International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Institutional Readiness for the Adoption of Artificial Intelligence in Cybersecurity: The Case Study of Ghana

Eugenia Aba Moses

Ghana Armed Forces Command and Staff College

Abstract

Artificial Intelligence (AI) is increasingly transforming cybersecurity practices worldwide, offering advanced capabilities in threat detection, incident response, and predictive analytics. This study examines Ghana's institutional readiness for AI adoption in cybersecurity using secondary data and policy analysis grounded in the Technology–Organization–Environment (TOE) framework. Findings indicate that Ghana has made significant progress in cybersecurity governance, achieving Tier 1 status in the Global Cybersecurity Index. However, gaps remain in technical capacity, research infrastructure, and human capital. The study concludes that while Ghana demonstrates strong policy readiness, institutional strengthening is required for effective AI-driven cybersecurity implementation.

1. Introduction

The rapid evolution of digital technologies has transformed the global cybersecurity landscape. Artificial intelligence (AI) has emerged as a critical tool for detecting cyber threats, predicting attacks, and automating defensive responses. For developing economies, AI integration presents both opportunities and challenges, particularly in institutional readiness, infrastructure, and human capital.

2. Literature Review

AI has reshaped cybersecurity strategies globally through predictive analytics and automation. In Africa, debates focus on AI governance, digital sovereignty, and dependence on foreign technologies. Scholars emphasize the need for locally driven AI ecosystems, strong regulatory frameworks, and ethical governance. The Technology–Organization–Environment (TOE) framework explains adoption through technological, organizational, and environmental factors, making it suitable for analyzing Ghana's context.

3. Methodology

This study adopts a qualitative approach using secondary data and policy analysis. Data sources include international indices, Ghanaian policy documents, institutional reports, and academic literature. Thematic analysis was conducted using the TOE framework to assess technological, organizational, and environmental readiness. The TOE framework was selected due to its comprehensive ability to capture institutional and contextual dynamics influencing AI adoption.

4. Ghana's Cybersecurity Landscape

Cybercrime remains a significant concern in Ghana due to the expansion of digital services. The government has established institutions such as the Cyber Security Authority and enacted the Cybersecurity Act 2020 to strengthen national resilience.

5. Artificial Intelligence Development in Ghana

Ghana is advancing AI through national strategies and international collaborations. Initiatives emphasize ethical AI, innovation, and sectoral integration including cybersecurity.

6. Institutional Readiness for AI-Driven Cybersecurity in Ghana

Ghana has improved digital infrastructure but still lacks advanced AI capabilities. Human capital limitations and insufficient research facilities hinder adoption, despite growing technological ecosystems.

7. Challenges to AI Adoption

Challenges include limited infrastructure, high costs, skills shortages, and fragmented data governance. Institutional resistance and regulatory gaps further constrain adoption.

8. Policy Recommendations

Key recommendations include expanding AI education, investing in research infrastructure, strengthening data governance, enhancing regulatory frameworks, and promoting public–private partnerships.

9. Conclusion

Ghana demonstrates strong policy readiness for AI in cybersecurity but faces operational challenges. Addressing infrastructure, skills, and governance gaps is essential for effective implementation and national digital resilience.

References

1. Anomah, S. (2025). Assessing institutional readiness for AI adoption in Ghana.
2. African Union. (2023). Digital Transformation Strategy for Africa.
3. Brynjolfsson, E., & McAfee, A. (2017). Machine, platform, crowd.
4. International Telecommunication Union. (2024). Global Cybersecurity Index.
5. Kshetri, N. (2021). AI in cybersecurity.
6. Ministry of Communications and Digitalisation. (2024). AI Readiness Report.
7. Netwrix. (2025). Cybersecurity Trends.
8. OECD. (2023). AI governance.
9. UNESCO. (2023). AI readiness methodology.
10. World Bank. (2022). Digital Development Report.
11. Zuboff, S. (2019). Surveillance capitalism.