

Artificial Intelligence Applications for Enhancing Security and Threat Detection in Northeast Nigeria

IBRAHIM MUSA IBRAHIM¹, AHMAD ABDULKAREEM², MOHAMMED WAKILBE³

^{1,2,3}*Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Maiduguri, Maiduguri, Borno State, Nigeria. Graduate Members, Nigeria Society of Engineers (NSE).*

Abstract- — *The security landscape of Northeast Nigeria has, for over a decade and a half, been shaped by the protracted Boko Haram and Islamic State West Africa Province (ISWAP) insurgency, whose mass-casualty attacks, large-scale abductions and cross-border operations across the Lake Chad basin have produced one of the world's largest internally displaced populations. Conventional security architectures, reliant on manual intelligence gathering, static checkpoints and after-the-fact investigation, have struggled to keep pace with the speed, mobility and adaptive tactics of these threat actors. This paper presents a comprehensive review and conceptual framework for the application of Artificial Intelligence (AI) — spanning machine learning, deep learning, natural language processing, computer vision, and predictive geospatial analytics — to security and threat detection in Northeast Nigeria. The paper synthesizes evidence from the global and Nigeria-specific literature on AI-enabled surveillance, biometric identification, unmanned aerial vehicle (UAV) reconnaissance, social-media-based extremism monitoring, financial-crime detection, and predictive crime mapping, and proposes a layered architecture that integrates these techniques into a coherent threat-detection pipeline suited to a low-connectivity, resource-constrained operating environment. The discussion further examines the practical, infrastructural, and ethical constraints that condition AI adoption in the region — including unreliable electricity supply, data scarcity, algorithmic bias, and privacy risk — and closes with policy-oriented recommendations for security agencies, technology developers, and government institutions. The paper argues that AI should be understood not as a stand-alone solution but as a force multiplier that augments human intelligence and community policing, provided that deployment is grounded in transparency, local data governance, and human rights safeguards.*

Index Terms — *Artificial intelligence, Boko Haram, insurgency, machine learning, national security, Northeast Nigeria, predictive policing, threat detection.*

I. INTRODUCTION

Security has, for much of the last two decades, remained one of the most persistent and consequential development challenges confronting Nigeria, and nowhere is this more visible than in its North-East geopolitical zone. Since 2009, the region has endured a protracted insurgency waged by Boko Haram and its splinter faction ISWAP, resulting in mass displacement, the destruction of public infrastructure, and tens of thousands of fatalities across Borno, Yobe and Adamawa States [10], [11]. The conflict has repeatedly spilled across the Lake Chad basin into Cameroon, Chad and Niger, complicating both the military response and the underlying intelligence picture, while successive waves of displacement have left millions of people in camps and host communities in need of continuous monitoring and protection [12], [20].

These threats share several structural features that conventional, largely manual security methods are ill-equipped to address: they are geographically dispersed across vast and often inaccessible terrain; they are highly mobile and adaptive, with armed groups shifting operating bases in response to military pressure; and they generate large volumes of open-source, communications, financial and geospatial data that vastly exceed the analytical capacity of human intelligence teams operating with limited manpower and equipment [9], [17]. Nigeria's security agencies have historically relied on informant networks, static checkpoints, after-the-fact forensic investigation and periodic military operations — approaches that are reactive by design and that struggle to anticipate attacks before they occur [6], [19].

Artificial Intelligence has, over the past decade, matured from a largely experimental technology into

an operationally deployed capability across policing, defense and border-management functions worldwide, encompassing machine learning-based anomaly detection, deep learning-driven computer vision, natural language processing for open-source intelligence, and predictive geospatial analytics for crime and conflict forecasting [1], [112], [113]. A growing body of Nigeria-focused scholarship has begun to examine how these capabilities might be adapted to the country's specific threat environment, from AI-assisted intelligence coordination among security agencies [9] to machine-learning classification of terrorist attack patterns using historical incident data [13], [14], and from AI-enhanced fraud detection in the banking sector [70], [72] to proposals for AI-integrated CCTV and drone surveillance at the sub-national level [6].

This paper contributes to that emerging literature by presenting a structured, Northeast-Nigeria-focused synthesis of AI applications for security and threat detection. Its objectives are threefold: first, to review the principal families of AI technique relevant to threat detection and to map them against the specific security challenges of the North-East zone — insurgency, mass displacement, and cross-border movement across the Lake Chad basin; second, to propose a conceptual, layered architecture through which these techniques can be integrated into a coherent threat-detection pipeline suited to the region's infrastructural realities; and third, to critically examine the practical, ethical and governance constraints — data scarcity, unreliable electricity, algorithmic bias, and privacy risk — that must be addressed for such systems to be deployed responsibly. The remainder of the paper is organized as follows. Section II reviews related work. Section III characterizes the security landscape of Northeast Nigeria in greater depth. Section IV surveys the core AI techniques applicable to threat detection. Section V presents the proposed conceptual framework. Section VI discusses specific application domains. Section VII offers an illustrative comparative analysis of technique characteristics. Section VIII examines challenges and limitations. Section IX presents recommendations, and Section X concludes the paper.

II. RELATED WORK

A substantial and rapidly growing literature addresses the intersection of artificial intelligence and national security in the Nigerian context, with clear relevance to the North-East's counter-insurgency setting. Zakari and Musa [3] examined the implications of AI for Nigeria's security agencies through a documentary research design, concluding that AI-powered surveillance capabilities such as facial recognition and video analytics carry significant prospects for identifying and monitoring insurgent and terrorist threats, while also cautioning that adoption remains constrained by weak institutional capacity. Suleiman [9] investigated the application of AI to intelligence gathering and national-security management, framing insurgency and terrorism, alongside other interlocking national threats, as challenges that the existing security architecture is not structurally equipped to detect, deter or neutralize at scale. Mohammed [6], drawing on stakeholder survey data from a neighboring northern state, found that AI integration with closed-circuit television systems can materially improve the monitoring of suspicious activity, support search-and-rescue operations, and reduce response time — findings with direct bearing on Northeast Nigeria's own urban and checkpoint security needs — while recommending sustained government investment in AI infrastructure and capacity building.

A second cluster of studies applies machine learning directly to historical incident data to model and forecast attack patterns. Adeyemi [13] used classification algorithms trained on daily terrorism-incident records to predict the likelihood, targets and weapon types associated with future attacks in Nigeria. Braimah [16] combined descriptive statistics with ARIMA and SARIMA time-series models to forecast Boko Haram activity using more than a decade of geolocated incident data, identifying the North-East as the most volatile zone and demonstrating that control-chart methods can flag periods of heightened insurgent activity before they peak. Nwokorie [19] applied a dynamic k-reference clustering algorithm to Boko Haram attack data and recommended the deployment of intelligent, automated border-monitoring systems — including gunshot-detection sensors, video analytics and robotic

detection platforms — at frontline positions. Kolawole [20] conducted a geospatial risk analysis of school attacks by Boko Haram spanning nearly fourteen years of open-source data, building machine-learning risk scores that account for urbanization, proximity to prior attack sites, and other spatial covariates.

A related body of work addresses AI applications in adjacent security-relevant domains that this paper treats as integral to a holistic threat-detection architecture. In the financial domain, several Nigeria-focused studies document the growing adoption of machine learning and deep learning for fraud and anomaly detection in the banking and mobile-money sectors [70], [71], [74], [76], with the Central Bank of Nigeria formally committing to AI- and machine-learning-based fraud surveillance as part of its Payments System Vision 2028 reform agenda [72]. In the domain of open-source and social-media intelligence, natural language processing techniques — including transformer-based models such as BERT — have been shown to substantially improve the automated detection of hate speech, extremist rhetoric and radicalization signals in online text, even in low-resource and multilingual settings [49], [50], [56], [57]. In the domain of aerial surveillance, the international literature on UAV-based border and perimeter monitoring documents mature use cases in threat detection, obstacle avoidance and real-time video analytics that are directly transferable to Nigeria's porous land borders [60], [61], [66].

Finally, a growing critical literature cautions against uncritical AI adoption in security contexts, documenting demonstrated biases in facial recognition accuracy across demographic groups [41], [45], the risk of function creep from narrowly scoped surveillance deployments toward broader population monitoring [44], and the infrastructural constraints — chiefly unreliable electricity and constrained connectivity — that condition the feasibility of AI deployment across Sub-Saharan Africa more broadly [88], [91], [93]. This paper situates itself at the intersection of these three literatures: it draws on the Nigeria-specific security-AI scholarship to ground its problem framing, on the global technical literature to inform its account of applicable AI techniques, and on the critical infrastructure-and-ethics literature to

temper its recommendations with an appropriately cautious, context-sensitive outlook.

III. THE SECURITY LANDSCAPE OF NORTHEAST NIGERIA

An accurate assessment of where AI can add value requires a clear-eyed characterization of the security threat itself, since the North-East's counter-insurgency environment presents operational demands that differ materially from conventional crime and require a correspondingly tailored analytical response.

A. Insurgency and Asymmetric Warfare

The Boko Haram insurgency, and its ISWAP offshoot, has for over fifteen years combined guerrilla ambushes, improvised explosive devices, mass-casualty attacks on civilian and military targets, and periodic large-scale abductions, most infamously the 2014 Chibok schoolgirls' kidnapping [10]. The conflict has produced one of the world's largest internally displaced populations and has repeatedly targeted schools, further degrading human-capital development in the affected states [20]. The insurgents' operating pattern — dispersed forest and riverine hideouts, cross-border movement into the Lake Chad basin, and opportunistic targeting informed by observed troop movements — creates a genuine intelligence problem: threats are numerous, geographically diffuse, and only weakly correlated with any single observable signal, which is precisely the type of pattern-recognition problem for which machine learning and geospatial analytics are well suited [16], [19].

B. Humanitarian Displacement and the IDP Crisis

The insurgency has produced one of Africa's largest internal-displacement crises, with millions of people across Borno, Yobe and Adamawa States having passed through formal camps, informal settlements and host communities since 2009 [11], [12]. Recurrent attacks on camps and resettlement sites, coupled with the gradual, security-contingent return of displaced populations to newly recovered local government areas, create a fluid and continuously shifting population-security picture that conventional, static security methods struggle to track in real time. This dynamic is compounded by the destruction of schools,

health facilities and other public infrastructure, which both degrades human-capital development in affected communities and complicates the safe return and reintegration process [20].

C. Cross-Border Dynamics in the Lake Chad Basin

Boko Haram and ISWAP operate across a porous, multinational frontier spanning north-eastern Nigeria, northern Cameroon, western Chad and south-eastern Niger, using the creeks, islands and forested terrain of the Lake Chad basin as a sanctuary from which to regroup, resupply and stage cross-border attacks. This transnational operating pattern means that insurgent movements, weapons flows and abducted persons routinely cross international boundaries that regional forces — including the Multinational Joint Task Force — are only partially able to monitor. The result is a threat environment that is spatially clustered around identifiable riverine and forest corridors, and that generates recurring, quasi-predictable episodes of cross-border movement that lend themselves to geospatial and temporal pattern analysis in the same manner as insurgency hotspots elsewhere [82], [83].

D. Structural Constraints on Response

Across the North-East, several structural constraints recur: weak border management along the Lake Chad basin frontier that allows the cross-border movement of weapons, personnel and abducted persons; an intelligence architecture that remains heavily dependent on human informants and after-the-fact reporting rather than continuous monitoring [9]; and severe resource asymmetries between security forces and the areas they are tasked with covering, given the sheer geographic scale of forest, riverine and semi-arid terrain relative to available personnel and surveillance assets [17]. It is against this backdrop — geographically dispersed, data-rich but analytically under-resourced, and characterized by threats that leave detectable behavioral and communications traces — that the case for AI-assisted threat detection is best understood, not as a silver-bullet replacement for security personnel, but as a means of extending the analytical reach of a limited force.

IV. AI TECHNIQUES FOR SECURITY THREAT DETECTION

AI techniques relevant to security and threat detection can usefully be grouped into five overlapping families, each suited to different categories of data and threat signature. Figure 2 summarizes this taxonomy.

A. Machine Learning

Classical machine learning algorithms — including support vector machines [114], random forests [115], gradient-boosted trees, and unsupervised clustering methods — remain the workhorse of structured-data security analytics. Supervised classifiers trained on historical incident records can learn to associate attack characteristics (location, time, weapon type, group signature) with future risk, as demonstrated in Nigeria-focused studies that used classification algorithms to model terrorist-attack likelihood from historical data [13], [14]. Unsupervised anomaly-detection methods, by contrast, require no labeled attack examples and instead flag deviations from established behavioral baselines, a property that is particularly valuable for financial-fraud detection, where the earliest signals of a new fraud typology are, by definition, not present in any training set [70], [76].

B. Deep Learning

Deep neural networks — convolutional neural networks (CNNs) for image and video data, and recurrent architectures such as long short-term memory (LSTM) networks for sequential data [116] — substantially outperform classical methods on high-dimensional, unstructured inputs. The 2012 demonstration that deep CNNs could dramatically improve image-classification accuracy [117] catalyzed the subsequent adoption of deep learning across computer vision, and the same architectures now underpin facial recognition, object and weapon detection in CCTV and drone footage, and automated damage assessment from satellite imagery [95], [99]. Deep learning-based intrusion-detection systems have likewise become a mature sub-field within network security, with recent systematic reviews cataloguing the trade-offs between detection accuracy, computational overhead and explainability across dozens of proposed architectures [32], [33], [36].

C. Natural Language Processing

Natural language processing (NLP), and in particular transformer-based language models such as BERT [118] built on the attention mechanism [119], enables the automated analysis of text at a scale far beyond manual review — a capability directly applicable to monitoring social media, messaging platforms and other open-source channels for indicators of radicalization, incitement or coordinated planning. Recent NLP research demonstrates that fine-tuned transformer models can achieve strong performance in detecting hate speech and extremist rhetoric even in low-resource and multilingual settings [49], [50], [56], which is directly relevant to Northeast Nigeria's linguistically diverse population spanning Hausa, Kanuri, Shuwa Arabic and English-language online discourse. Complementary work has applied NLP specifically to tracking the temporal evolution of extremist discourse on social media platforms, offering a template for longitudinal radicalization monitoring [57].

D. Computer Vision

Computer vision techniques extend beyond simple image classification to encompass facial recognition, license-plate recognition, and object or weapon detection in real time video streams. While these capabilities offer clear operational value for perimeter security, checkpoint screening and crowd monitoring, the international literature is equally clear that facial recognition systems exhibit measurably higher error rates for darker-skinned individuals and other demographic subgroups, a bias with direct implications for wrongful identification if deployed without careful validation on locally representative datasets [41], [45].

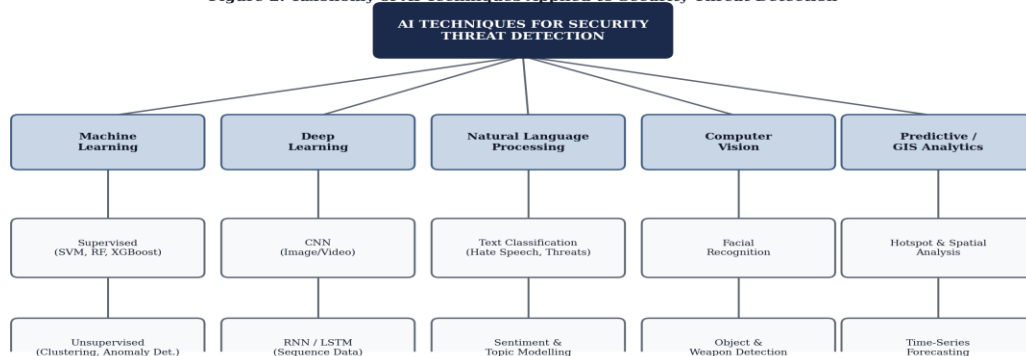
E. Predictive and Geospatial (GIS) Analytics

Geographic Information System (GIS)-based predictive analytics — including kernel density estimation, hotspot mapping and spatio-temporal forecasting models — has an established track record in international policing for identifying areas of elevated crime risk and allocating patrol resources accordingly [80], [83], [86]. A systematic review of nearly three hundred studies published between 2000 and 2023 documents the field's evolution from static crime mapping toward AI-integrated predictive models that incorporate socioeconomic, mobility and historical-incident data [82]. Applied to Northeast Nigeria, such methods are directly transferable to the mapping of insurgent movement corridors, IED-incident clusters, and cross-border infiltration routes into the Lake Chad basin, provided that the underlying incident data is of sufficient quality and geographic granularity [19], [20].

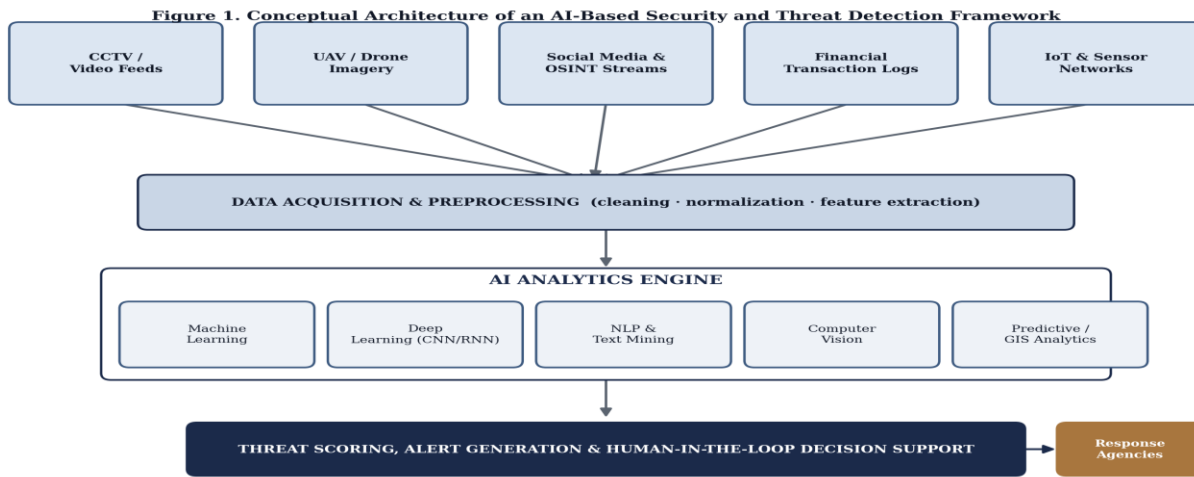
F. Sensor Fusion and the Internet of Things

Finally, the integration of AI with IoT sensor networks — acoustic gunshot-detection sensors, seismic and vibration sensors, and low-power edge devices — enables continuous, automated monitoring of remote areas without requiring constant human presence, addressing precisely the resource-asymmetry problem identified in Section III. UAV-based systems represent a particularly mature instance of this integration, combining onboard computer vision, GPS-based geofencing, and real-time data transmission to extend the reach of border and perimeter surveillance well beyond what fixed installations or foot patrols can achieve [60], [61], [64].

Figure 2. Taxonomy of AI Techniques Applied to Security Threat Detection



V. PROPOSED AI-BASED SECURITY FRAMEWORK



Building on the technique taxonomy in Section IV, this paper proposes a conceptual, layered architecture for integrating AI into Northeast Nigeria's security operations, illustrated in Figure 1. The architecture is deliberately generic with respect to the specific threat (insurgency, terrorism financing, or humanitarian-corridor security), on the premise that the same underlying pipeline — data acquisition, preprocessing, multi-model analysis, and human-in-the-loop decision support — can be instantiated with different data sources and models depending on the operational context.

A. Data Acquisition Layer

The foundation of the framework is a multi-source data acquisition layer drawing on CCTV and video feeds, UAV and drone imagery, social-media and open-source intelligence (OSINT) streams, financial-transaction logs, and IoT sensor networks. Given the resource constraints discussed in Section VIII, this layer should be designed for graceful degradation: a deployment that begins with a small number of fixed CCTV points and a modest social-media monitoring capability should still deliver operational value, with additional sources (UAV coverage, financial data feeds) layered in as budget and institutional capacity allow.

B. Preprocessing and Feature Extraction

Raw data from each source is rarely usable directly. Video streams require frame sampling and object detection before downstream classification; text data requires language identification, tokenization and normalization for Hausa, Kanuri, Fulfulde and Nigerian Pidgin English content; and financial-transaction logs require entity resolution and temporal aggregation before anomaly-detection models can operate on them effectively. This preprocessing stage is frequently underestimated in AI deployment planning, yet the quality of feature extraction has a first-order effect on downstream model accuracy [35], [36].

C. AI Analytics Engine

At the core of the framework sits a modular analytics engine comprising the five technique families discussed in Section IV — machine learning, deep learning, NLP, computer vision, and predictive/GIS analytics — operating where appropriate in parallel over the same preprocessed data. Modularity is important for two reasons: first, it allows individual models to be updated, retrained or replaced as new data becomes available without disrupting the entire pipeline; second, it allows lower-resource models (classical machine learning, lightweight NLP classifiers) to be substituted for computationally expensive deep-learning models in edge or low-

connectivity deployment contexts, consistent with the trade-offs summarized in Figure 4.

D. Threat Scoring and Human-in-the-Loop Decision Support

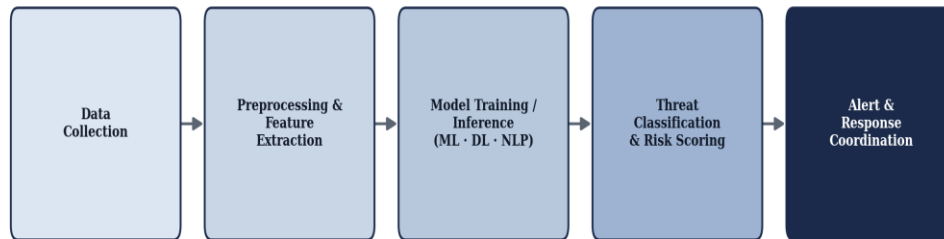
Outputs from the analytics engine are aggregated into a threat-scoring layer that assigns a composite risk score to each detected event or entity, incorporating confidence estimates from the underlying models. Critically, the framework treats this layer as decision support rather than autonomous decision-making: consistent with the explainable-AI literature's caution against blind reliance on algorithmic recommendations in law-enforcement contexts [99], [102], [104], the framework routes high-confidence, high-severity alerts to trained analysts for verification before any operational response is triggered, and it

retains an audit trail of both the algorithmic recommendation and the human decision for subsequent review.

E. Response Coordination

The final layer coordinates verified alerts with the relevant response agency — military, police, or civil-defense units, depending on the nature and severity of the threat — and, where applicable, financial-intelligence units in the case of fraud or terrorism-financing alerts. Feedback from response outcomes (false positive, confirmed threat, resolved incident) should be captured and fed back into the training pipeline for the relevant models, enabling the system to improve over time as more Nigeria-specific ground-truth data accumulates.

Figure 3. Generalized AI-Based Threat Detection Processing Pipeline



VI. APPLICATION DOMAINS

This section discusses six application domains in which the framework of Section V can be instantiated, drawing on both the international and Nigeria-specific literature.

A. Video Surveillance and Facial Recognition

AI-enhanced CCTV systems combining object detection, motion analysis and, where appropriate, facial recognition offer a direct upgrade path for urban and checkpoint security in Northeast Nigerian cities such as Maiduguri, Damaturu and Yola. Survey evidence from a comparable northern Nigerian state, Katsina, indicates that stakeholders view AI-integrated CCTV as capable of improving the monitoring of suspicious activity, supporting search-

and-rescue operations, and reducing response times — findings that plausibly generalize to Northeast Nigeria's own urban centers [6]. However, the demonstrated accuracy disparities of facial recognition across demographic groups [41], [45] mean that any deployment must be validated against locally representative data and paired with clear governance rules limiting the retention and secondary use of biometric data, consistent with the broader African experience of surveillance-technology deployment sparking civil-liberties concern where such safeguards were absent [44].

B. UAV and Drone-Based Reconnaissance

Unmanned aerial vehicles equipped with high-resolution and thermal cameras offer a means of extending surveillance coverage across the vast, often

inaccessible terrain characteristic of the North-East's forest reserves, riverine areas and the Lake Chad basin, without the cost and risk associated with manned aerial patrols. International deployments demonstrate mature use cases in border monitoring, obstacle avoidance, and real-time threat detection [60], [66], [68], and the underlying sensor and edge-computing technology continues to improve rapidly [61]. For Northeast Nigeria, UAV reconnaissance is particularly well suited to monitoring known insurgent movement routes and cross-border infiltration corridors into the Lake Chad basin identified through the geospatial analytics discussed below, allowing scarce manned assets to be directed toward the highest-priority areas.

C. Social Media and Open-Source Intelligence Monitoring

NLP-based monitoring of public social-media content, adapted to the multilingual character of Northeast Nigerian online discourse (Hausa, Kanuri and English), can help surface early indicators of radicalization, incitement, or coordinated mobilization that would otherwise be lost in the sheer volume of daily content [49], [57]. Such monitoring must, however, be carefully scoped to public content and clearly defined threat indicators; the same technology that can identify genuine incitement can, if deployed indiscriminately, chill legitimate political speech and civic organizing, a tension explicitly flagged in the international literature on AI-enabled surveillance [44], [87].

D. Financial Crime and Terrorism-Financing Detection

Insurgent groups rely on financial flows — ransom payments, extortion, informal taxation of communities under their influence, and increasingly formal or informal banking channels — that leave a transactional trace. Machine-learning-based anomaly detection, already being adopted at scale by Nigerian commercial banks and by the Central Bank of Nigeria's own Payments System Vision 2028 initiative [72], [74], can in principle be extended to flag transaction patterns consistent with ransom payment, extortion or terrorism financing, complementing the existing work of financial-intelligence units. The core

technical challenge here is class imbalance — genuinely fraudulent or illicit transactions represent a very small fraction of total activity — a problem well documented in the AI fraud-detection literature and requiring specialized handling through resampling, cost-sensitive learning or generative data-augmentation techniques [75].

E. Predictive Crime and Conflict Mapping

GIS-based hotspot analysis and spatio-temporal forecasting, applied to historical incident data on insurgent attacks, IED incidents and abduction events, can support the proactive allocation of security patrols to areas of elevated near-term risk, mirroring international predictive-policing practice [80], [82], [83]. Nigeria-specific applications of related clustering and geospatial-risk methods to Boko Haram and school-attack data demonstrate technical feasibility [19], [20], though the transferability of these methods to real-time operational use depends heavily on the quality, completeness and timeliness of the underlying incident-reporting data — a data-governance challenge discussed further in Section VIII.

F. Biometric Identity and Border Management

Weak border management has been repeatedly identified as a contributing factor in the cross-border movement of insurgents, weapons and abducted persons between Nigeria and its Lake Chad basin neighbors — Cameroon, Chad and Niger. AI-assisted biometric identity verification at formal and informal border crossings — building on Nigeria's existing National Identity Number infrastructure — combined with UAV and sensor-based monitoring of unmonitored crossing points, offers a plausible path toward tightening this vulnerability, though it raises its own data-protection and interoperability challenges that are beyond the immediate scope of this paper.

VII. ILLUSTRATIVE COMPARATIVE ANALYSIS

TABLE I
Comparative Characteristics of AI Technique Families for Security Threat Detection

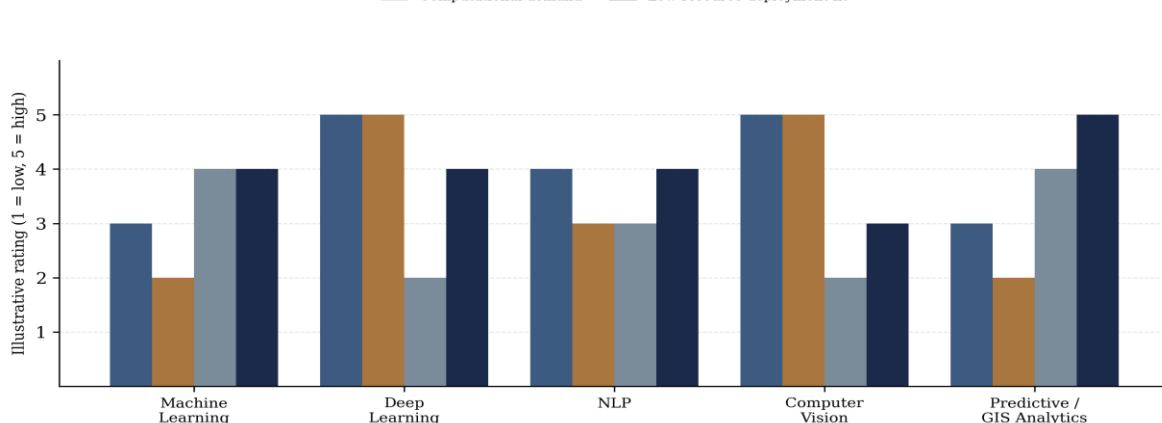
Technique	Primary Data Type	Typical Use Case	Relative Compute Cost	Interpretability
Machine Learning	Structured / tabular	Fraud detection, attack classification	Low	High
Deep Learning	Image, video, audio	Facial/weapon detection, IDS	High	Low
NLP	Text (social media, OSINT)	Extremism & hate-speech monitoring	Medium	Medium
Computer Vision	Image / video	CCTV & UAV surveillance	High	Low
Predictive / GIS	Geospatial + temporal	Hotspot mapping, patrol allocation	Low–Medium	High

To contextualize the trade-offs among the technique families discussed in Section IV, Table I summarizes their principal characteristics with respect to deployment in a resource-constrained security environment, and Figure 4 presents these characteristics graphically on an illustrative, literature-informed rating scale. It is important to emphasize that Figure 4 is a conceptual synthesis of general trends reported across the reviewed literature, rather than the output of a controlled empirical comparison on Nigerian operational data; no such controlled comparison currently exists in the public literature, and generating one is identified in Section IX as a priority for future work.

As Table I and Figure 4 indicate, classical machine learning methods offer the most favorable balance of interpretability and computational efficiency, making

them a sensible starting point for agencies with limited computing infrastructure, particularly for structured data such as financial transactions and tabular incident logs. Deep learning and computer-vision methods deliver substantially higher accuracy on unstructured image, video and audio data but at correspondingly higher computational and data-volume cost, which has direct implications for feasibility given the electricity and connectivity constraints discussed in Section VIII. NLP methods occupy an intermediate position, and predictive/GIS analytics — building as they do on well-established, computationally modest spatial-statistics techniques — offer a particularly favorable fit for low-resource deployment, provided that underlying incident data of adequate quality is available.

Figure 4. Illustrative Comparison of AI Technique Characteristics Relevant to Deployment in Northern Nigeria (Conceptual, Based on General Literature Trends)



VIII. CHALLENGES AND LIMITATIONS

The preceding sections have argued for the technical feasibility and operational relevance of AI-based threat detection in Northeast Nigeria. Responsible deployment, however, requires an honest accounting of the substantial constraints that condition what is realistically achievable in the near term.

A. Data Scarcity and Quality

Machine learning and deep learning models are only as good as the data on which they are trained, and Nigeria-specific security data — particularly labeled incident data linking attack characteristics to outcomes — remains scarce, fragmented across multiple agencies, and of uneven quality [9], [19]. Several of the Nigeria-focused studies reviewed in Section II explicitly relied on open-source or web-scraped data in the absence of structured official datasets [14], underscoring the urgency of formal data-governance and data-sharing arrangements among security agencies.

B. Electricity and Connectivity Constraints

AI systems, and deep-learning models in particular, require reliable electricity and network connectivity for continuous operation — precisely the infrastructure that remains least reliable in the rural and semi-urban areas most affected by insurgency. Recent analyses of AI adoption across Sub-Saharan Africa document that frequent power outages and constrained, costly internet access materially hinder real-time AI deployment, with an estimated several hundred million Africans still lacking reliable electricity access altogether [88], [91], [93]. Any Northeast Nigeria-focused deployment must therefore be designed around edge computing, offline-capable models, and solar-powered infrastructure where grid electricity is unavailable, rather than assuming continuous cloud connectivity.

C. Cost and Technical Capacity

AI deployment carries substantial upfront and recurring costs, and Nigeria faces a well-documented shortage of data-science and AI-engineering talent, which constrains both the initial deployment and the ongoing maintenance of these systems [74]. Smaller state-level security outfits, in particular, may lack the

budget to adopt AI-driven systems at the same pace as federal agencies or large commercial banks, risking uneven capability across the very states — Borno, Yobe, Adamawa — that face the most acute security threats.

D. Algorithmic Bias and Fairness

As discussed in Section VI-A, facial-recognition and other computer-vision systems have repeatedly demonstrated measurably higher error rates for darker-skinned individuals and other demographic subgroups when trained predominantly on non-representative datasets [41], [45]. Deploying such systems without local validation risks generating wrongful identifications with serious consequences in a security context, and risks entrenching biased policing outcomes of the kind documented in other algorithmic-decision domains [111].

E. Privacy, Civil Liberties and Function Creep

The African experience with surveillance-technology deployment includes documented instances of systems initially justified on crime-prevention grounds being repurposed to monitor political dissidents and civil-society actors [44]. Given Northeast Nigeria's fraught recent history of conflict and displacement, any AI-based social-media or biometric monitoring capability carries a genuine risk of misuse against political opponents, ethnic or religious minorities, or civil-society organizations if deployed without robust legal safeguards, independent oversight, and narrowly defined use-case authorization.

F. Explainability and Human Oversight

Black-box deep-learning models present a particular challenge in law-enforcement and security contexts, where decisions carry serious consequences for individual liberty and where any evidence derived from AI systems may ultimately face legal scrutiny [99], [104]. The explainable-AI (XAI) literature cautions that even well-designed explanation mechanisms do not, by themselves, guarantee appropriate reliance on AI recommendations, and that confirmation bias among human operators can undermine the intended safeguard of human-in-the-loop review [99]. This reinforces the framework design choice, discussed in Section V-D, to treat AI

outputs strictly as decision support requiring human verification rather than as autonomous authority.

G. Adversarial Manipulation

Finally, as with any AI-based security system, sufficiently sophisticated adversaries may attempt to manipulate or evade detection — for example, by structuring financial transactions to fall below anomaly-detection thresholds, or by adapting movement patterns in response to observed UAV surveillance routines. The cybersecurity literature on adversarial machine learning documents a range of such evasion techniques [33], [34], underscoring the need for continuous model retraining and red-teaming as part of any operational deployment.

IX. RECOMMENDATIONS AND POLICY IMPLICATIONS

Drawing on the preceding analysis, this paper offers the following recommendations for security agencies, technology developers and policymakers considering AI adoption for security purposes in Northeast Nigeria.

A. Establish Inter-Agency Data-Governance Frameworks

Federal and state security agencies should establish standardized data-collection protocols and secure data-sharing arrangements to address the data scarcity and fragmentation identified in Section VIII-A, drawing on Nigeria's existing National Artificial Intelligence Strategy as an institutional anchor [125].

B. Prioritize Low-Resource, Interpretable Models for Initial Deployment

Given the electricity, connectivity and capacity constraints documented in Section VIII, initial deployments should favor classical machine learning and lightweight NLP models over computationally intensive deep-learning architectures, reserving the latter for well-resourced urban centers or for offline batch-processing use cases such as periodic satellite-imagery analysis [98], [99].

C. Mandate Local Validation of Biometric and Computer-Vision Systems

Any facial-recognition or biometric system procured for security use should be validated for accuracy across Nigeria's demographic diversity before deployment, with published performance metrics disaggregated by relevant subgroups, consistent with international best practice on FRT governance [42], [48].

D. Build Legal and Oversight Safeguards Before Deploying Surveillance Capability

Legislative and regulatory frameworks governing the collection, retention, and use of biometric and social-media surveillance data should precede — not follow — large-scale deployment, with independent oversight mechanisms empowered to audit use-case compliance and investigate reported misuse.

E. Invest in Off-Grid and Edge Computing Infrastructure

Given the centrality of electricity access to AI feasibility, security agencies and development partners should prioritize solar-powered edge-computing infrastructure for rural surveillance nodes, consistent with emerging practice in other AI-for-development domains across the continent [93].

F. Build Domestic AI and Data-Science Capacity

Universities and technical institutions in Northeast Nigeria, including the University of Maiduguri, have a direct role to play in training the data-science and AI-engineering talent required to develop, deploy and maintain these systems locally, reducing long-term dependence on external vendors and improving contextual fit with local languages, terrain and threat patterns.

G. Treat AI as a Complement to, Not a Substitute for, Community Policing

Finally, AI-based threat detection should be explicitly positioned as a force multiplier that augments — rather than replaces — human intelligence networks, community engagement, and the socio-economic interventions that address the underlying drivers of insurgency. No AI system, however capable, can substitute for addressing the poverty, displacement

and governance gaps that continue to fuel recruitment into armed groups across Northeast Nigeria.

X. CONCLUSION

This paper has presented a comprehensive review and conceptual framework for the application of artificial intelligence to security and threat detection in Northeast Nigeria, a region confronting an unusually complex and geographically dispersed insurgency marked by mass displacement, cross-border movement and recurring abduction. Drawing on both the international technical literature and a growing body of Nigeria-specific scholarship, the paper has argued that machine learning, deep learning, natural language processing, computer vision and predictive geospatial analytics each offer genuine, complementary capabilities for extending the analytical reach of a security architecture that remains, in absolute terms, badly outmatched by the scale of territory and threat activity it must cover. The proposed layered framework — spanning data acquisition, preprocessing, a modular AI analytics engine, and human-in-the-loop threat scoring — is offered as a conceptual template rather than a finished operational system, intended to guide the phased, resource-appropriate adoption of these techniques by security agencies operating under genuine infrastructural and budgetary constraints.

At the same time, the paper has been deliberately candid about the limitations and risks of this technology: data scarcity, unreliable electricity, constrained technical capacity, algorithmic bias, and the real risk of surveillance overreach in a region with a fraught recent history of conflict and displacement. None of these constraints is a reason to forgo AI adoption altogether, but each is a reason to insist that adoption proceed with appropriate caution, transparency, and legal safeguards, and with sustained investment in the local data infrastructure and technical talent needed to ensure these systems are built for, and validated against, the specific realities of Northeast Nigeria rather than imported wholesale from other operating contexts. Future work should prioritize the empirical validation of the technique comparisons offered here against real Nigerian operational data, the development of Hausa, Kanuri

and Shuwa Arabic-language NLP resources for open-source intelligence monitoring, and rigorous, independent evaluation of any deployed system's accuracy, fairness and civil-liberties impact.

ACKNOWLEDGMENT

The authors acknowledge the Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Maiduguri, for institutional support during the preparation of this manuscript.

REFERENCES

- [1] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed. Hoboken, NJ: Pearson, 2021.
- [2] L. Floridi, *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities*. Oxford: Oxford Univ. Press, 2023.
- [3] A. Zakari and I. Musa, "Implication of artificial intelligence on national security for the Nigeria security agencies," *J. Terrorism Studies*, vol. 6, no. 1, art. 6, 2024, doi: 10.7454/jts.v6i1.1075.
- [4] O. Adeyemi et al., "Impact of artificial intelligence on cybersecurity in Nigeria," *American J. Computing and Engineering*, vol. 7, no. 2, pp. 45-58, 2024.
- [5] C. Okonkwo, "Artificial intelligence and the future of knowledge preservation: Implications for national security and strategic decision-making in Nigeria," *Center of Artificial Intelligence J.*, vol. 1, no. 1, pp. 47-54, Jan. 2026.
- [6] A. B. Mohammed, "Artificial intelligence as a tool for combating insecurity in Nigeria," *ResearchGate preprint*, Jul. 2022.
- [7] F. Yusuf, "Artificial intelligence and cybersecurity in Nigeria: Communicative strategies for risk mitigation and opportunities in digital security," *Top Academic J. Humanities and Social Sciences*, vol. 4, no. 2, pp. 12-29, Apr. 2025.
- [8] O. P. Ochinya, "Influence of artificial intelligence-based malware detection systems on the security of digital assets in public universities in Rivers State, Nigeria," *Int. J.*

- Educational Management, Rivers State Univ., vol. 2, no. 2, pp. 184-198, 2026.
- [9] M. A. Suleiman, "Role of artificial intelligence in intelligence gathering and national security management in Nigeria," *Int. J. Social Sciences and Applied Research*, vol. 3, no. 3, pp. 206-225, Sep. 2025.
- [10] A. C. Okoli and P. Iortyer, "Terrorism and humanitarian crisis in Nigeria: Insights from Boko Haram insurgency," *Global J. Human Social Science*, vol. 14, no. 1, pp. 39-49, 2014.
- [11] E. Ben-Edet, "Terrorism: A case study of the global security threat of Boko Haram and the ISIS alliance in Nigeria," Ph.D. dissertation, Texas Southern Univ., Houston, TX, 2022.
- [12] Institute for Economics and Peace, *Global Terrorism Index 2023: Measuring the Impact of Terrorism*. Sydney: IEP, 2023.
- [13] O. E. Adeyemi, "Data science insights and the classification of terrorist attacks in Nigeria using machine learning techniques," *ResearchGate preprint*, Oct. 2024.
- [14] T. Onuoha, "Prediction of crime in Nigeria using artificial intelligence," *ResearchGate preprint*, Jun. 2024.
- [15] V. S. Subrahmanian, A. Mannes, A. Silva, J. Shakarian, and J. P. Dickerson, *Computational Analysis of Terrorist Groups: Lashkar-e-Taiba*. New York: Springer, 2013.
- [16] J. O. Braimah, "Predicting the path of insurgency: Data-driven strategies to counter Boko Haram in Nigeria," *F1000Research*, vol. 13, art. 989, Sep. 2024.
- [17] Techpoint Africa, "Predictive policing, Boko Haram and the Nigerian security challenges," *Techpoint Africa*, Dec. 2015.
- [18] O. I. Abiodun, A. Janta, A. E. Omolara, M. M. Singh, L. Z. Abubakar, and A. M. Umar, "Big data: An approach for detecting terrorist activities with people's profiling," in *Proc. Int. MultiConf. Engineering and Computer Science (IMECS)*, Hong Kong, 2018.
- [19] N. Nwokorie, "Big data analytics of Boko Haram insurgency attacks menace in Nigeria using dynamic k-reference clustering algorithm," *ResearchGate preprint*, Jun. 2020.
- [20] E. Kolawole, "A quantitative geospatial analysis of the risk that Boko Haram will target a school," *PLOS Global Public Health*, 2023.
- [21] Southern African Times, "Harnessing artificial intelligence to combat insecurity and violence in Nigeria," *Southern African Times*, Apr. 2025.
- [22] Human Rights Watch, *World Report 2026: Nigeria*. New York: HRW, 2026.
- [23] The Soufan Center, "From criminality to insurgency: The convergence of bandits and jihadists in Nigeria's northwest," *IntelBrief*, The Soufan Center, Aug. 2025.
- [24] A. B. Abraham, C. Ojo, and M. Ezeibe, "Weak border management and banditry in the northwest region, Nigeria," *Int. J. Research and Innovation in Applied Science*, vol. 10, no. 4, pp. 1-14, 2025.
- [25] U. Ibrahim, "Full article: Forces of terror: Armed banditry and insecurity in north-west Nigeria," *African Security Review*, vol. 33, no. 2, 2023, doi: 10.1080/17419166.2023.2164924.
- [26] K. J. Danjuma, "Shock and awe: Military response to armed banditry and the prospects of internal security operations in northwest Nigeria," *Scientia Militaria*, vol. 51, no. 1, 2023, doi: 10.1080/10246029.2023.2246432.
- [27] S. Aliyu, "The impact of banditry on Nigeria's security in the Fourth Republic," *Zamfara J. Politics and Development*, vol. 4, no. 1, 2023.
- [28] SBM Intelligence, "Nigeria's north-west security situation: 2026 overview," *SBM Intelligence Report*, 2026.
- [29] Reuters, "'Armed bandits' kill 47 in northwest Nigeria's Katsina state: police," *Reuters News*, Bauchi, Nigeria, 2025.
- [30] Reuters, "Gunmen kidnap 20 in northwest Nigeria as crisis spreads," *Reuters News*, Maiduguri, Nigeria, 2021.
- [31] H. M. Yusuf, "Overview of banditry and kidnapping scenarios in Katsina and Zamfara states of North West Nigeria: An Islamic antidote," *ResearchGate preprint*, Jun. 2024.
- [32] Z. Xu, Y. Wu, S. Wang, J. Gao, T. Qiu, Z. Wang, H. Wan, and X. Zhao, "Deep learning-

- based intrusion detection systems: A survey," ACM Computing Surveys, 2025.
- [33] A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning for intrusion detection in emerging technologies: A comprehensive survey and new perspectives," Artificial Intelligence Review, Springer, 2025.
- [34] W. Yang, A. Acuto, Y. Zhou, and D. Wojtczak, "A survey for deep reinforcement learning based network intrusion detection," arXiv:2410.07612, 2024.
- [35] L. Zhang et al., "A review of deep learning applications in intrusion detection systems: Overcoming challenges in spatiotemporal feature extraction and data imbalance," Applied Sciences, vol. 15, no. 3, art. 1552, 2025.
- [36] K. Ahmed et al., "Performance analysis of explainable deep learning-based intrusion detection systems for IoT networks: A systematic review," PMC, 2026.
- [37] H. Wang et al., "In-vehicle network intrusion detection systems: A systematic survey of deep learning-based approaches," Cybersecurity, Springer, 2023.
- [38] E. Hodo, X. Bellekens, A. Hamilton, C. Tachtatzis, and R. Atkinson, "Shallow and deep networks intrusion detection system: A taxonomy and survey," arXiv:1701.02145, 2017.
- [39] Y. Xin et al., "Review: Deep learning methods for cybersecurity and intrusion detection systems," arXiv:2012.02891, 2020.
- [40] S. MahdaviFar and A. A. Ghorbani, "Application of deep learning to cybersecurity: A survey," Neurocomputing, vol. 347, pp. 149-176, 2019.
- [41] IAPP, "Notes from the Asia-Pacific region: Facial recognition technology's ethical, privacy concerns cannot be overlooked," IAPP News, 2026.
- [42] International Compliance Association, "Ethical compliance for facial recognition technology," ICA Insight, 2025.
- [43] H. Palmiotto and E. Gonzalez, "Beyond surveillance: Privacy, ethics, and regulations in face recognition technology," Frontiers in Big Data, vol. 7, art. 1337465, 2024.
- [44] Africa Center for Strategic Studies, "The spread of surveillance technology in Africa stirs security concerns," ACSS Spotlight, 2023.
- [45] Institute for Security Studies, "Future of facial recognition technology in Africa," ISS Today, ISS Africa, 2021.
- [46] C. Kind, "Facial recognition technology and privacy concerns," ISACA Journal, vol. 51, 2022.
- [47] IEEE Public Safety Technology Initiative, "Ethical considerations in the use of facial recognition for public safety," IEEE Public Safety, 2025.
- [48] D. Adeyemi and R. Kariuki, "The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: A comparative analysis of US, EU, and UK regulatory frameworks," PMC, 2021.
- [49] S. Alatwi, A. Alhothali, and K. Moria, "Detection of hate speech using BERT and hate speech word embedding with deep model," arXiv:2111.01515, 2021.
- [50] M. Springer et al., "Enhancing social media hate speech detection in low-resource languages using transformers and explainable AI," Social Network Analysis and Mining, vol. 15, 2025.
- [51] F. Del Vigna, A. Cimino, F. Dell'Orletta, M. Petrocchi, and M. Tesconi, "Challenges of hate speech detection in social media," SN Computer Science, vol. 2, 2021.
- [52] J. Lu, H. Lin, X. Zhang, Z. Li, T. Zhang, L. Zong, F. Ma, and B. Xu, "Hate speech detection via dual contrastive learning," arXiv:2307.05578, 2023.
- [53] J. D. Gallacher, "Leveraging cross-platform data to improve automated hate speech detection," arXiv:2102.04895, 2021.
- [54] K. Alrehili, "Use of natural language processing for the detection of hate speech on social media," ResearchGate preprint, Sep. 2024.

- [55] A. Rana and S. Jha, "Emotion based hate speech detection using multimodal learning," arXiv:2202.06218, 2022.
- [56] K. Mnassri, R. Farahbakhsh, and N. Crespi, "Multilingual hate speech detection: A semi-supervised generative adversarial approach," *Entropy*, vol. 26, no. 4, art. 344, 2024.
- [57] O. Ali, "Leveraging natural language processing to analyse the temporal behavior of extremists on social media," ResearchGate preprint, Oct. 2024.
- [58] H. Saleh, A. Alhothali, and K. Moria, "Detection of hate speech using BERT and hate speech word embedding with deep model," King Abdulaziz Univ. tech. rep., 2021.
- [59] S. G. Roy, U. Narayan, T. Raha, Z. Abid, and V. Varma, "Leveraging multilingual transformers for hate speech detection," arXiv:2101.03207, 2021.
- [60] JOUAV, "Border patrol drone: How are drones used for border security?," JOUAV Technical Report, 2026.
- [61] ACM Computing Surveys, "Future UAV/drone systems for intelligent active surveillance and monitoring," ACM Computing Surveys, 2026.
- [62] S. K. Islam et al., "6G communications: A vision on the potential applications," arXiv:2005.07531, 2020.
- [63] J. Vasquez et al., "Towards real-time fast unmanned aerial vehicle detection using dynamic vision sensors," arXiv:2403.11875, 2024.
- [64] U.S. Patent Office, "Unmanned aerial vehicle based security system," U.S. Patent 10,204,520, 2019.
- [65] H. Chen, S. Chen, and W. Zhao, "Small object detection: A comprehensive survey on challenges, techniques and real-world applications," arXiv:2503.20516, 2025.
- [66] L. Pollozek, "Automated decision-making and artificial intelligence at European borders and their risks for human rights," arXiv:2410.17278, 2024.
- [67] Elistair, "Cross border surveillance drone: Our solutions," Elistair Technical Documentation, 2026.
- [68] Aeronautics Defense Systems, "UAVs for border surveillance," Aeronautics Technical Brief, 2025.
- [69] Inside Unmanned Systems, "Border patrol: Detecting and countering threats," Inside Unmanned Systems, 2025.
- [70] J. Adebayo, "The impact of artificial intelligence (AI) on fraud detection in banks in Nigeria," ResearchGate preprint, Sep. 2025.
- [71] O. Ajala and T. Balogun, "Harnessing artificial intelligence and machine learning for fraud detection and prevention in Nigeria," ScienceDirect, 2025.
- [72] iAfrica, "Central Bank of Nigeria deploys AI and machine learning to cut financial fraud losses by 70% by 2028," iAfrica News, Jun. 2026.
- [73] Devdiscourse Technology Desk, "AI in fraud detection: Nigeria's new defense against financial crimes," Devdiscourse, 2025.
- [74] E. C. Chianumba, "The role of artificial intelligence in enhancing cybersecurity and fraud detection in Nigerian banks," ResearchGate preprint, Aug. 2025.
- [75] A. A. Abohany et al., "AI-integrated approaches for credit card fraud detection: A systematic review," ResearchGate preprint, 2025.
- [76] O. I. Odufisan, O. V. Abhulimen, and E. O. Ogunti, "AI-powered fraud detection in digital banking: Enhancing security through machine learning," ResearchGate preprint, Mar. 2025.
- [77] CreedTec, "Machine learning fraud detection for mobile money in Nigeria: A critical defense," Medium, Dec. 2025.
- [78] A. J. Bello, "Artificial intelligence-enabled accounting information systems and fraud detection in Nigeria's financial services sector: The moderating role of natural language processing," arXiv:2607.01257, 2026.
- [79] K. O. Adigun, "Adoption of AI-driven fraud detection system in the Nigerian banking sector: An analysis of cost, compliance, and competency," arXiv:2511.00061, 2025.
- [80] Atlas GIS, "Predictive policing - GIS use cases," Atlas Knowledge Base, 2024.

- [81] IJIRT, "The use of geographic information system (GIS) in predictive policing," *Int. J. Innovative Research and Technology*, 2025.
- [82] A. Cheng and Q. Chen, "Evolution and prospects of geographic information systems (GIS) applications in urban crime analysis: A review of literature," *ScienceDirect*, 2025.
- [83] Y. Hu, F. Wang, C. Guin, and H. Zhu, "A spatio-temporal kernel density estimation framework for predictive crime hotspot mapping and evaluation," *Applied Geography*, vol. 99, pp. 89-97, 2018.
- [84] C. E. Catlett et al., "Analysis of criminal spatial events in GIS for predicting hotspots," *ResearchGate preprint*, Nov. 2020.
- [85] Bent Ear Solutions, "GIS crime mapping: How law enforcement uses spatial data," *Bent Ear Solutions Blog*, 2026.
- [86] Spatial Eye, "Understanding hot spot analysis in crime prevention," *Spatial Eye Insights*, 2026.
- [87] M. Oswald, "Transparency, governance and regulation of algorithmic tools deployed in the criminal justice system: A UK case study," *arXiv:2205.15258*, 2022.
- [88] Global Voices Advox, "A lack of electricity and internet access hinders AI adoption in Sub-Saharan Africa," *Global Voices*, Apr. 2026.
- [89] A. K. Mensah et al., "Themed challenges to solve data scarcity in Africa: A proposition for increasing local data collection and integration," *arXiv:2508.00925*, 2025.
- [90] T. Osei et al., "Artificial intelligence for public health surveillance in Africa: Applications and opportunities," *arXiv:2408.02575*, 2024.
- [91] Frontiers in Energy Research, "Aligning artificial intelligence and electricity systems for sustainable development in Africa," *Frontiers in Energy Research*, vol. 14, art. 1845467, 2026.
- [92] M. Adeyeye et al., "Harnessing artificial intelligence for sustainable agricultural development in Africa: Opportunities, challenges, and impact," *arXiv:2401.06171*, 2024.
- [93] African Leadership Magazine, "Africa's digital divide: Why AI success demands reliable energy," *African Leadership Magazine*, 2026.
- [94] F. Witmer, "Remote sensing of violent conflict: Eyes from above," *Int. J. Remote Sensing*, vol. 36, no. 9, pp. 2326-2352, 2015.
- [95] H. Baker, R. Braithwaite, and B. Chen, "Monitoring war destruction from space using machine learning," *Proc. Nat. Acad. Sci. (PNAS)*, vol. 118, no. 23, 2021.
- [96] L. Gueguen and R. Hamid, "Large-scale damage detection using satellite imagery," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, 2015, pp. 1321-1328.
- [97] N. Jean, M. Burke, M. Xie, W. M. Davis, D. B. Lobell, and S. Ermon, "Combining satellite imagery and machine learning to predict poverty," *Science*, vol. 353, no. 6301, pp. 790-794, 2016.
- [98] C. Yeh, A. Perez, A. Driscoll, G. Azzari, Z. Tang, D. Lobell, S. Ermon, and M. Burke, "Using publicly available satellite imagery and deep learning to understand economic well-being in Africa," *Nature Communications*, vol. 11, art. 2583, 2020.
- [99] J. Z. Xu, W. Lu, Z. Li, P. Khaitan, and V. Zaytseva, "Building damage detection in satellite imagery using convolutional neural networks," *arXiv:1910.06444*, 2019.
- [100] M. Sticher, S. Wegner, and L. Pfeifle, "Toward the remote monitoring of armed conflicts," *PNAS Nexus*, vol. 2, no. 6, art. pgad181, 2023.
- [101] R. Engstrom, D. Newhouse, and J. Hersh, "Poverty from space: Using high resolution satellite imagery for estimating economic well-being and geographic targeting," *World Bank Policy Research Working Paper*, 2017.
- [102] F. Selten, "Explainable AI is no silver bullet: Towards a contextual understanding of appropriate reliance on AI in law enforcement," in *Public Administration and Artificial Intelligence*, Springer, 2025, ch. 4.
- [103] Proofpoint, "What is explainable AI (XAI)? Definition, methods and more," *Proofpoint Threat Reference*, 2026.

- [104] M. Robeer, "Beyond trust: A causal approach to explainable AI in law enforcement," Ph.D. dissertation, Utrecht Univ., 2025.
- [105] OpenReview, "Mitigating bias in generative AI: The role of explainable AI," OpenReview preprint, 2025.
- [106] H. Rong et al., "Explainable AI for facilitating recognition of algorithmic bias: An experiment from imposed users' perspectives," ScienceDirect, 2024.
- [107] L. Zhang, "Algorithmic governance for explainability: A comparative study," arXiv:2303.00651, 2023.
- [108] A. B. Arrieta et al., "Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI," Information Fusion, vol. 58, pp. 82-115, 2020.
- [109] A. Rawal, J. McCoy, D. B. Rawat, B. M. Sadler, and R. S. Amant, "Recent advances in trustworthy explainable artificial intelligence: Status, challenges, and perspectives," IEEE Trans. Artificial Intelligence, vol. 3, pp. 852-866, 2021.
- [110] M. T. Ribeiro, S. Singh, and C. Guestrin, "'Why should I trust you?': Explaining the predictions of any classifier," in Proc. 22nd ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining, 2016, pp. 1135-1144.
- [111] Z. Obermeyer, B. Powers, C. Vogeli, and S. Mullainathan, "Dissecting racial bias in an algorithm used to manage the health of populations," Science, vol. 366, no. 6464, pp. 447-453, 2019.
- [112] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, pp. 436-444, 2015.
- [113] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA: MIT Press, 2016.
- [114] C. Cortes and V. Vapnik, "Support-vector networks," Machine Learning, vol. 20, no. 3, pp. 273-297, 1995.
- [115] L. Breiman, "Random forests," Machine Learning, vol. 45, no. 1, pp. 5-32, 2001.
- [116] S. Hochreiter and J. Schmidhuber, "Long short-term memory," Neural Computation, vol. 9, no. 8, pp. 1735-1780, 1997.
- [117] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," in Advances in Neural Information Processing Systems (NeurIPS), 2012, pp. 1097-1105.
- [118] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "BERT: Pre-training of deep bidirectional transformers for language understanding," in Proc. NAACL-HLT, 2019, pp. 4171-4186.
- [119] A. Vaswani et al., "Attention is all you need," in Advances in Neural Information Processing Systems (NeurIPS), 2017, pp. 5998-6008.
- [120] S. Chainey and J. Ratcliffe, GIS and Crime Mapping. Chichester, UK: Wiley, 2013.
- [121] T. Chukwuma, "Financial fraud detection using AI in Nigeria's banking sector," Finance and Security Journal, vol. 17, no. 6, pp. 23-39, 2023.
- [122] World Bank Group, Digital Economy for Africa: Nigeria Country Diagnostic. Washington, DC: World Bank, 2023.
- [123] National Bureau of Statistics, Nigeria Crime Statistics Report 2024. Abuja: NBS, 2024.
- [124] International Telecommunication Union, Measuring Digital Development: Facts and Figures 2025. Geneva: ITU, 2025.
- [125] National Information Technology Development Agency (NITDA), National Artificial Intelligence Strategy. Abuja: NITDA, 2024.
- [126] African Union, Continental Artificial Intelligence Strategy. Addis Ababa: African Union Commission, 2024.