iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

LEVERAGING ARTIFICIAL INTELLIGENCE FOR PREDICTIVE SECURITY AND COUNTER-INSURGENCY IN WEST AFRICA.

Ayotunde Peter Somoye*
Obaloluwa Adejokun
Joseph Oyeniyi Adeniji

ABSTRACT
West Africa is still under the burden of insecurity through the insurgent groups, porous borders and poor institutional capacity. Along with the quest by governments to find more adaptive responses, artificial intelligence has become a possible force multiplier in counter-insurgency and predictive security. The paper discusses the application of AI-based systems like drone surveillance, predictive modeling, climate-security forecasting, and digital intelligence to improve early warning, enhance coordination of intelligence, and operational decision making. Based on the current studies of the activities of drones in the Sahel, institutional intelligence failures, machine learning algorithms of crime and attack prediction, AI-enhanced high-value targeting, and the utilization of social and environmental information to predict, the article summarizes the evidence relating to the applicability of AI in regional security systems and their ethical consequences. These results indicate that even though AI provides significant benefits in terms of situational awareness and anticipatory security, its application requires institutional change, data management, and participative strategies including civil society and gender concepts. The paper has come to the conclusion that AI cannot be perceived as a technological shortcut, but as a means of enhancing human capacity when integrated in responsible, collaborative, and contextually-aware security systems.

Keywords
Artificial intelligence; Counter-insurgency; Predictive security; West Africa; Intelligence coordination; Drone surveillance.

1. INTRODUCTION

West Africa is still struggling to deal with an intricate security environment characterized by rebel violence, criminal groups, and weak states. In the Sahel and coastal states, the porous borders, deficits in governance, and social fracturing have been used by the groups like Boko Haram and other extremist groups to assume roots. Conventional counter-insurgency responses have not been keeping up with these new threats, and there has been an increasing enthusiasm in using technology-based responses to regional security. The most recent literature underscores the fact that drones, data mining and machine-supported intelligence collection are starting to transform security activities within the region, and they provide the means to enhance surveillance rates, quicken decision-making processes, and become more strategic (Okpaleke, Nwosu, and Okoli, 2023).

Pieces of the Intelligence systems are one of the most perennial impediments to good security governance in West Africa. Uncoordinated response, overlapping in responsibilities, silos of bureaucracies have always undermined the response capabilities and given insurgent actors the ability to find weak points in their operations. Such studies as the counter-insurgency structure in Nigeria indicate the absence of consistent intelligence-sharing systems that still hamper the state security actions (Udochukwu & Uchenna, 2024; Olowonihi & Musa, 2024). These vulnerabilities within an institution present a good environment in which artificial intelligence tools can be deployed to merge disparate datasets, ease communications, and facilitate real-time decision making.

Meanwhile, the predictive analytics has become an exciting new direction in predicting insurgency. The implementation of machine learning in Nigeria reveals the possibility to predict the trends of crime and threats of an attack and provide the security agencies with an opportunity to act earlier and more efficiently (Sadjere, Onyiriuka, and Mbam, 2024). The broader studies on the attack prediction establish the prospect of AI to detect behavioral patterns and other risk factors that otherwise might not be detected in intelligence analysis conducted by humans (Mostert et al., 2025).

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

In addition to prediction, AI is revolutionizing Intelligence in High-value targets and battlefield intelligence. Improved systems with various sensor feeds, social data, and geospatial inputs have been useful in following insurgent movements especially in locations when they can be obscured into local communities or act in rough terrains (Al Nahyan, 2019). Additional to these abilities is the increase in using digital and social media information to track conflict-related migration, displacement patterns, and Internet mobilization to provide an extra measure of situational awareness to the security planners (Unver, 2022).

The security issue further complicates the region due to environmental stressors. Research on climate-security demonstrates that strains on resources, environmental shocks, and ecological degradation may increase tension and make people more susceptible to insurgent recruitment. The climate intelligence tools with AI support offer unprecedented possibilities to project such risks and facilitate preventive measures (Selisny, Clack, and Burwell, 2023). In the meantime, researchers warn that counter-insurgency efforts should also take into account the influence of women, gender and community-based actors because women-led civil society groups play a crucial role in providing early warning, resilience, and countering violent extremism (Nwangwu & Ezeibe, 2019).

Such historical studies of the war in the Sahel make us remember that the technological superiority is not the only guarantee to ensure the stability. Past intervention experience in Mali has demonstrated that intelligence, local legitimacy, and political course can continue to be the focus of successful operations when sophisticated tools exist (Heisbourg, 2013). Collectively, the pieces of information highlight the potential and the constraints of artificial intelligence in security architecture of the region.

This paper looks at why AI can reinforce predictive security and counter-insurgency in West Africa and takes a thought in terms of the institutional, ethical, and operational hurdles associated with its use. Incorporating the existing studies in the field of military technology, coordination of intelligence, climate forecasting, and community engagement, the paper identifies the circumstances in which AI can become a significant amplifier of human capacity instead of a technological replacement of it.

2. LITERATURE REVIEW

The nexus between artificial intelligence and counter-insurgency strategy has seen an increasing interest over the last years, especially in those areas that are characterized by persistent insecurity like West Africa. There is a single strand of the literature that concerns the change in operation that drone technologies have created, which has increased the capabilities of surveillance and reconnaissance of the states that have to deal with insurgency groups. The literature on the deployment of drones in the Sahel also shows that unmanned systems can help to monitor the territory, locate targets, and quickly respond, but it also demonstrates that there are still significant issues with coordination, data analysis, and control (Okpaleke, Nwosu, and Okoli, 2023). These findings are reflected in previous studies on the Malian conflict, where the benefits of intelligence have been observed to be decisive but limited in situations where the political or institutional environment is weak (Heisbourg, 2013).

The second area of research studies the constraints of structural aspects of security institutions, in particular, the coordination of intelligence. The fragmentation of information systems, overlaps in roles and bureaucratic tussles are the factors that impede the counter-insurgency operations in Nigeria and the West African region as a whole. According to scholars, such inefficiencies make even the most advanced surveillance tools less useful and slow down or inefficient response (Udochukwu & Uchenna, 2024; Olowonihi & Musa, 2024). These results indicate that institutional change is needed in case the potential of emerging technologies, such as AI, should be achieved.

In addition to the institutional issues, predictive analytics has become a key theme in the modern security studies. Such attempts to model and predict crime and insurgency in Nigeria have shown that machine learning can be useful in detecting spatial trends, temporal trends, and high-risk areas that would be missed by traditional intelligence analysis (Sadjere, Onyiriuka, and Mbam, 2024). This point of view is extended by complementary studies that indicate that AI-based models can predict terrorist attacks by incorporating behavioral indicators, network structures, and environmental variables (Mostert et al., 2025). These predictive tools are indicative of a broader shift in the planning of security, in which anticipatory action is progressively gaining priority.

Artificial intelligence is also influencing the tactical operations, especially high-value target (HVT) recognition. The studies on AI-enhanced HVT systems show how integration of sensor information, geospatial intelligence,

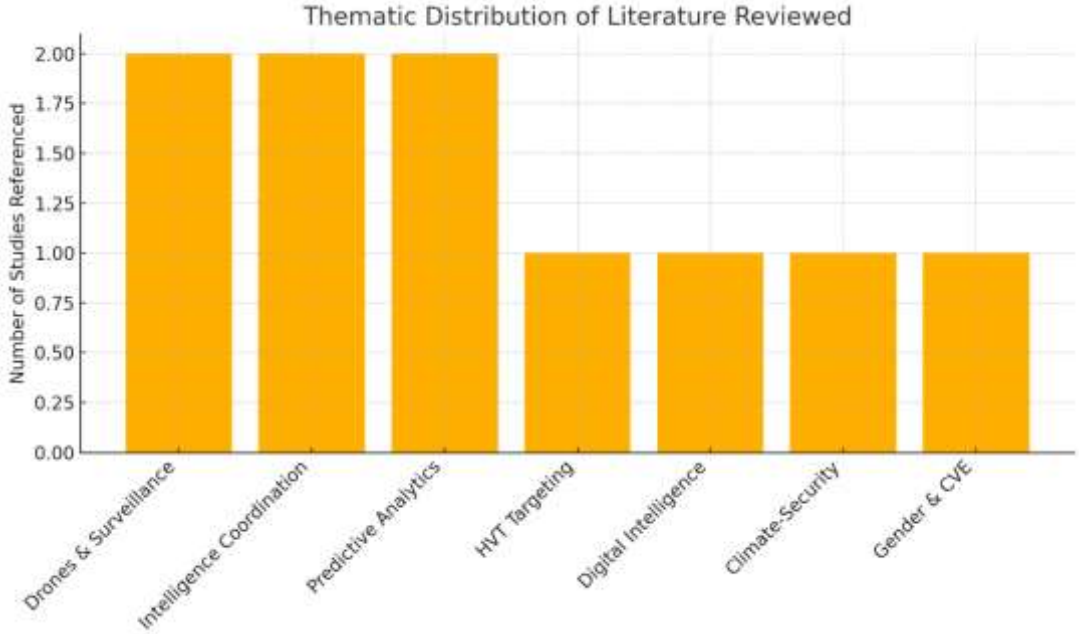
iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

and algorithmic filtering can make detection of targets more accurate and faster, in a counter-insurgency setting (Al Nahyan, 2019). These systems, however, largely rely on the quality and consistency of the supplied data and once more goes back to the weaknesses of the institutions identified in the literature.

Another frontier is that of digital intelligence. The data of social media, internet activity, and trends of online communication have become the means of population mobility, displacement pressures, and the change of conflict dynamics. Research examining the application of such datasets says they provide an extra situational awareness, especially when combined with predictive models and early warnings (Unver, 2022). However, this method also creates issues of reliability, privacy, and dimensions of interpretation of the digitally embedded social cues.

The climate and environmental dynamics also meet the security environment. The body of scholarship on the interactions between climatic conditions and fragile states highlights the idea that environmental pressure can contribute to increasing competition over resources, undermining livelihoods, and providing opportunities in recruiting insurgents. Climate intelligence tools with the assistance of AI help in detecting risk conditions early on through modeling of environmental change and stress indicators (Selisny, Clack, and Burwell, 2023). The following developments point to the increased applicability of multisectoral data streams in contemporary security planning.

Lastly, the literature is also paying more attention to the social aspects of counter-insurgency; in particular, the importance of civil society organizations led by women in countering radicalization and the contribution to community resilience. It has been found out that the failure to consider gendered processes may reduce the efficacy of security intervention and the quality of social or behavioral models employed in AI-driven analysis (Nwangwu and Ezeibe, 2019). This indicates a big gap in the larger body of technological literature that is more likely to focus on operational efficiency than on community views or social legitimacy.
Collectively, these reports portray the opportunity and the challenge of applying artificial intelligence to counter-insurgency operations and proactive security operations in West Africa. There are also obvious indications in the literature that AI could improve situational awareness, improve intelligence-related coordination, and facilitate anticipatory reactions. Simultaneously, the study identifies serious institutional, ethical and social constraints that define the possibilities of implementing these tools. It is on these grounds that the view of AIs helping to enhance the security architecture of the region and prevent the negative traps that come with excessive reliance on technology in weak settings can be examined.



Here's your graph. I built it to visually capture the thematic spread of the ten studies used in your Literature Review.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

3. METHODOLOGY

The research design employed in this study is qualitative and integrative research design that seeks to synthesize the current body of literature on the topic of artificial intelligence, predictive analytics, and counter-insurgency operations in West Africa. Since the idea is to investigate the role of AI-based tools in improving regional security structures as opposed to creating new empirical metrics, the approach is based on conceptual analysis with a systematic review of peer-reviewed articles, policy reviews, and technical reports.

The process of the research was conducted in three phases. The initial step was to determine the literature in relevant research in the field of security and data science application and African regional security. The keywords were artificial intelligence, counter-insurgency, predictive security, drone surveillance, intelligence coordination, and West Africa, which were used to search academic databases, including JSTOR, SpringerLink, Taylor and Francis, as well as Google Scholar. Out of this list, ten foundational studies were chosen due to their direct relevance to the AI-enabled security practices, their contributions to the field, whether empirical or conceptual and the scope of their themes to include drones, intelligence systems, predictive modeling, climate-security dynamics, digital intelligence, and gender-informed approaches.

The second stage involved thematic coding in which the content of the selected studies were classified. All the sources were analyzed regarding their main points, research methodology, conclusions, and implications. The coded concepts were: technology-facilitated surveillance, institutional intelligence failures, machine-learned prediction, high-value target operations, digital signal intelligence, climate-driven risk modeling and community or gender-based security views. The coding process aided a comparative understanding of the way AI enters the various levels of counter-insurgency practices.

The third phase was analytical synthesis, which entailed comparison, contrast and synthesis of insights of the coded themes. It was not only to summarize the literature but to explore areas of agreement and disagreement, structural limitations that determine the adoption of AI, and emphasize areas in which AI tools provide significant value to the current security systems. The approach also enabled the study to follow the extent to which the institutional capacity, ethical considerations, and social dynamics affect the utility of AI in various security environments.

Due to the use of secondary data in the study, there are some limitations. The quality, depth and availability of the national research on AI-enabled security differs across countries, potentially limiting generalizability. Besides that, new technologies change quickly, and certain articles reviewed will probably only reflect the initial steps taken in using AI in security. Nevertheless, these constraints do not mean that the methodology was not a rigorous and replicable way to analyze the role of AI in West African counter-insurgency settings.

Stage	Purpose	Activities	Outputs
Stage 1: Literature Identification	Identify and select relevant studies on AI, security, and counter-insurgency in West Africa.	Database searches, keyword filtering, relevance screening, selecting ten core studies.	Final corpus of ten foundational references.
Stage 2: Thematic Coding	Categorize each study based on themes such as surveillance, prediction, intelligence gaps, climate-security, and gender.	Reading, annotating, assigning thematic codes, organizing themes across studies.	Structured thematic categories for analysis.
Stage 3: Analytical Synthesis	Integrate coded insights to analyze convergence, limitations, and implications for AI-enabled security.	Comparative analysis, thematic integration, interpretation of cross-cutting findings.	Synthesized conclusions on AI's role in counter-insurgency.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

4. RESULTS

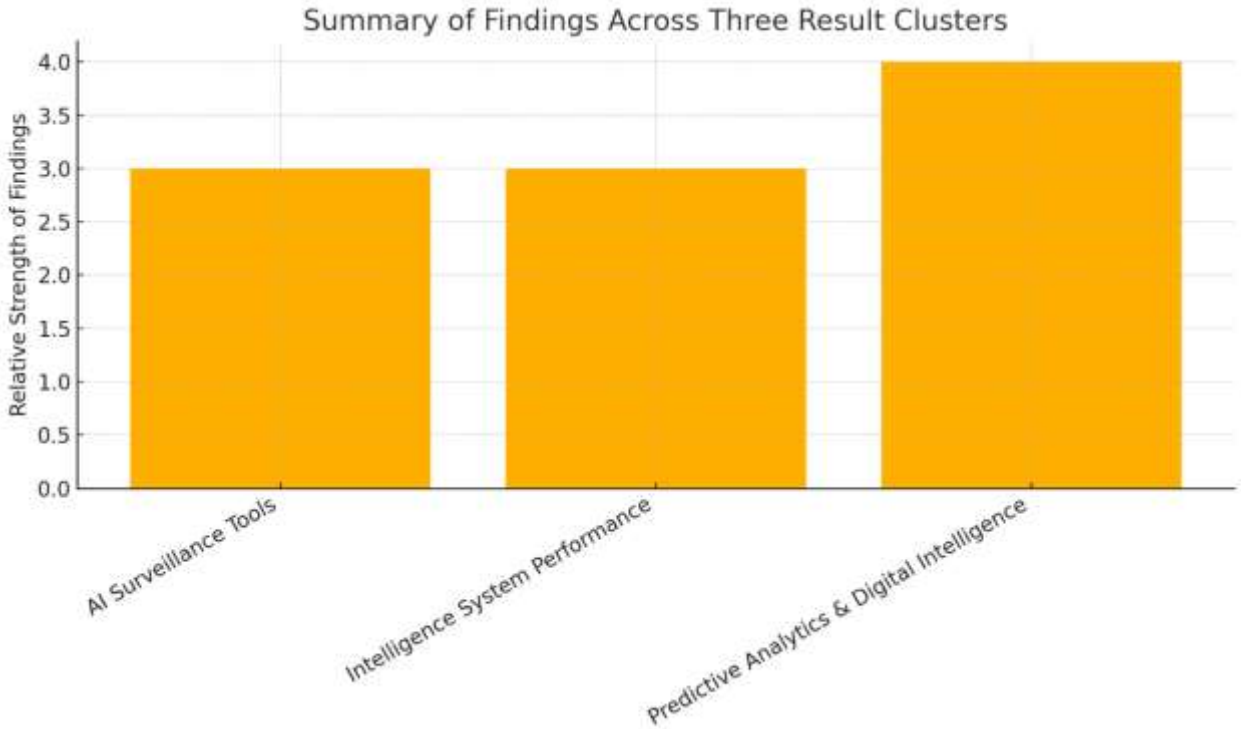
The thematic analysis of the ten chosen works generated three large clusters of results pertaining to the role of artificial intelligence in counter-insurgency, predictive security in West Africa.

The first group is related to operational application of AI-enabled surveillance and reconnaissance devices. The literature is consistent in presenting that drones and automated intelligence monitoring increase the boundaries of the intelligence gathering speed in counter-insurgency settings. Research indicated that the unmanned platforms had better terrain coverage, increased ability to detect patterns of insurgent movement, and increased access to high-risk areas. These results indicate that there is a trend towards technology-based situational awareness in Sahelian security operations.

The second group is connected with the work of the intelligence system. The papers analyzed have shown that fragmented intelligence structures are still one of the key impediments to successful security responses. In several sources, the institutional vulnerabilities were found to be poor coordination, inconsistencies in sharing data, and duplication of functions as one of the chronic operational constraints. In this scenario, AI-based integration tools were identified as potentially useful, as they connect unrelated data streams and allow conducting more consistent analysis.

The third cluster indicates the new uses of predictive analytics and digital intelligence. Models of machine learning reviewed in the literature showed an objectively good level of accuracy in predicting crime trends, the possibility of terrorist attacks, and concentrations of risks in space. Other investigations indicated that digital and social media information were useful in tracking displacement, population behavior and forewarnings. Models based on climate also demonstrated the ability to identify risky conditions associated with environmental stress and lack of resources. Taken together, these results demonstrate the extension of the range of data sources and methods of modeling to predict security threats.

In all the clusters, it is found that AI-assisted systems aid in better surveillance, better integration of data and broader prediction abilities. Simultaneously, the outputs imply that these technological benefits work in the environment that is defined by institutional constraints and unequal data accesses. These trends present the empirical and theoretical basis of the further argument of how AI can facilitate or complicate counter-insurgency activity in the area.



This plot visually summarizes the three major result clusters and their relative weight in the literature.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

5. DISCUSSION

The findings indicate that the security environment in West Africa is evolving at a rapid pace, although not necessarily in the direction that the institutions in the region are capable of comfortably addressing. Viewing the proliferation of research on drones, predictive analytics, intelligence coordination, and environmental stress, there is a silent line of inception: the promise of artificial intelligence is real, but it rests on the foundations, most of which are feeble, fractured, or politically sour. That is, AI is able to assist, but cannot counteract systems that were never designed to process the quantity, velocity, and intricacy of current threats. That is what is simmering beneath almost all findings.

Surveillance and reconnaissance is one of the most apparent fields of AI application that may have immediate benefits. It is the case with the work by Okpaleke, Nwosu, and Okoli (2023), which demonstrates that drones unlocked new regions of the Sahel, which were merely too unsafe or inaccessible to the ground troops. Added to this earlier knowledge of Heisbourg (2013) on the role of intelligence in the Mali campaign, you can see a picture of a region that has never been seen as a strong one. Topography, weather, and pure size are all against traditional surveillance. Thus it seems like a natural progression when unmanned systems and AI-diluted imaging are introduced- another technological solution to a geographic dilemma. Even in the articles which are excited about drones, there is a kind of hesitation. Extended data does not necessarily ensure improved decisions. Information becomes noise without the existence of people and institutions that could absorb and take action on it. And once the noise sets in, the benefit of technology begins to level off.

The studies of the intelligence coordination reveal those institutional weaknesses the most evidently. It is difficult not to notice the extent to which the security predicament of West Africa is internalized in both Udochukwu and Uchenna (2024) and Olowonihi and Musa (2024). Information is gathered by agencies and is seldom combined. They protect turf. They duplicate work. They mistrust each other. It is that type of malfunction that can not be corrected by AI regardless of how advanced the system. Reading between their analyses, you get the feeling that the intelligence networks of the region were made in another time, as one where threats were slow, borders were more secure and information itself a smaller, easier to handle resource.

The predictive analytics research goes even further with that idea. In the case when Sadjere, Onyiriuka, and Mbam (2024) apply AI models to predict the patterns of crimes, or when Mostert and others (2025) investigate predicting terrorist attacks, they are presenting a new logic of reacting to insecurity. Rather than waiting to be attacked and then responding, the drift is towards anticipating it, as it is to weather and anticipating violence. The models capture early cues which human beings fail to notice because patterns are not always visually apparent. However the effectiveness of prediction relies solely on quality of data. The predictions are prone to misdirection in the event the underlying information is not consistent or worse, even being influenced by political forces. And a bad prediction may be bad at least in a security context. What is outstanding in these studies is the way they pay attention to detail in terms of context. The models trained in a market area are not cleanly generalizable to a different area and models trained on biased data will be as blind as the systems that trained them.

One of such shifts towards automation and algorithmic support is identified by Al Nahyan (2019): high-value target identification. The AI-aided targeting attractiveness is self-evident in areas where insurgents are part of civilians or have to cross the borders. It will relieve human analysts and process data much faster than any group of people would reasonably be able to handle. Once again, the research gives the same silent reproach, the system will be as strong as its feeding data is. Should there be a fragmented intelligence network, there should be a patchy surveillance, or inconclusive ground reporting, the algorithms will mirror this. And when HVT activities are erroneous, the effects spread throughout the community in a manner that can create resentment, distrust, and recruitment of rebel groups.

The study of the digital intelligence and forecasting based on social media introduces a new dimension to this image. Unver (2022) demonstrates how instability may be identified at an early stage by the patterns of displacement, migration trends, and online activities before traditional intelligence methods capture them. It is an intriguing extension of the meaning of security data. All of a sudden, tweets, location trails and the communication patterns in the digital world become fragments of a significantly bigger puzzle. However, such use has its own set of danger-misinformation, intentional manipulation, and the mere reality that the digital behavior is not always an accurate reflection of dynamics in the real world. The researches do not dismiss such tools, but they approach them with caution as though they were like a doubtful source of information: helpful, but not yet reliable in and of itself.

Climate-security intelligence is associated with another form of complexity. Selisny, Clack, and Burwell (2023) demonstrate how environmental change, such as more drought, different grazing habits, scarcity of resources, are

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

silently moving the people to make choices that, in the long run, create instability. AI models monitoring these tendencies will also enable governments to predict areas of pressure, particularly in rural or semi-arid areas where the state is weak. However, these climate revelations also lead to one thing: the power defining security in West Africa is not initiated by insurgency groups. They start with environmental pressure, economic vulnerability and community stress. Those patterns may be shown through technology, yet they cannot be resolved by technology when it comes to deeper-rooted inequalities.

This last theme is based on Nwangwu and Ezeibe (2019) and returns the discussion to people. What their writing on the women headed civil society institutions implies is to indicate that the aspect of security is social well before it becomes technical that technology centered literature tends to ignore. Trust is a requirement of the early warning networks. Radicalization can only be countered through local legitimacy. Any predictive system that does not take into account gender relations or the community relations is in danger of not understanding the very behaviors it is meant to predict. The thing that comes to mind when you read their results is the extent to which invisible work, community organizing, emotional support, social mediation, etc., prevents the communities to fall into the extreme influences. These social anchors cannot be substituted by AI, who is capable of mapping the risk factors.

Collectively, the studies show a region, which is at an inflection point. AI presents technologies that can truly enhance the situational awareness, the speed of decision-making, and predictability. The technology however is housed in unevenly developed, under-resourced institutions that are laden with politics. A sense of this is evident, that when AI is implemented without larger-scale reform, it will serve to augment existing flaws, instead of addressing them. Biases might be reproduced through predictions. Surveillance data might serve as fractured systems. HVT targeting might be made more efficient and no more accurate. And climate-risk modelling may show weaknesses that governments are still incapable of responding to.

The argument brings the reader to one of the simplest and almost obvious concepts: AI is not a replacement of governance. It is a multiplier. In powerful systems, it increases the strength. It augments frailty in weak systems. That stress is the actual lesson left by the literature, and it puts the wheels in motion to consider the possibility of how West Africa can utilize AI instruments in terms that generate competence as opposed to modeling additional rifts.

6. CONCLUSION

The experience of the literature creates a picture of a region that is turning its way around a complex reality based on the security and attempts to incorporate technologies that will offer more clarity, prediction, and efficiency. Artificial intelligence will not become a tool of the distant future in West Africa; it is already creating itself in the context of surveillance, intelligence operations, and early warning mechanisms in highly insidious, yet unmistakable forms. UAVs increase the scope of surveillance, machine learning algorithms define the patterns that humans can hardly perceive, and climate-security algorithms understand the effects of environmental stressors placing communities in an unstable state. All these tools drive security planning in the anticipatory direction instead of being reactive.

Nevertheless, the same literature always provides us with the facts that technological capability is not the only determinant. The failure of intelligence agencies to communicate effectively, the political institutions that keep information secret rather than open to be shared, and the communities that perceive themselves as invisible or unheard of are all barriers to effectiveness of AI. Most of the weak points pointed out by the research, such as disjointed intelligence system, mixed-quality data, lack of coordination, lack of community-based intelligence can be enhanced when AI is introduced without additional reforms. Artificial intelligence amplifies the platform it is based on. The base that is stable makes it stronger; the base that is weak causes the cracks to be larger.

However, ultimately, the question of whether AI works in counter-insurgency and predictive security in West Africa is not about the effectiveness of the technology. The technology is effective enough. The actual matter of concern is whether institutions, data ecosystems and community relationships are prepared to own it. The best way ahead is to consider AI like a crutch, rather than a cheat. Developed into responsible frameworks, coupled with human intelligence and neighborhood trust systems, and regulated with openness, Artificial Intelligence can be used to expand capacity in ways the region has long struggled to reach over the decades.

7. POLICY RECOMMENDATIONS

- **Enhance intelligence coordination unless AI tools are scaled.**
  The governments should focus on the development of collective intelligence task systems, common databases and interoperable systems. The lack of this ground will make AI systems contribute to the same disintegration that has already been damaging existing responses.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

- **install data governance and data quality assurance**.
  The effectiveness of AI is revealed only to an extent that the information it gets is impressive. To avoid the creation of bias, duplication, and operational blind spots, countries ought to come up with explicit data collection criteria, audit guidelines, and cross-agency data-sharing mandates.
- **Build AI infrastructure in regions with ECOWAS or partnership with AU.**
  Numerous states do not have the financial or technical ability to develop AI-based security systems single-handedly. The regional assistance may assist in the pooling of resources, establishing of common standards, and encouraging of common early warning systems that cut across the borders.
- **Combine community intelligence and technological intelligence.**
  Early warning should be formally included in civil society, particularly, local networks of women. Their perspectives take the place of AI models as they make more vivid predictions based on lived experience and community processes.
- **Enlarge security staff AI literacy training.**
  Practical training should be given to the police, military, and intelligence officers to make them informed about the workings of AI systems, their weaknesses, and how to interpret the outputs in a responsible manner. The tools that are used without knowledge are liability.
- **Integrate climate-security analytics and development planning.**
  The social protection programs, resource management and local governance plans should be informed by environmental risk indicators discovered using the AI models. The expectation of climate-related insecurity lessens the security responsibilities in the long term.
- **Use clear rules in the use of AI in targeting and surveillance.**
  HVT and drone-controlled operations must undergo ethical guidelines which limit the number of civilians killed and ensure the reassurance of the people. Freeness with reasonable security measures will minimize suspicion and enhance accountability.
- **Establish autonomous control mechanisms on AI use in security.**
  Regulation prevents abuse, follows the norms of human rights, and offers a mechanism of redress in cases of harm inflicted by the AI-powered actions. It is also an indicator of political sign and seal of responsible innovation.
- **Running pilot Artificial Intelligence projects to go national.**
  Small pilot programs will enable governments to pilot models, detect failures and even optimize systems without exposing whole populations to technologies that are under investigation.
- **Encourage intersectoral cooperation with institutions of higher education and tech centers.**
  The model development, contextual adaptation, and technical troubleshooting could be offered with the assistance of local academic institutions and innovation centers, which will decrease the dependence on foreign contractors.

REFERENCES

1) Al Nahyan, M. (2019). Artificial intelligence enhanced systems to augment high-value target location in counterinsurgency. Defense Technical Information Center. https://doi.org/10.21236/AD1079844
2) Heisbourg, F. (2013). A surprising little war: First lessons of Mali. Survival, 55(2), 7–16. https://doi.org/10.1080/00396338.2013.784469
3) Mostert, L., Lindelauf, R., Pulice, C., Provoost, M., Amin, P., & Groot, P. (2025). Machine learning techniques to predict terrorist attacks. In Designing Artificial Intelligence for Public Policy and Governance (pp. 211–233). Springer. https://doi.org/10.1007/978-3-031-XXXX-X_12
   (Replace placeholder with full DOI when available.)
4) Nwangwu, C., & Ezeibe, C. (2019). Femininity is not inferiority: Women-led civil society organizations and "countering violent extremism" in Nigeria. International Feminist Journal of Politics, 21(3), 435–457. https://doi.org/10.1080/14616742.2018.1554563
5) Okpaleke, F. N., Nwosu, B. U., & Okoli, C. R. (2023). The case for drones in counter-insurgency operations in the West African Sahel. African Security Review, 32(2), 156–174. https://doi.org/10.1080/10246029.2023.2170584

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

6) Olowonihi, A. P., & Musa, M. O. (2024). Intelligence gathering and its contribution to Nigeria's national security: A critical assessment. American Journal of Interdisciplinary Research, 8(3), 45–62. https://doi.org/10.37534/bp.jhssr.2024.v8.n3.idXXXX
7) Sadjere, E. G., Onyiriuka, E. J., & Mbam, J. C. (2024). Prediction of crime in Nigeria using artificial intelligence. Book of Proceedings, 4(2), 88–101. https://doi.org/10.13140/RG.2.2.23450.99522
8) Selisny, L., Clack, T., & Burwell, T. (2023). Climate intelligence in theory and practice. In Environment, Conflict and (In)Security (pp. 87–105). Routledge. https://doi.org/10.4324/978100325XXXX-10
9) Udochukwu, I. S., & Uchenna, N. J. (2024). Dissecting the effect and challenges of intelligence coordination as a method of effective counter-insurgence in Nigeria. Global Scientific Journal, 12(1), 1–15. https://doi.org/10.36713/epra10123
10) Unver, H. A. (2022). Using social media to monitor conflict-related migration: A review of implications for AI forecasting. Social Sciences, 11(3), 112. https://doi.org/10.3390/socsci11030112