversight.
2. **Strengthen institutional and technical capacity.** The government should increase investment in digital infrastructure, computing capacity, cybersecurity systems, and specialized human resources. Greater collaboration among NITDA, NCAIR, cybersecurity institutions, security agencies, universities, and the private sector would help translate AI policy objectives into effective security capabilities.
3. **Promote digital sovereignty and indigenous AI capacity.** Nigeria should continue developing locally relevant AI models, datasets, research capacity and digital infrastructure while reducing unnecessary dependence on foreign technologies. This does not require technological isolation; rather, international partnerships should be structured to facilitate knowledge transfer, skills development and sustainable domestic capacity.
4. **Strengthen regional AI and cybersecurity cooperation.** Nigeria should deepen cooperation within ECOWAS and the African Union on cyber-threat intelligence sharing, AI governance, technical capacity building, incident response, and digital-security standards. Regional mechanisms should also support coordinated responses to emerging AI-enabled security threats.
5. **Promote Nigeria's participation in global AI governance.** Nigeria should play a more active role in international discussions on AI governance, cybersecurity, and digital sovereignty. Its participation should promote the interests of developing countries, particularly equitable access to AI infrastructure and expertise, responsible AI standards, data governance, and a more inclusive international digital order.

6. Conclusion

Artificial intelligence is increasingly transforming the nature and governance of contemporary security. This study examined how this transformation is unfolding in Nigeria and its implications for state capacity, digital sovereignty, regional security cooperation, and the evolving international order. The findings indicate that Nigeria has begun incorporating AI into its broader digital security governance through national cybersecurity policies, emerging AI institutions, technological capacity-building initiatives, and consideration of AI applications in threat detection, intelligence, and other security functions. However, the transformation remains gradual and is constrained by infrastructural, institutional, technical, and regulatory limitations.

The study further demonstrates that AI presents a dual challenge for Nigeria. On the one hand, it offers opportunities to strengthen security institutions through improved data analysis, threat detection, intelligence processing, and early-warning capabilities. On the other hand, dependence on external technologies, infrastructure and expertise can create new vulnerabilities and constrain digital sovereignty. Nigeria's experience therefore suggests that technological adoption alone does not guarantee stronger security capacity; effective governance, institutional capability and domestic technological capacity are equally important.

The analysis also shows that Nigeria's digital security environment is increasingly shaped by regional and international interdependence. Cyber threats, digital infrastructures, AI technologies and data networks extend beyond national borders, making cooperation through regional and international institutions

© 2026 The Authors. Published by Bexford Publishing Ltd

essential. At the same time, growing competition over AI, computing infrastructure, data and technological capabilities is creating new forms of strategic dependence and geopolitical influence.

The study concludes that AI should be understood not merely as a technological innovation but as a transformative force in digital security governance and international relations. Nigeria's experience shows how a developing state can benefit from AI-enabled security capabilities, confront the challenges of technological dependence, and seek greater digital sovereignty within an increasingly interconnected international system. The transformation of the international order is therefore occurring not only through competition among major technological powers but also through the changing capacity and agency of developing states such as Nigeria.

Ultimately, Nigeria's ability to benefit from AI while protecting its security interests and technological autonomy will depend on effective governance institutions, indigenous technological capacity, responsible AI regulation, and meaningful regional and international cooperation. An inclusive international digital order will require developing countries to move beyond being primarily consumers of emerging technologies and participate more actively in shaping the rules, standards and institutions that govern them.

References

African Union. (2024). *Continental artificial intelligence strategy*. African Union strategy document

Akujobi, C., Ogwueleka, F., Aimufua, G., & Bassey, S. (2026). Cyber fraud in Nigerian banks: Trends, regulatory gaps, and mitigation strategies (2020–2025). *Engineering and Technology Journal, 11*(1), 8575–8580. https://doi.org/10.47191/etj/v11i01.18

Almahmoud, Z., Yoo, P. D., Alhussein, O., Farhat, I., & Damiani, E. (2023). A holistic and proactive approach to forecasting cyber threats. *Scientific Reports, 13*, Article 9214. https://doi.org/10.1038/s41598-023-35198-1

Arakpogun, E. O., Elsahn, Z., Olan, F., & Elsahn, F. (2021). Artificial intelligence in Africa: Challenges and opportunities. In A. Hamdan, A. E. Hassanien, A. Razzaque, & B. Alareeni (Eds.), *The fourth industrial revolution: Implementation of artificial intelligence for growing business success* (pp. 375–388). Springer. https://doi.org/10.1007/978-3-030-62796-6_22

Arsenault, A. C., & Kreps, S. E. (2022). AI and international politics. In J. B. Bullock (Ed.), *The Oxford handbook of AI governance* (pp. 959–980). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780197579329.013.49

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: The false promise of digital sovereignty. *European Foreign Affairs Review, 27*(4), 415–434. https://doi.org/10.1080/09662839.2022.2101885

Chesterman, S., Gao, Y., Hahn, J., & Sticher, V. (2024). The evolution of AI governance. *Computer, 57*(9), 80–92. https://doi.org/10.1109/MC.2024.3381215

Costa-Barbosa, A., Herlo, B., & Joost, G. (2024). Digital sovereignty in times of AI: Between perils of hegemonic agendas and possibilities of alternative approaches. *Liinc em Revista, 20*(2), Article e7312. https://doi.org/10.18617/liinc.v20i2.7312

Deeks, A. S. (2023). *National security AI and the hurdles to international regulation*. Lawfare Research

© 2026 The Authors. Published by Bexford Publishing Ltd

Paper Series. Lawfare Research Paper

Economic Community of West African States. (2021). *Regional cybersecurity and cybercrime strategy*. ECOWAS Regional Cybersecurity and Cybercrime Strategy

Effoduh, J. O. (2026). Decolonizing the governance of artificial intelligence in Africa: From normative mimicry to epistemic sovereignty. *Science and Public Policy, 53*(2), 245–257. https://doi.org/10.1093/scipol/scag005

Falade, P. V., & Osho, O. (2025). *Nigeria's digital sovereignty: Analysis of cybersecurity legislation, policies, and strategies*. arXiv. https://doi.org/10.48550/arXiv.2601.06050

Federal Republic of Nigeria. (2021). *National cybersecurity policy and strategy 2021*. Office of the National Security Adviser. National Cybersecurity Policy and Strategy 2021

Gagliardone, I. (2024). Lock-out, lock-in, and networked sovereignty: Resistance and experimentation in Africa's trajectory towards AI. *Liinc em Revista, 20*(2), Article e7319. https://doi.org/10.18617/liinc.v20i2.7319

Gilbert, C., & Gilbert, M. A. (2024). Organizational and leadership aspects of cybersecurity governance. *International Journal of Research Publication and Reviews, 5*(12), 1174–1191. https://doi.org/10.55248/gengpi.5.1224.3429

Horvitz, E., Young, J., Elluru, R. G., & Howell, C. (2021). *Key considerations for the responsible development and fielding of artificial intelligence*. arXiv. https://doi.org/10.48550/arXiv.2108.12289

Huang, K., Madnick, S., Choucri, N., & Zhang, F. (2021). A systematic framework to understand transnational governance for cybersecurity risks from digital trade. *Global Policy, 12*(S6), 625–638. https://doi.org/10.1111/1758-5899.13014

Jude, O. (2025). Cybersecurity and Nigeria's role in combating transnational digital threats. *Irish International Journal of Law, Political Sciences and Administration, 9*(5), Article 17296358. https://doi.org/10.5281/zenodo.17296358

Keohane, R. O., & Nye, J. S. (1977). *Power and interdependence: World politics in transition*. Little, Brown.

Madubuko, C. C., & Chitsungo, C. (2024). The evolution of China's cyber-espionage tactics: From traditional espionage to AI-driven cyber threats against critical infrastructure in the West. *American Journal of International Relations, 9*(4), 25–50. https://doi.org/10.47672/ajir.2424

Maleh, Y., Sahid, A., & Belaissaoui, M. (2021). A maturity framework for cybersecurity governance in organizations. *EDPACS, 63*(6), 1–22. https://doi.org/10.1080/07366981.2020.1815354

Meleouni, C., & Efthymiou, I. P. (2023). Artificial intelligence and its impact in international relations. *Journal of Politics and Ethics in New Technologies and AI, 2*(1), Article e35803. https://doi.org/10.12681/jpentai.35803

Meleouni, C., & Efthymiou, I. P. (2024). The use of artificial intelligence (AI) in national security: Defining international standards and guidelines. *Journal of Politics and Ethics in New Technologies and AI, 3*(1), Article e37847. https://doi.org/10.12681/jpentai.37847

Mügge, D. (2024). EU AI sovereignty: For whom, to what end, and to whose benefit? *Journal of European Public Policy, 31*(8), 2200–2225. https://doi.org/10.1080/13501763.2024.2318475

© 2026 The Authors. Published by Bexford Publishing Ltd

National Center for Artificial Intelligence and Robotics. (n.d.). *National Center for Artificial Intelligence and Robotics*. NCAIR

National Information Technology Development Agency. (n.d.). *National Information Technology Development Agency*. NITDA

Ndrejaj, A., & Ali, M. (2022). Artificial intelligence governance: A study on the ethical and security issues that arise. In *2022 International Conference on Computing, Electronics & Communications Engineering (iCCECE)* (pp. 112–117). IEEE. https://doi.org/10.1109/iCCECE53966.2022.9842535

Njoroge, J. W. (2024). Potential role of the African Union in the development of AI governance across the continent. *European Journal of Social Sciences Studies, 10*(4). https://doi.org/10.46827/ejsss.v10i4.1822

Organization for Economic Co-operation and Development. (2026). *AI governance in Africa: Insights from a policy dialogue with 12 countries*. OECD Publishing. OECD AI governance in Africa

Organization for Economic Co-operation and Development. (2026). *National Artificial Intelligence Strategy (NAIS)*. OECD.AI. OECD.AI National Artificial Intelligence Strategy

Posey, M., Fellows, W., Lenoir, T., & Vaden, H. (2026, August 1). *Compute sovereignty: The strategic importance of digital infrastructure*. S&P Global. S&P Global report

Roberts, H. (2024). Digital sovereignty and artificial intelligence: A normative approach. *Ethics and Information Technology, 26*, Article 70. https://doi.org/10.1007/s10676-024-09810-5

Sayler, K. M. (2019). *Artificial intelligence and national security* (CRS Report No. R45178). Congressional Research Service. Congressional Research Service report

Srivastava, S., & Bullock, J. (2024). *AI, global governance, and digital sovereignty*. SSRN. https://doi.org/10.2139/ssrn.4996387

Tzimas, T. (2021). AI and international security: The case of AWS and the collective security system. In *Legal and ethical challenges of artificial intelligence from an international law perspective* (pp. 149–165). Springer. https://doi.org/10.1007/978-3-030-78585-7_7

Wakunuma, K., Ogoh, G. I., Eke, D. O., & Akintoye, S. (2022). Responsible AI, SDGs, and AI governance in Africa. In *2022 IST-Africa Conference Proceedings* (pp. 500–512). IEEE. https://doi.org/10.23919/IST-Africa56635.2022.9845598

Zukis, B. (2022). Digital and cybersecurity governance around the world. *Annals of Corporate Governance, 7*(1), 1–92. https://doi.org/10.1561/109.00000032

© 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the **Creative Commons Attribution (CC BY 4.0) licence** (https://creativecommons.org/licenses/by/4.0/)