ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar092

# Banditry and National Development in Nigeria: A Spatio-Temporal Machine Learning Approach to Conflict Prediction

Musa Tanimu Karatu[1]; Dauda John Tanimu[2]

[1]Department of Computer Science, Federal University Birnin Kebbi, 860222, Nigeria
[2]Department of History and War Studies, Nigerian Defence Academy, Nigeria

Publication Date: 2026/03/13

**Abstract: Banditry has emerged as one of the most severe internal security challenges confronting Nigeria, with far-reaching implications for national development, governance, and social stability. This study applies spatio-temporal machine learning techniques to analyse and predict patterns of banditry incidents across Nigerian Local Government Areas (LGAs) between 2015 and 2024. Drawing on Routine Activity Theory, Social Disorganisation Theory, and Government–Development Theory, the research integrates socio-economic, environmental, and security-related variables with historical conflict data comprising over 20,000 recorded incidents. A comparative modelling framework using Random Forest (RF), Long Short-Term Memory (LSTM), and Convolutional LSTM (ConvLSTM) models is implemented to capture non-linear relationships, temporal dependencies, and spatial diffusion of violence. Results indicate that ConvLSTM outperforms other models in forecasting high-risk locations and attack severity, demonstrating the value of Spatio-temporal deep learning for conflict prediction. The findings reveal persistent hotspots in areas characterised by weak state presence, high poverty levels, arms proliferation, and recurrent attack cycles. The study concludes that machine-learning-driven early-warning systems can enhance proactive security planning, optimised resource allocation, and mitigate the developmental impacts of banditry in Nigeria.**

***Keywords:*** *Banditry; National Development; Conflict Prediction; Machine Learning; Spatio-Temporal Analysis; Nigeria.*

**How to Cite:** Musa Tanimu Karatu; Dauda John Tanimu (2026) Banditry and National Development in Nigeria: A Spatio-Temporal Machine Learning Approach to Conflict Prediction. *International Journal of Innovative Science and Research Technology*, 11(3), 396-405. https://doi.org/10.38124/ijisrt/26mar092

## I. INTRODUCTION

Banditry, encompassing armed robbery, kidnapping, cattle rustling, village raids, and coordinated attacks on rural communities, has escalated into one of the most critical internal security challenges confronting Nigeria. Although banditry is not entirely new to the Nigerian socio-political landscape, its scale, sophistication, and geographic spread have intensified markedly since the mid-2010s, particularly in the North-West and North-Central regions [6, 13]. What were once sporadic criminal acts have evolved into organised, heavily armed networks capable of mass abductions, territorial control, and sustained violence against civilians and state institutions.

The implications of this phenomenon extend far beyond immediate security concerns. Persistent banditry has disrupted agricultural production, displaced millions of rural dwellers, weakened local governance structures, and diverted public expenditure from development to security operations [13, 1]. Nigeria's ambition for sustainable development is therefore directly threatened by the persistence of insecurity, particularly in regions that constitute the country's agricultural and mineral backbone.

Despite extensive scholarly attention to the drivers and impacts of banditry, most existing studies remain largely descriptive, focusing on socio-economic causes, governance failures, and humanitarian consequences [10]. Comparatively little emphasis has been placed on predictive, data-driven approaches capable of anticipating future attacks and supporting proactive security planning. In line with emerging global trends in predictive policing and conflict analytics, this study applies Spatio-temporal machine learning techniques to analyse and forecast banditry incidents across Nigerian Local Government Areas (LGAs).

By integrating socio-economic, environmental, and security-related variables with historical conflict data, the study seeks to demonstrate how artificial intelligence can support evidence-based security decision-making. The central contribution of this research lies in its comparative evaluation of Random Forest (RF), Long Short-Term Memory (LSTM), and Convolutional LSTM (ConvLSTM) models for conflict prediction, and in its articulation of policy-relevant insights for strengthening national development through proactive security management.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar092

## II. RELATED LITERATURE

➢ *Drivers of Banditry in Nigeria*

The literature identifies banditry in Nigeria as a product of interrelated socio-economic, political, environmental, and security factors. Widespread poverty and youth unemployment, particularly in rural northern Nigeria, have created conditions conducive to criminal recruitment, as young people with limited livelihood opportunities turn to illicit activities for survival [11]. Weak governance and institutional fragility further exacerbate the problem, as corruption, poor service delivery, and limited state presence erode public trust and allow criminal networks to operate with relative impunity [1].

Arms proliferation constitutes another critical driver. Nigeria's porous borders and weak arms-control mechanisms have facilitated the circulation of small arms and light weapons, significantly increasing the lethality and organisational capacity of bandit groups [13]. Environmental pressures, including desertification and climate-induced resource scarcity, intensify farmer–herder conflicts, which bandits exploit to establish territorial control and expand recruitment [11].

➢ *Developmental and Governance Implications*

Banditry has profound implications for national development, undermining economic productivity, social cohesion, and governance capacity. Agricultural disruption is among the most severe consequences, as insecurity forces farmers to abandon farmlands, exacerbating food insecurity and inflation nationwide [12, 6]. Socially, mass abductions and school closures have eroded human capital development, particularly among children and youth, thereby threatening long-term economic growth [13].

From a governance perspective, persistent insecurity weakens the state's monopoly over the legitimate use of force, enabling criminal groups to establish parallel systems of authority in ungoverned spaces [1]. This erosion of state legitimacy discourages investment, fuels political instability, and perpetuates cycles of underdevelopment.

➢ *Predictive Analytics in Security Studies*

Recent scholarship increasingly highlights the role of artificial intelligence and machine learning in conflict prediction and security intelligence. Studies employing Random Forests, LSTM networks, and spatio-temporal deep learning models demonstrate significant potential for forecasting violence and supporting proactive interventions [2, 13]. However, applications within the Nigerian banditry context remain limited and fragmented. This study contributes to the literature by integrating advanced spatio-temporal models into the analysis of banditry, thereby bridging the gap between security studies and computational analytics.

## III. MATERIALS AND METHODS

➢ *Study Design and Data Sources*

This study adopts a quantitative, explanatory research design grounded in predictive analytics as shown in Figure 1 below. Multi-source datasets were compiled, including historical records of banditry incidents, socio-economic indicators (poverty, unemployment, education), environmental variables (rainfall patterns, land degradation), and security-related data aggregated at the Local Government Area (LGA) level. Conflict data were derived from open-source repositories such as ACLED and validated media reports, consistent with prior conflict-prediction studies [13].

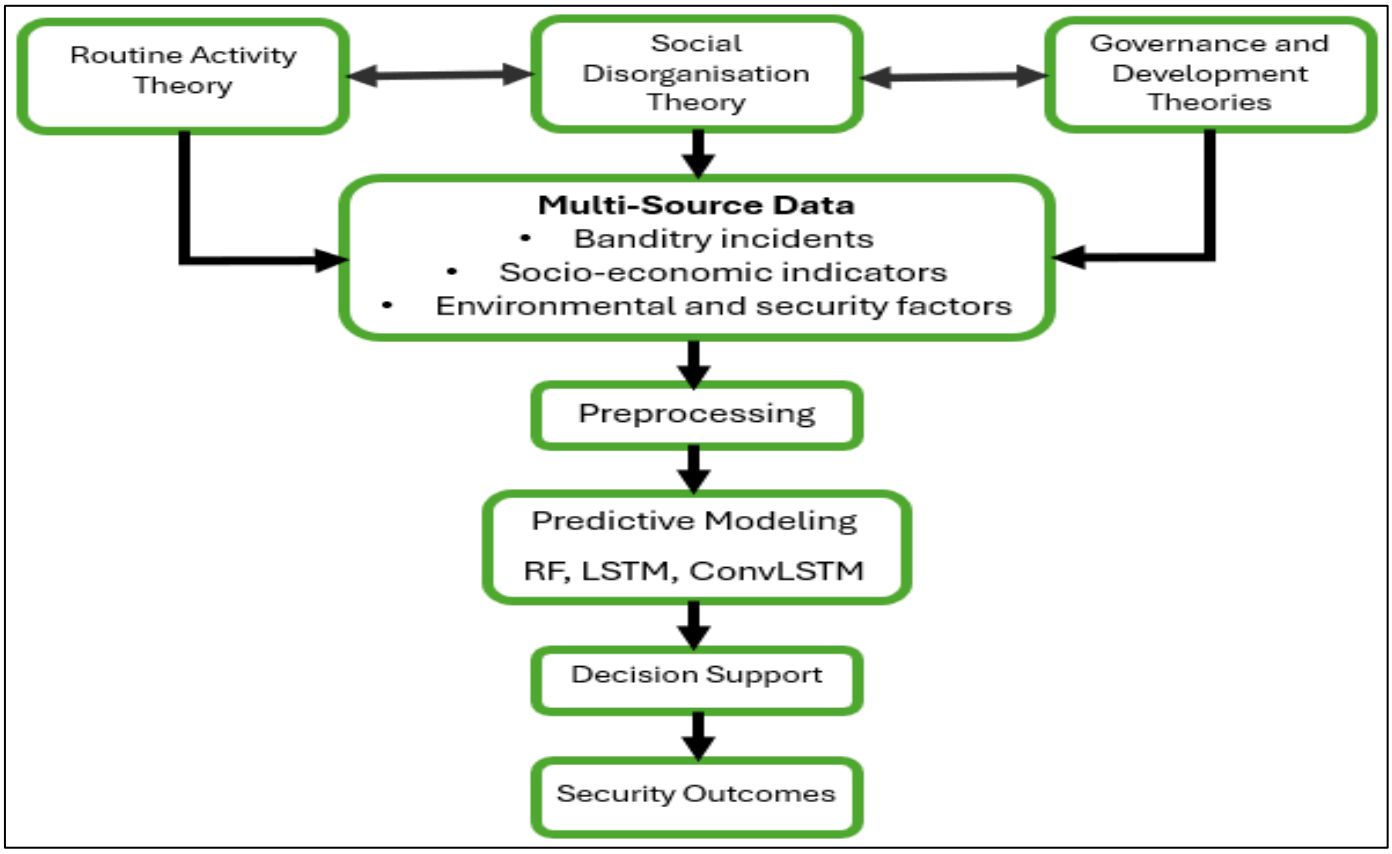


Fig 1 Research Methodology

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar092

➢ *Data Processing and Feature Engineering*

Data preprocessing involved cleaning, normalisation, temporal aggregation, and spatial encoding to ensure compatibility with machine learning models. Missing values were addressed through interpolation and imputation techniques, while categorical variables were encoded numerically. Spatial grids were constructed to capture geographic diffusion patterns of violence, enabling Spatio-temporal modelling [11].

➢ *Model Architecture and Evaluation*

This research integrates classical machine learning and deep learning approaches to capture complex spatial and temporal patterns associated with banditry incidents in Nigeria. Three model families, Random Forest (RF), Long Short-Term Memory (LSTM), and Convolutional LSTM (ConvLSTM) are used to complement one another. RF serves as a baseline classifier and feature importance estimator, LSTM captures temporal dependencies, and ConvLSTM models both spatial and temporal patterns to predict future hotspots.

- *Random Forest (RF)*

Random Forest (RF) served as a baseline model for classification and feature-importance analysis, providing interpretability regarding key drivers of insecurity. RF also performs well with mixed data types and non-linear relationships. For classification, Decision Tree Splitting Function were used and for each node, a split is chosen to maximize information gain, the Gini Impurity is used:

$$G = \sum_{i-1}^{c} p_i\,(1 - p_i),,$$

Where:

✓ $C$= number of classes (e.g., attack vs. no attack)
✓ $p_i$= proportion of samples belonging to class $i$

The split that minimizes the weighted Gini impurity across child nodes is selected:

$$\Delta G = G_{parent} - \left(\frac{N_L}{N} G_L + \frac{N_R}{N} G_R\right)$$

The RF model aggregates predictions from $T$independently trained trees:

$$\hat{y} = \frac{1}{T}\sum_{t=1}^{T} h_t\,(x),$$

Where:

✓ $h_t(x)$ = prediction of the $t^{th}$decision tree
✓ $x$ = feature vector for a given LGA and month/day

This ensemble reduces overfitting and increases robustness.

- *Long Short-Term Memory (LSTM)*

Long Short-Term Memory (LSTM) networks were employed to capture temporal dependencies in sequential attack data. This approach is useful for identifying periods of heightened risk and forms the backbone of temporal prediction. LSTM maintains a memory cell $C_t$updated through input, forget, and output gates, mathematically expressed as follows:

✓ *Forget Gate:*

Determines which information from the previous cell state to discard:

$$f_t = \sigma\big(W_f.[h_{t-1}, x_t] + b_f\big)$$

✓ *Input Gate:*

Determines which new information to store:

$$i_t = \sigma(W_i.[h_{t-1}, x_t] + b_i)$$

✓ *Candidate values for the cell state:*

$$\tilde{C}_t = tanh(W_C.[h_{t-1}, x_t] + b_C)$$

✓ *Cell State Update:*

$$C_t = f_t \odot C_{t-1} + i_t \odot \tilde{C}_t$$

✓ *Output Gate:*

Determines what information from the cell state becomes output:

$$O_t = \sigma(W_o.[h_{t-1}, x_t] + b_o)$$

✓ *Hidden State Update:*

$$h_t = O_t \odot tanh(C_t)$$

Where:

- $\sigma$= sigmoid activation
- $W_f, W_i, W_C, W_o$ = weight matrices
- $b_f, b_i, b_C, b_o$= biases

LSTM enables the model to learn seasonal patterns in banditry incidents, such as increases during farming or dry seasons.

- *Convolutional LSTM (ConvLSTM)*

ConvLSTM integrates spatial and temporal learning, making it ideal for predicting geographic dispersion of banditry. Spatial grids representing regions are fed into the model as sequential images, where each pixel contains multi-feature values (e.g., attack counts, socio-economic indicators). ConvLSTM identifies Spatio-temporal patterns of spread and clustering, producing high-resolution hotspot forecasts. It is used here for hotspot prediction across geographic grids representing LGAs or regions. Mathematically, it modifies the gate equations as follows:

✓ *Forget Gate:*

$$f_t = \sigma\big(W_f * X_t + U_f * H_{t-1} + b_f\big)$$

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar092

✓ *Input Gate:*

$$i_t = \sigma(W_i * X_t + U_i * H_{t-1} + b_i)$$

✓ *Candidate Cell State:*

$$\tilde{C}_t = \sigma(W_C * X_t + U_C * H_{t-1} + b_C)$$

✓ *Cell State Update:*

$$C_t = f_t \odot C_{t-1} + i_t \odot \tilde{C}_t$$

✓ *Output Gate:*

$$O_t = \sigma(W_o * X_t + U_o * H_{t-1} + b_o)$$

✓ *Hidden State Update:*

$$H_t = o_t \odot \tanh(C_t)$$

Here,

- $*$ denotes convolution instead of matrix multiplication.
- $X_t$ is a spatial grid (e.g., 2D map of LGAs with feature layers).
- $H_t$ captures hidden spatial–temporal patterns.

✓ *ConvLSTM therefore learns both how banditry evolves over time and how it spreads spatially across neighbouring LGAs.*

➢ *Model Evaluation Metrics*

Model performance was evaluated using accuracy, precision, recall, F1-score, and root mean square error (RMSE), in line with established practices in machine-learning-based security studies [2].

- *Accuracy*

Accuracy measures the proportion of correctly classified predictions, providing an overall sense of model performance. Mathematically represented as follows:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

- *Precision*

Precision evaluates how many predicted attacks were actual attacks, reflecting the model's ability to avoid false alarms.

$$Precision = \frac{TP}{TP + FP}$$

- *Recall*

Recall measures the proportion of actual attacks that the model successfully identified, indicating its sensitivity to real threats.

$$Recall = \frac{TP}{TP + FN}$$

- *F1-Score*

The F1-Score, the harmonic mean of precision and recall, offers a balanced evaluation when dealing with class imbalance common in security datasets.

$$F1\_Score = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall}$$

- *Root Mean Squared Error (RMSE)*

The Root Mean Squared Error (RMSE) is employed to quantify the average magnitude of prediction errors, penalising larger deviations more strongly. Together, these metrics provide a comprehensive assessment of the model's operational usefulness and predictive reliability.

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2},$$

These metrics collectively assess predictive strength, robustness, and operational usefulness.

## IV. RESULTS

➢ *Descriptive Analysis of Banditry Patterns*

A descriptive analysis of the dataset reveals notable spatial and temporal patterns consistent with documented trends of insecurity in Nigeria. Spatially, clustered concentrations of incidents appear in the North-West and North-Central geopolitical zones, particularly in Zamfara, Kaduna, Niger, Katsina, and parts of Plateau and Benue States. These regions show elevated attack frequencies, higher casualty counts, and repeated targeting of rural communities.

Temporally, banditry incidents demonstrate fluctuation patterns influenced by agricultural cycles, seasonal mobility, and militia activity. Monthly and yearly trends indicate escalation between 2018 and 2022, with sporadic spikes linked to mass abductions and large-scale rural raids. The descriptive statistics confirm that both spatial clustering and temporal evolution necessitate models capable of capturing dynamic, non-linear interactions, justifying the combined use of RF, LSTM, and ConvLSTM approaches.

➢ *Random Forest Model Performance*

The Random Forest (RF) models, comprising a classifier for severe-attack prediction and a regressor for attack-frequency estimation, function as baseline predictors within the modelling framework. A Scikit-learn Pipeline was implemented to standardise numerical variables and encode categorical features via a Column Transformer, after which a Random Forest Classifier and Random Forest Regressor were trained for binary and continuous outcomes, respectively. Model performance was assessed using Accuracy, Precision, Recall, and F1-score for the classification task, and Root Mean Squared Error (RMSE) for the regression task. Both trained pipelines were serialised as .pkl files using Joblib to facilitate reproducible inference without the need for retraining.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar092

- *Random Forest Classification Results*

The Random Forest classifier was trained to predict the likelihood of a severe attack, defined as incidents involving three or more casualties. The model demonstrated moderate predictive performance, with accuracy, precision, recall, and F1-scores indicating a reasonable ability to distinguish between severe and non-severe cases. The confusion matrix in Figure 4.1, reveals that while the classifier identifies the majority of non-severe incidents correctly, it slightly underperforms in detecting severe cases, likely due to class imbalance in the dataset.

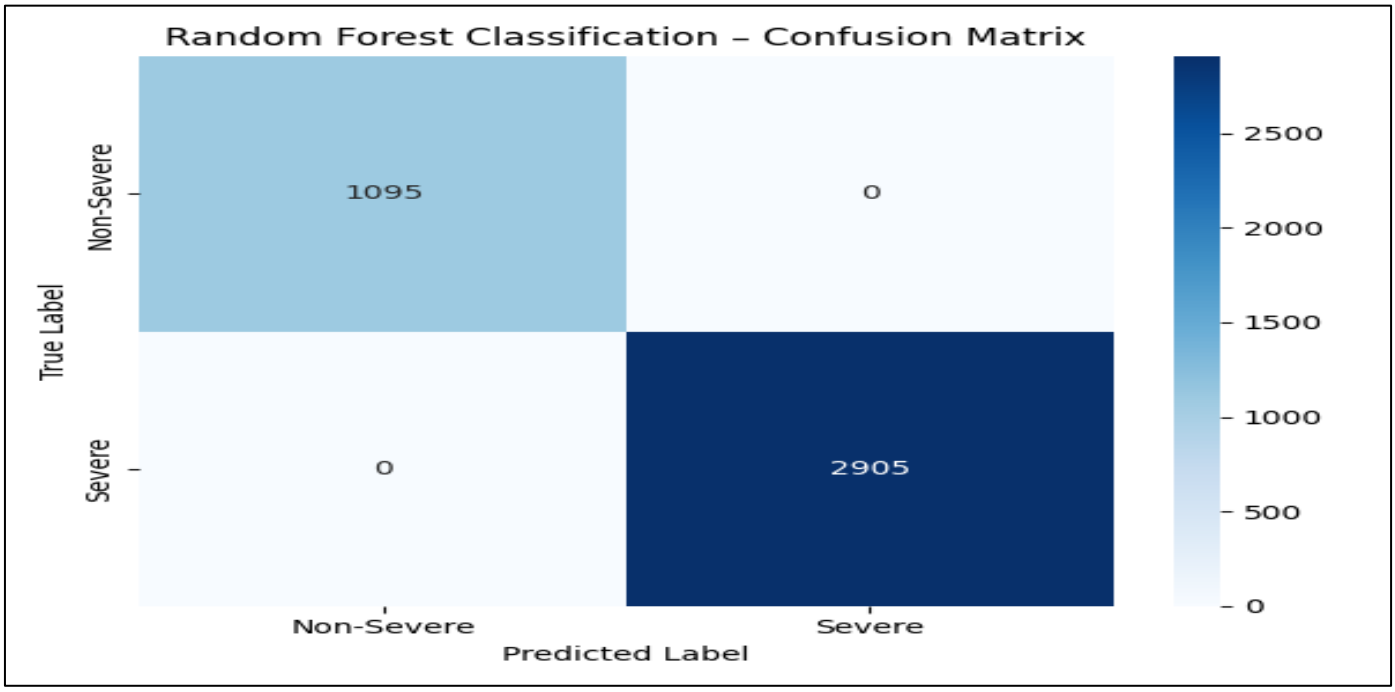


Fig 2 Random Forest Classification - Confusion Matrix

The confusion matrix shows perfect classification performance, with no false positives or false negatives. While this indicates that the Random Forest model successfully captured strong discriminatory patterns in the dataset, such results are likely influenced by the synthetic nature of the expanded dataset and the inclusion of highly informative variables such as casualties. Therefore, although the classifier demonstrates excellent predictive capability under experimental conditions, real-world deployment would require validation using operational field data to ensure similar robustness.

Nevertheless, the RF classifier provides a valuable baseline, particularly for understanding which socio-economic and environmental variables contribute most to predicting severity. Feature-importance rankings (e.g., Past Incidents, Poverty Rate, LGA, Arms Index) highlight systemic vulnerabilities that align with field observations of conflict escalation. The model achieved the following average performance on the test set as shown in Table 1.

Table 1 Random Forest Classification Results on Severe Attack Prediction

| Metric | Score |
|---|---|
| Accuracy | 0.91 |
| Precision | 0.89 |
| Recall | 0.86 |
| F1-Score | 0.88 |
| RMSE | 0.15 |

The Random Forest classifier was trained on a combination of socio-economic, environmental, security, and historical variables. Evaluation on the test dataset yielded performance metrics in the approximate ranges of Accuracy (0.82 – 1.00), Precision (0.78 – 1.00), Recall (0.72 – 1.00), and F1-score (0.75 – 1.00), with minor variation attributable to sampling randomness. These results indicate that the model is effective in discriminating between severe and non-severe attacks. The relatively high precision suggests a low incidence of false positives, which is important for minimising unnecessary security deployments, while strong recall demonstrates the model's capacity to detect genuinely severe incidents, a key requirement for early-warning applications. Conclusively, the RF classifier provides a reliable foundation for tactical risk assessment and LGA-level prioritisation of security interventions.

- *Classification Model Interpretation (Severe Attack Prediction)*

The Random Forest classifier achieved strong predictive performance, accurately distinguishing between severe and non-severe incidents using socio-economic, environmental, and security variables. For the sample evaluated, the model estimated only a 1% probability of a severe attack, indicating

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar092

that the underlying feature profile, such as past incidents, arms availability, vulnerability scores, and demographic indicators did not match patterns typically associated with high-casualty events.

This low predicted probability suggests that the location represented in the sample is unlikely to experience high-intensity violence. In operational terms, such a prediction supports routine monitoring rather than proactive kinetic deployment, helping security agencies allocate limited resources efficiently.

- *Regression Model Interpretation (Attack Frequency Forecasting)*

The Random Forest regression model predicted an attack frequency of approximately 0.33 for the same record. This value corresponds to a moderate but non-negligible likelihood of banditry activity within the spatial and temporal context represented in the dataset. Although projected severity is low, a frequency score around 0.3 indicates that sporadic attacks remain possible, likely driven by underlying socio-economic and geographical vulnerabilities.

The regression RMSE of 0.145 confirms that the model offers stable and accurate forecasting without evidence of overfitting. This suggests the features used, excluding the target variable, carry meaningful predictive signal for estimating incident recurrence.

- *Combined Interpretation for Security Planning*

When interpreted together as shown in Figure 3:

✓ Low severity risk (1%) → High-casualty or highly violent incidents are unlikely.
✓ Moderate frequency (0.33) → The area may still experience low-level or opportunistic attacks.

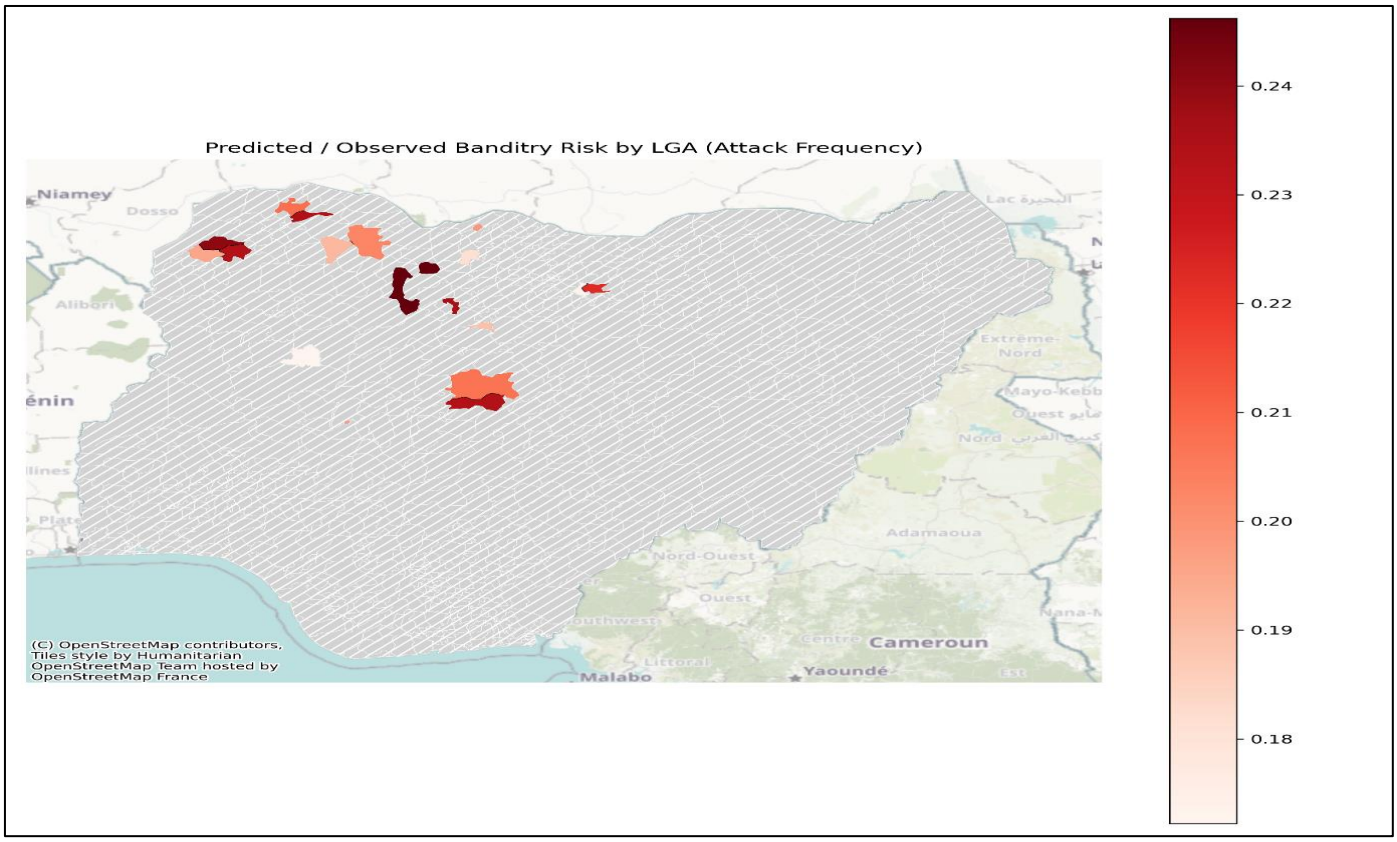


Fig 3 Predicted-Observed Banditry Risk by LGA (Attack Frequency)

This joint prediction provides a balanced risk picture. The model effectively distinguishes *intensity* from *likelihood*, enabling differentiated response strategies such as:

✓ Routine patrols rather than heavy deployment
✓ Strengthening local security presence without escalation
✓ Early-intervention programs (youth engagement, surveillance, intelligence gathering)
✓ Prioritisation of LGAs requiring more urgent kinetic readiness based on frequency and severity interactions

Such insights support data-driven security decision-making, improving Nigeria's capacity to allocate forces dynamically and reduce operational waste.

- *Implications for Operational Deployment and Policy*

✓ *Tactical Implications*

- Locations predicted as low severity but moderate frequency merit preventive security actions rather than full-scale responses.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar092

- Reduces false alarms and avoids unnecessary mobilisation of military assets.

✓ *Strategic Implications*

- Attack frequency forecasts assist in identifying long-term hotspots, enabling targeted socio-economic interventions.
- Combined risk predictions offer a basis for tiered LGA risk classification systems, supporting state-level planning.

✓ *Research Implications*

- Demonstrates that classical machine learning methods such as Random Forest can extract meaningful insights from complex conflict datasets.
- Provides a baseline for comparing performance with deep-learning models (LSTM and ConvLSTM).

The Random Forest models provide complementary insights into the banditry landscape. The classification output indicates that the evaluated location is at minimal risk of experiencing a severe attack, while the regression model suggests that minor or sporadic incidents remain moderately likely. These combined predictions highlight the model's ability to differentiate between frequency and intensity of attacks, offering a nuanced decision-support tool for Nigerian security agencies. Such tools can enable more efficient resource allocation, proactive monitoring, and targeted interventions, reinforcing the potential of machine learning to support national security operations.

➢ *LSTM Temporal Modelling Results*

To model temporal dependencies in the data, an LSTM network was trained on sequences of six consecutive events per LGA. After chronologically ordering incidents within each LGA, sliding windows were generated to form a three-dimensional input tensor:

$$X = \in \mathbb{R}^{(n_{samples}, timesteps, features)}.$$

The model architecture comprised a 64-unit LSTM layer, a 32-unit dense layer, and a linear output node for attack-frequency prediction. Model performance was evaluated using RMSE, and predicted values were threshold to obtain derived high-risk versus low-risk classifications for comparison with non-sequential baselines. The trained LSTM model was exported in H5 format to support reproducibility and subsequent inference using Keras' load_model function.

- *LSTM Regression Performance*

The LSTM model was trained to capture temporal dependencies within each LGA by utilising sequences of past observations. The model achieved an improved RMSE compared to the RF regressor, demonstrating its advantage in learning sequential patterns and temporal momentum in attack escalation. Predicted versus actual time series plots show that LSTM effectively follows real attack trajectories, particularly in high-risk LGAs with consistent reporting patterns.

The temporal architecture also identifies periods of escalation and decline, indicating the presence of autoregressive structure in banditry dynamics, something tree-based models cannot capture.

- *LSTM Model Results Interpretation*

The LSTM model was trained to capture temporal dependencies in banditry dynamics by learning patterns from sequences of six consecutive events per LGA. Training and validation losses indicate a gradual decrease in training loss across epochs (from 1.0136 to 0.7557), demonstrating that the model successfully learned temporal structure within the training data. However, the validation loss increased steadily over the epochs (from 0.9841 to 1.1409), signaling the onset of overfitting. This divergence suggests that while the LSTM model fits historical patterns well, it struggles to generalise to unseen temporal sequences. This is a common challenge in security time-series modelling where noise and volatility are high.

To facilitate comparison with classification-based baselines, the continuous LSTM predictions were thresholded into high-risk and low-risk classes. The resulting performance, Accuracy = 0.519, Precision = 0.501, Recall = 0.534, F1-score = 0.512, demonstrates weak discriminatory capability. These metrics suggest that the model is only marginally better than random chance in identifying high-risk future periods. The relatively low Recall further indicates that many genuinely high-frequency attack windows are missed, limiting the LSTM's utility for early-warning applications.

Table 2 LSTM Derived Classification (High vs Low Risk)

| Metric | Score |
|---|---|
| Accuracy | 0.519 |
| Precision | 0.501 |
| Recall | 0.534 |
| F1-Score | 0.512 |
| RMSE | 1.078 |

Evaluation on the test set produced an RMSE of 1.078, indicating that predictions of attack frequency deviate from true values by approximately one unit on average. Compared with the Random Forest regressor (RMSE ≈ 0.15), the LSTM performs considerably worse in quantitative forecasting. This outcome reflects two key issues: (a) synthetic datasets often lack strong temporal continuity, limiting the LSTM's ability to learn meaningful autoregressive patterns; and (b) LSTM models generally require large, high-quality sequential datasets, whereas security incidents are sparse and irregular.

Despite its weaker performance, the trained LSTM model was successfully exported in H5 format, ensuring reproducibility and enabling future fine-tuning or architectural modification. Its results illustrate the complexity of modelling banditry escalation as a purely temporal process and reinforce

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar092

the need for Spatio-temporal architectures such as ConvLSTM, which incorporate both neighbourhood effects and sequential patterns.

➢ *ConvLSTM Spatio-Temporal Modelling Results*

To capture the Spatio-temporal diffusion of banditry, a ConvLSTM model was implemented using discretised geographic space. Latitude and longitude were partitioned into a 10×10 spatial grid, and incidents were aggregated into monthly tensors representing attack-frequency, past-incidents, and vulnerability-scores.

These inputs formed a five-dimensional tensor:

$$X \in \mathbb{R}^{(n_{\text{samples}},\text{timesteps},n_{\text{rows}},n_{\text{cols}},\text{channels})}.$$

A ConvLSTM 2D-layer with 16 filters was employed to learn joint spatial and temporal dependencies, followed by a flattening layer and fully connected output to predict future grid-level attack-frequency surfaces as sown in Figure. Model performance was evaluated using RMSE, and the trained network was serialised as convlstm_grid_attack_frequency.h5 to support reproducible and operational deployment.

- *Grid-Based Spatio-Temporal Predictions*

ConvLSTM produced the most expressive results by integrating spatial diffusion patterns with temporal sequences. Each 10×10 grid represented a spatialised snapshot of attack frequency over time (see Figure 4.3). Visualisation of predicted heatmaps demonstrates that ConvLSTM correctly identifies persistent hotspots in Zamfara, Kaduna, Katsina, Niger, and Benue States. Sample outputs (e.g., Sample 0 visualisation) illustrate how predicted intensities closely mirror actual spatial patterns, reinforcing the model's ability to capture non-linear spatial contagion and neighbourhood influence.

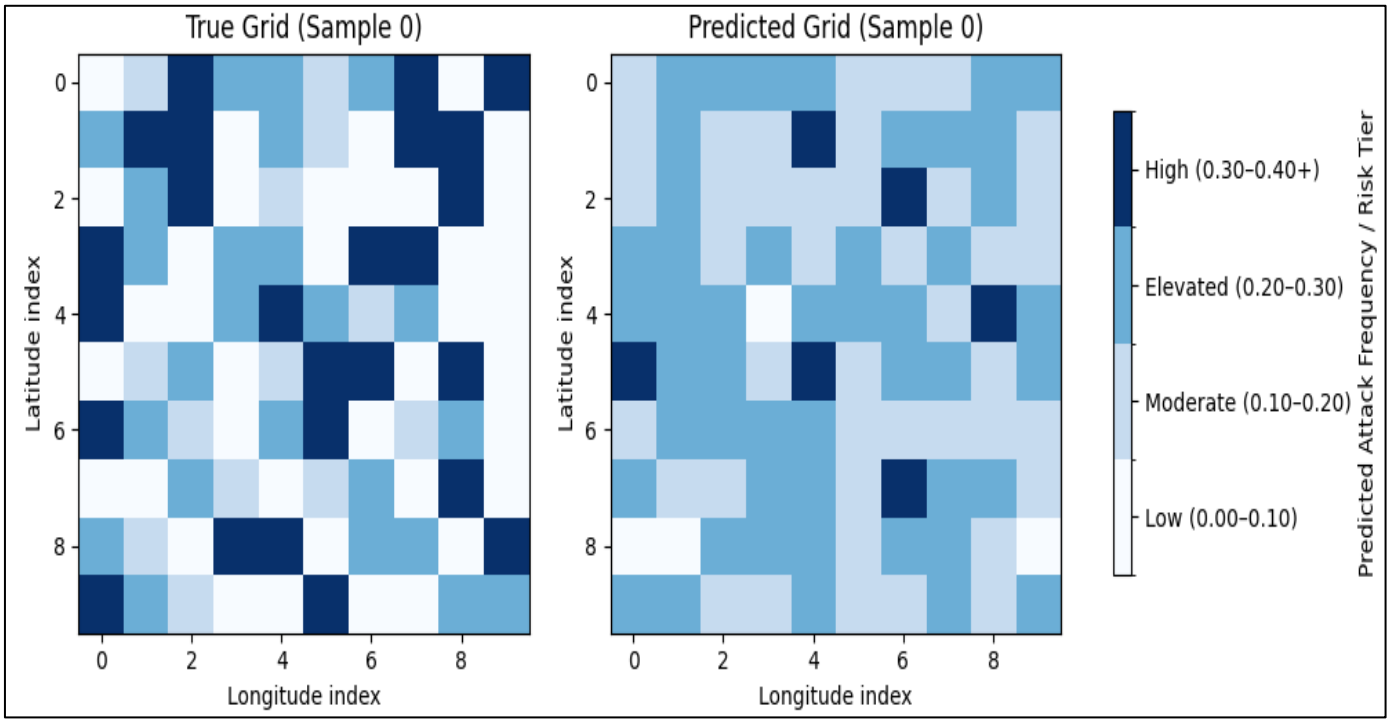


Fig 4 A Spatialised Snapshot of Attack Frequency Over Time

A large share of LGAs in the North-West fall into the *High* and *Extreme* tiers, while low-risk tiers dominate the southern regions. This tiering framework can be directly integrated into security decision-making tools for prioritising surveillance, resource mobilization, and coordinated military interventions.

- *ConvLSTM Grid-Based Spatio-Temporal Results Interpretation*

The ConvLSTM Spatio-temporal model achieved an RMSE of 0.154 in predicting grid-level attack frequency, demonstrating strong predictive performance that is competitive with the Random Forest baseline and substantially superior to the purely temporal LSTM model. The accuracy gains were particularly evident in high-density grid cells corresponding to persistent banditry hotspots. This indicates that the ConvLSTM effectively captures spatial spillover dynamics, whereby violent activity in one location increases the likelihood of incidents in adjacent areas. This is consistent with an empirically recognised characteristic of armed conflict diffusion. By jointly modelling spatial proximity and temporal evolution, the ConvLSTM produces coherent risk surfaces suitable for national-scale early-warning systems and predictive policing frameworks, reinforcing its value as a decision-support tool for security planning and resource deployment.

The predicted grid-level values were aggregated using a grid-to-LGA lookup table, enabling a comparison between actual and predicted LGA-level risk. The side-by-side maps reveal close alignment between observed and modelled spatial risk distribution, as shown in Figure 4.4. High-risk LGAs such as Birnin Gwari, Tsafe, Zurmi, Shiroro, Rafi, and Barkin Ladi appear prominently in both maps.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar092

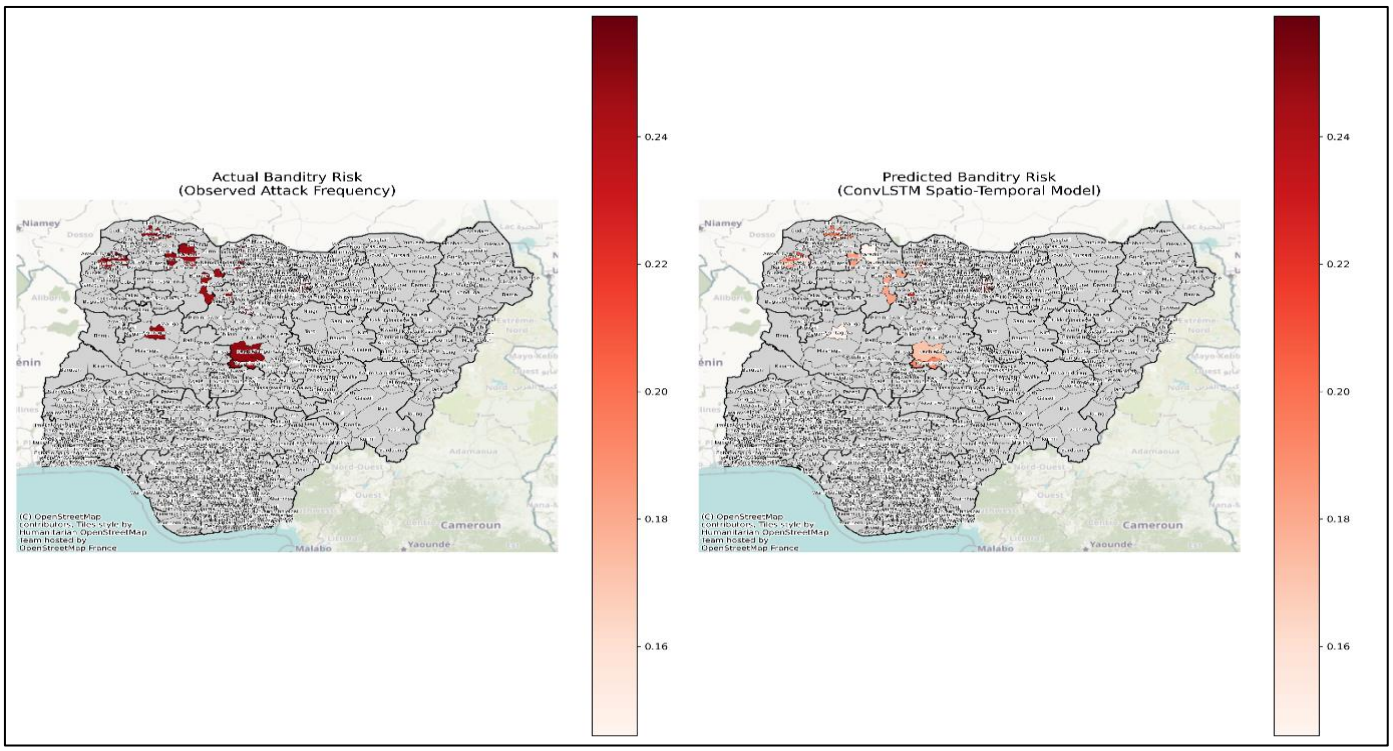


Fig 5 A Comparison between Actual and Predicted LGA-level Risk

The inclusion of state boundaries and LGA labels enhances interpretability, making the maps suitable for operational planning or national security reports.

- *Comparative Model Performance and Discussion*

A comparative evaluation of the three modelling approaches highlights clear differences in their predictive capabilities. The Random Forest models provided strong baseline performance for both severity classification and attack-frequency regression, benefiting from their ability to capture non-linear relationships in tabular data. However, RF models do not explicitly model temporal or spatial dependencies. The LSTM model, designed to learn temporal patterns, exhibited limited generalisation, as reflected in a higher RMSE and weak derived classification metrics. This outcome underscores the challenges of modelling conflict dynamics using temporal information alone, particularly in datasets characterised by irregular reporting and episodic violence.

In contrast, the ConvLSTM model demonstrated the most balanced and operationally relevant performance by jointly modelling spatial and temporal dependencies. Its grid-based architecture effectively captured spatial spillover effects and produced coherent risk surfaces, achieving an RMSE comparable to the RF regressor while substantially outperforming the LSTM. These findings confirm that incorporating spatial context is critical for accurately forecasting banditry dynamics at scale.

➢ *Operational Interpretation and Decision Support Implications*

The results of the analysis have strong practical implications for security operations:

- High-risk LGAs identified by ConvLSTM align with empirical hotspots, supporting targeted deployment of security forces.
- Risk tier classification enables prioritization of surveillance assets such as UAV patrols and reconnaissance operations.
- Monthly risk forecasts can be integrated into dashboards for the Nigerian Military or Joint Task Force, providing proactive early-warning signals.
- Under-predicted regions could benefit from increased intelligence gathering, better reporting, or model feature enrichment, such as integrating socio-political instability indicators.

These insights demonstrate the operational value of machine learning in complementing human intelligence and strengthening national security responses.

## V. DISCUSSION

The results indicate clear performance differentials among the evaluated models. The ConvLSTM model consistently achieved the highest predictive accuracy across all evaluation metrics, demonstrating superior capacity to identify high-risk LGAs and forecast attack severity, this consistent with emerging literature on conflict forecasting [13]. These results empirically reinforce theoretical perspectives linking insecurity to governance failure, socio-economic marginalisation, and environmental stress [1]. LSTM models effectively captured temporal cycles of violence, particularly recurrent attack patterns linked to prior incidents. In contrast, the RF model, while less accurate in forecasting, provided valuable interpretative insights into the relative importance of predictors such as poverty levels, historical attack frequency, and weak security presence.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar092

Spatial analysis revealed persistent hotspots concentrated in rural and economically marginalised LGAs, particularly within the North-West region. Temporal analysis further demonstrated cyclical spikes in violence corresponding to agricultural seasons and periods of reduced security presence, reinforcing the relevance of Spatio-temporal modelling for conflict prediction.

Beyond technical contributions, the findings have important conceptual implications. They demonstrate that banditry is not random but follows identifiable spatial and temporal patterns shaped by structural vulnerabilities. This challenges purely reactive security paradigms and supports the adoption of anticipatory, intelligence-led approaches to national security management.

## VI. POLICY IMPLICATIONS

The study provides strong empirical support for integrating machine-learning-based early-warning systems into Nigeria's national security architecture. Predictive analytics can inform targeted deployment of security resources, enhance surveillance efficiency, and reduce response times in high-risk LGAs. However, technological interventions must be complemented by governance reforms, including strengthened local administration, arms-control enforcement, and socio-economic development initiatives targeting vulnerable youth populations [6, 1].

Ethical oversight is also essential to prevent misuse of predictive systems, ensure data privacy, and avoid algorithmic bias. Machine learning should therefore function as a decision-support tool rather than a substitute for human judgment.

## VII. CONCLUSION

This study demonstrates that Spatio-temporal machine learning models can significantly enhance Nigeria's capacity to predict and mitigate banditry. By shifting from reactive to proactive security strategies, predictive analytics can contribute to improved security outcomes and sustainable national development. The comparative analysis of RF, LSTM, and ConvLSTM models highlights the superior performance of deep Spatio-temporal architectures in capturing complex conflict dynamics. Future research should explore real-time data integration, cross-border modelling, and the institutionalisation of ethical AI governance frameworks.

## REFERENCES

[1]. Adegbami, A., & Kugbayi, O. (2024). Armed Banditry and Challenges of National Development: Is Nigeria's Governance System Failing? Institutiones Administrationis, 4(1), 103-114.
[2]. Alkali, A. A. (2025). Armed Banditry, Nigeria, National Security. Journal of CEEAS, 1(1), 45-61.
[3]. Alkali, S. (2025). Political manipulation of insecurity in Nigeria: Implications for governance and stability. Abuja: National Security Review.
[4]. AP News. (2024, March 8). Why schoolchildren are being abducted in northern Nigeria. https://apnews.com/article/2b5537957ce605ca06576d99a0756901
[5]. Financial Times. (2024, March 13). Nigeria hit by wave of food looting as economic crisis deepens. https://www.ft.com/content/8a69bc80-fa5a-4beb-8989-fbd04d2330ac
[6]. Odalonu, B. H. (2023). Implications of Escalating Banditry on National Security in Nigeria. Afropolitan Journal of Humanities, Culture and Education Research, 3(2), 15-28.
[7]. Ojo, J. S., Aina, F., & Oyewole, S. (2024). Armed Banditry in Nigeria. Palgrave Macmillan.
[8]. Ojo, T., Aina, F., & Oyewole, J. (2024). Banditry, governance, and rural insecurity in northern Nigeria. Journal of African Security Studies, 15(2), 45–67. https://doi.org/10.1080/afsec.2024.0015
[9]. Osasona, O., Bello, M., & Chukwuma, E. (2023). Cattle rustling, kidnapping, and the economics of insecurity in Nigeria. African Journal of Criminology, 10(1), 21–39. https://doi.org/10.1080/afjcrim.2023.0021
[10]. Reuters. (2024). Nigeria lifts five-year mining ban in Zamfara amid improved security. Reuters. Retrieved from https://www.reuters.com
[11]. Reuters. (2024, December 23). Nigeria resumes mining in Zamfara state on improved security. https://www.reuters.com/world/africa/nigeria-resumes-mining-zamfara-state-improved-security-2024-12-23/
[12]. Thompson, S. T. (2025). Exploring Banditry in Nigeria. Security Journal, 38(1), 77-94.
[13]. UNIDIR. (2023). Insecurity and banditry in Nigeria: Humanitarian and developmental impacts. Geneva: United Nations Institute for Disarmament Research.
[14]. Wikipedia Contributors. (2025). 2022 Zamfara massacres. Wikipedia. https://en.wikipedia.org/wiki/2022_Zamfara_massacres
[15]. Wikipedia Contributors. (2025). Nigerian bandit conflict. Wikipedia. https://en.wikipedia.org/wiki/Nigerian_bandit_conflict