Digital Innovations & Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY
Vol. 14. No. 3, September 2026 Series

Article Citation Format
Ojerinde, O.A., Ojeniyi, J.A., Uduimoh A.A. & Noibi A.K. (2026): A Systematic Literature Review on the Logistics of Kidnapping and Banditry in Asymmetric Warfare: Problem Classes, Datasets, and Open Issues. Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology. Vol. 14, No. 3. Pp 9-30. www.isteams.net/digitaljournal dx.doi.org/10.22624/AIMS/DIGITAL/V14N3P2

Article Progress Time Stamps
Article Type: Research Article
Manuscript Received: 17th June, 2026
Review Type: Blind Peer
Final Acceptance: 22nd August, 2026

A Systematic Literature Review on the Logistics of Kidnapping and Banditry in Asymmetric Warfare: Problem Classes, Datasets, and Open Issues

[1]Ojerinde, O.A., [2]Ojeniyi J.A., [2]Uduimoh A. A. & [1]Noibi A.K.
[1]Department of Computer Science
[2]Department of Cybersecurity Science
Federal University of Technology
Minna, Niger State, Nigeria
E-mails: o.ojerinde@futminna.edu.ng, ojeniyija@futminna.edu.ng, a.uduimoh@futminna.edu.ng, abdulsalaam.m2203569@st.futminna.edu.ng

ABSTRACT

In rural conflict settings, getting actionable intelligence to military and security actors is difficult: formal communication channels reach few areas, the need for timely intelligence is high, and resources for collecting it are limited. Armed conflict, criminal banditry and kidnapping rely heavily on widely dispersed and informal communications and logistics systems in rural areas, yet reliable grassroots intelligence in these areas remains difficult to gather. This critical review of the literature examines the boundaries and challenges of bottom-up intelligence gathering in low-bandwidth, high-risk rural conflict zones, where conventional policing and data-driven intelligence are least effective. Following PRISMA guidelines, the review selected peer-reviewed studies published between 2010 and 2025 that offered empirical or conceptual analysis relevant to this problem. Eligible studies examined information flows within and to affected communities, human intelligence (HUMINT), and field data collection, conducted in insecure settings with limited infrastructure and state presence. The review underscores the effect of insecurity, mistrust and fear of reprisals on local reporting; challenges in degraded communications, poor connectivity and unreliable electricity for timely transmission and verification of field data; and struggles in collecting data on standardised questionnaires because of low literacy, language diversity and cultural issues. It also draws attention to institutional and methodological issues that influence the representativeness and validity of the data, such as the lack of equipment for intelligence units, ad hoc sampling, and a high level of bias in the reporting of events and actors. Existing frameworks and technologies, including reporting schemes, mobile data collection, and open-source intelligence, have narrowed these gaps only partially, remaining constrained by limited bandwidth and persistent community mistrust and security concerns. However, the evidence remains fragmented across disciplines, existing reviews have not systematically addressed rural grassroots intelligence, and this area has received limited dedicated attention despite its practical importance. Effective grassroots intelligence gathering therefore depends on approaches that are resilient to poor communications, participatory and reflexive in design, oriented toward trust-building, and equipped with clear safeguards for protecting sources. These insights inform the design and evaluation of a proactive threat-intelligence architecture for rural conflict settings, directly addressing the gap identified above.

Keywords: Armed Banditry, Criminal Logistics, Community Intelligence, Asymmetric Warfare

1. INTRODUCTION

Asymmetric warfare has taken on very different forms in today's low-government/weak-state areas, with kidnapping and banditry now flourishing as the main forms of rural insecurity. For example, in northwest region of Nigeria, armed banditry is characterised by violent displacement, cattle capture/rustling, mass abductions, killings, and the continuous disruption of rural livelihoods and has proved to be a sophisticated, complex technique of banditry today, which affects civilians' confidence in the state's ability to provide protection for them (Ojo et al., 2023). Likewise, in other "ungoverned" regions or poorly governed places, insurgent groups, militias and criminal entrepreneurs use the challenging topography and the poor management of logistics and borders to fuel violent practices and predatory economies (Ojo, 2020).

Although these dynamics are usually studied in the context of security and humanitarian actors, the importance of multi-layer datasets and sensing technologies in modern conflict environments (MTM) is increasingly emerging. The use of remote sensing and geospatial analytics, for instance, in monitoring displacement patterns, destruction of infrastructure, and changing conflict dynamics, with the resulting near real-time situational awareness for humanitarian and security actors, is widely used (Avtar et al., 2021). Alongside this, non-ground truth datasets are now being used to identify spatiotemporal changes in land use, population and settlement patterns using machine learning approaches, further enhancing the capacity for remote conflict monitoring (Mhanna et al., 2023; Sticher et al., 2023). Furthermore, as crowdsourcing and social media data analysis become a new area of data collection and tools, there is an opportunity to use it as supplementary information to inform and fill gaps in official data on the subject of abductions and disappearances, especially when combined with data from institutions in both digital and face-to-face settings (Garcia et al., 2021).

Despite these technological innovations, the vast majority of literature on kidnapping and banditry remains to be informed rather by security and humanitarian issues than by the fact of it being an organised transport system characterised by spatial, temporal and organisational features. Existing conflict datasets and spatial markers are able to provide information on the dates and places of violent events and their development over time (Walther et al., 2023), but they are not typical of the operational systems that underlie such events. This includes supply lines in abductions and ransom payment networks; safe havens; and multimodal transport networks along roads, informal trails and electronic communication networks that allow these activities to continue. On the other hand, an increasing volume of work in humanitarian logistics and supply chain management has been devoted to optimising and rebuilding normal transportation flows under the supply chain framework in disaster and conflict situations (Jabbour et al., 2019). What has not been explored is the ability of such similar analytical frameworks to model illicit and adversarial logistics in contested and low-governance regions.

Consequently, no single, consolidated view yet exists covering the following:

i. The problem classes that characterise the logistics of this form of asymmetric warfare: kidnapping and banditry.
ii. Datasets acquired over the internet that have a large number of observations can be massively analysed in "low bandwidth and non-governed" environments and are of a crowdsourced, remotely acquired or administrative type.
iii. The assessment measures that are used to separate proactive disruption from reactive policing.

This literature review is intended to remedy that lacuna and provides a summary and classification of a heterogeneous collection of literature scattered across the study of security in asymmetric conflicts, the use of remote sensing, humanitarian logistics, and computational social science to explicitly identify problem classes related to logistics, classify the existing data resources and critically assess current and future metrics used to detect, predict and counter kidnapping and banditry in the field of asymmetric warfare.

2. PROCESS OF THE SYSTEMATIC LITERATURE REVIEW (SLR)

To achieve this, a structured SLR approach is used, whereby the review is divided into three parts in which research relevant to kidnapping and banditry and its logistics as a form of asymmetric warfare is systematically identified, evaluated and synthesised.

2.1 Planning the Review

The logistical aspect of kidnapping and banditry was identified in the planning phase simply because armed banditry, kidnapping, and the related humanitarian crisis have been reported to be on the rise in some areas of the country, including North-West Nigeria (Ojo et al., 2023; Saminu et al., 2023). The review protocol is developed based on previous systematic and scoping reviews carried out on humanitarian logistics (Jabbour et al., 2019), remote sensing for peace and security (Avtar et al., 2021) and armed conflict monitoring (Sticher et al., 2023). Finally, the suitability of these standards is checked, modified and refocused to concentrate on the problem classes, the data sets and assessment metrics.

2.2 Conducting the Review

The conduct phase includes six steps, following the SLR guidelines:

1. Research Questions (RQs): Based on conflict and logistics-focused information review, research questions are posed to identify articles available that might shed light on (a) how kidnapping/banditry works logistically; (b) sensing modalities and data sources used (e.g., remote sensing, crowdsourcing); and (c) metrics for measuring kidnapping/banditry disruption and policing effectiveness.
2. Occurrence of Search Strategy (SS): A multiple-database search strategy is used as in past studies, using combinations of keywords across multiple databases. A snowballing approach was also used to extend the search corpora by backward and forward chaining, as well as the use of search facilities such as Scopus and Web of Science. (Jabbour et al., 2019; Sticher et al., 2023; Avtar et al., 2021).
3. Study Selection Criteria (SSC): Inclusion and exclusion criteria were established first, then applied to screen the title and abstract of each article. Articles retrieved in full text covered armed banditry, logistics of insurgency, humanitarian supply chains, remote/conflict monitoring, and rural policing in resource-rich and “ungoverned” areas (Ojo, 2020; Jabbour et al., 2019).
4. Methodological rigour based on logistics reviews and originality of research methodology (Jaiswal and Bhaskar, 2015); data transparency; methodology; and limitations (Kumar and Mahendran, 2016) are evaluated through the Quality Assessment Criteria (QAC) adapted from logistics and remote-sensing reviews (Xu et al., 2024; Guo et al., 2024).
5. Data Extraction and Monitoring (DEM): The developed extraction form provides a standardised collection of bibliographic data, contextual information on conflicts, problem classes of logistical issues, and data sources which include event data, remote sensing, and crowdsourced reports are evaluated (Al-Dhaqm et al., 2021; Jabbour et al., 2019).

6. Data Synthesis (DS): A structured synthesis, including descriptive coding and thematic analysis, is carried out, classifying studies by logistics problem classes, dataset types, sensing platforms, and assessment metrics, exposing vulnerabilities and research gaps (Jabbour et al., 2019; Xu et al., 2024).

2.3 Reporting the Review

In the last phase, the SLR is shared in an appropriate way with both an academic and practitioner-oriented audience. Flowcharts are used to show the selection process, which is informed by previous reviews (Avtar et al., 2021; Jabbour et al., 2019; Sticher et al., 2023), and tables provide a summary of key characteristics and classifications of the studies selected.

2.4 Research Questions (RQs)

Research questions (RQs) help to articulate the overall purpose and results of a study. Research questions come to the fore as the research is developed, and care is taken to ensure they are useful to the investigators in order to increase the chances of arriving at certainty regarding an area. Five questions (RQ1–RQ5) were followed up to better understand recent experiences in the kidnapping and banditry aspect of asymmetric warfare within the region in Table 1. The logistical links in armed syndicates, as reported in the literature, are analysed for the first time (Research Question 1). The datasets used for the mapping of conflict areas and monitoring of criminal logistics are discussed in the second (RQ2). The metrics applied to evaluate efficiency for proactive intelligence gathering and threat detection are evaluated in the context of the third research question (RQ3). The value and weaknesses of intelligence-based policing, compared to conventional reactive military operations, are clarified under the fourth research question (RQ4). Finally (RQ5), the constraints of the personal intelligence-gathering process, as well as the network infrastructure that rural environments with low bandwidth present, are examined. The objective mapping of RQs is explained in Table 1.

TABLE 1: Define research questions for the SLR

QID	Research Questions	Objectives
RQ1	How are the logistical supply chain dependencies of kidnapping and banditry syndicates categorising?	To identify and categorise the primary logistical supply chain dependencies and operational vulnerabilities of organised armed groups in rural environments.
RQ2	What datasets are commonly utilised to map asymmetric warfare and criminal logistics?	To identify and evaluate the availability of peer-reviewed and non-peer-reviewed conflict datasets commonly used for tracking asymmetric threats and criminal networks.
RQ3	What evaluation metrics are used to compute the performance of proactive threat detection and intelligence gathering?	To identify the evaluation metrics commonly used to assess the effectiveness and efficiency of proactive intelligence gathering and threat disruption strategies.
RQ4	What is the performance of intelligence-led policing compared to traditional reactive military responses?	To critically evaluate the performance of proactive, intelligence-led policing by comparing its disruption effectiveness against traditional kinetic or reactive military operations in rural conflict zones.
RQ5	What are the limitations and challenges in acquiring grassroots intelligence in these environments?	To analyse the critical infrastructural barriers, security risks, and communication challenges associated with acquiring civilian intelligence in low-bandwidth, high-risk rural conflict zones.

2.5 Search Strategy (SS)

An extensive investigation was not limited to only a few databases. A considerable number of repositories provide access to research articles; however, the focus was placed on popular repositories that are relevant and accessible, as described below.

- Digital Library ACM
- Digital Library, ScienceDirect (ELSEVIER)
- SpringerLink
- Google Scholar
- Semantic Scholar
- ResearchGate
- Arxiv
- Wiley Online Library
- IEEE Xplore

Journals, conferences and archives are included in the repositories. Our search is limited to 60 months – from January, 2020 to December, 2025. The search keywords and terms for this SLR are as follows: kidnapping/armed banditry, logistics/supply chain and community intelligence/rural security. Drugs / Alcohol / Substances: "drug crimes" "alcohol offences" "substances of abuse" "drug trafficking" "alcohol trafficking" "trafficking in substances of abuse" "trafficking in drugs" "trafficking in alcohol" "trafficking in substances of abuse" "trafficking in drugs" "trafficking in alcohol" Other terms for logistics include "supply chain", "resource procurement", "illicit supply", "criminal logistics", "arms trafficking", "supply network", "resource dependencies" and "illicit networks. Community Intelligence / Rural Security: "community intelligence", "grassroots reporting", "whistleblowing", "rural policing", "low-bandwidth environments", "informant protection", "offline data collection", "intelligence gathering" and "spatial conflict data".

2.6 Boolean Search

The purpose was to collect as many works as possible that are related to the research questions. An attempt was made to find all possible coinciding search phrases/countries, but to be sure, every possible combination of search terms was applied in order to gather research data on kidnapping, banditry and grassroots intelligence barriers. The main idea in Boolean is introducing 'and' and/or 'or' to the people who are searching for 'terms'. From the community intelligence perspective, the word cloud analysis of the concept Disruption of criminal logistics is displayed in Figure 1. The search words can be outlined primarily: ("kidnapping" OR "rural banditry" OR "armed banditry" OR "asymmetric warfare" OR "organised crime" OR "insurgency" OR "terrorist networks" OR "armed groups" OR "violent non-state actors") AND (("logistics" OR "supply chain" OR "resource procurement" OR "illicit supply" OR "criminal logistics" OR "arms trafficking" OR "supply network" OR "resource dependencies" OR "illicit networks") AND (("community intelligence" OR "grassroots reporting" OR "whistleblowing" OR "rural policing" OR "low-bandwidth environments" OR "informant protection" OR "offline data collection" OR "intelligence gathering" OR "spatial conflict data")).

Figure 1: Word Clouds analysis regarding Disruption of Criminal logistics based on Community Intelligence

2.7 Study Selection Process

The evidence gathering process is documented in a PRISMA flowchart, as depicted in Figure 2, which outlines the data selection and evaluation stages.

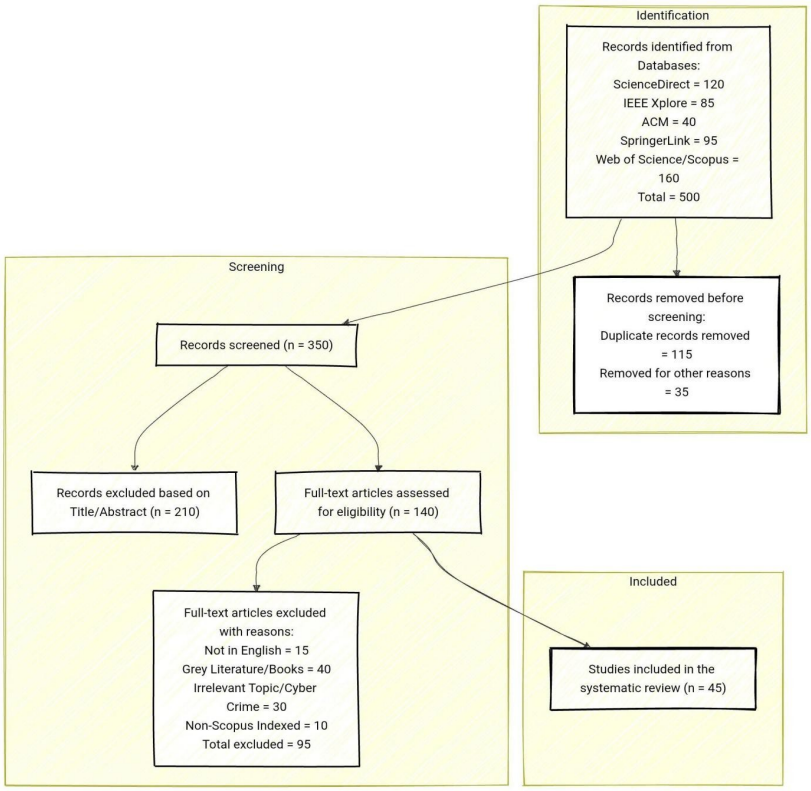

Figure 2: PRISMA flow diagram reporting the data selection and screening process.

2.8 Inclusion and exclusion criteria

To include relevant studies for our systematic review, a variety of inclusion and exclusion criteria were used. These were determined by the following criteria: Inclusion criteria: (i) peer-reviewed journal and conference articles between 2020 and 2025; (ii) articles found from the high-impact academic databases covering aspects related to the logistical supply chain dependencies of armed groups, grassroots intelligence barriers, spatial conflict datasets and proactive threat assessment metrics; and (iii) articles that were immediately related to the formulated research questions concerning asymmetric warfare and rural banditry.

The following articles were excluded: articles that were duplicate articles found in any of the databases; articles published in a language other than English; grey literature articles (books, policy reports, government documents and newsletters); articles that were specialised and did not cover the subject of interest (urban petty crime, cyber-banditry and geopolitical regions); and articles published in journals that were not indexed in Scopus or predatory journals. With this approach, all relevant studies were added to the systematic literature review, and studies which were not applicable were excluded from it.

2.9 Quality Evaluation

This is not just important in terms of the analysis of evidence in the systematic review but also in the evaluation of evidence. Weaker studies may have issues with their research design, which could impact their results and should be carefully considered. Figure 3 shows the results of visualisation analysis of the words that qualified for this study.

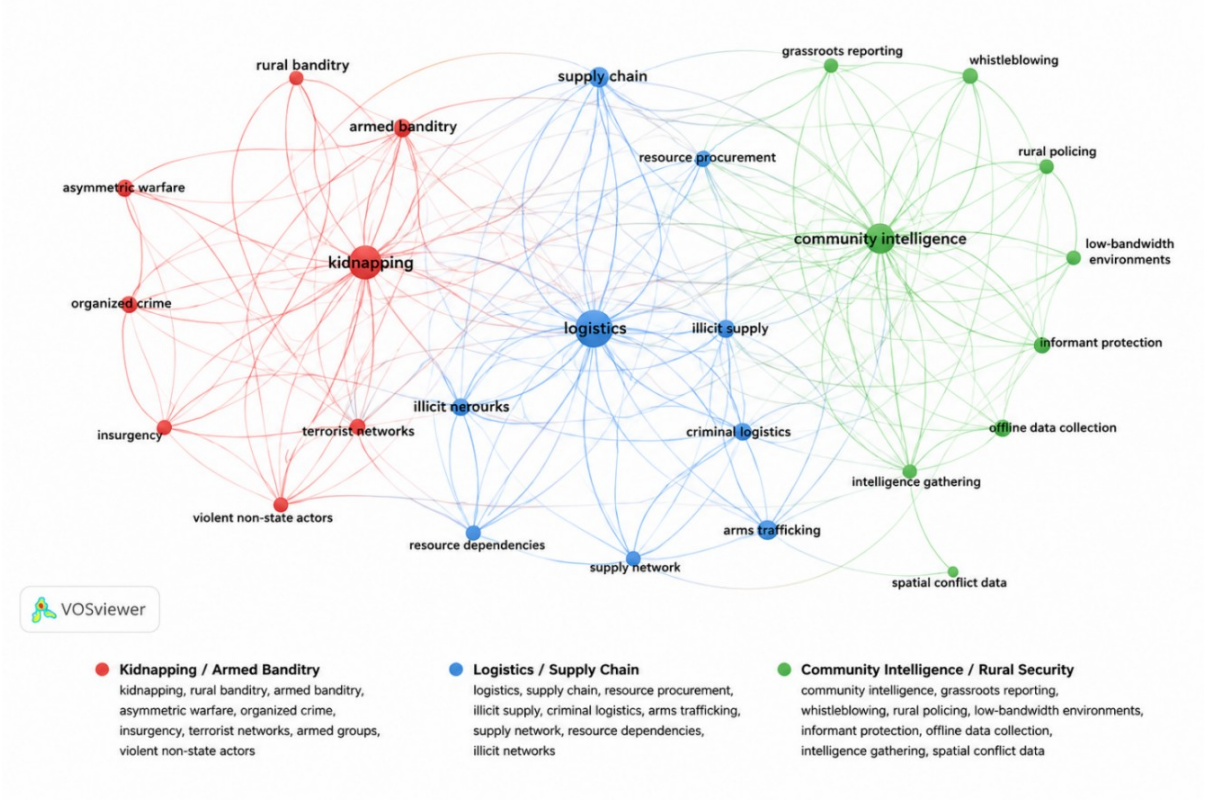

Figure 3: Keyword co-occurrence visualisation analysis of eligible studies using the VOSviewer tool.

In all these studies, the research methods used were analysed, and studies in which the methods were weak, were based on data from just a single point of measurement time or did not consider the suspicious spatial bias or width limit which could affect the validity of the studies' results, were individually identified and critically reviewed. Using appropriate procedures to assess the accuracy of information and potential issues in each investigation is also important. The selected studies were reported; rigour, credibility and relevance were assessed using an article quality assessment checklist and a Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) checklist. A further method used was compulsory confirmation, which involved checking all downloaded articles before gathering data, thus ensuring uniformity and high academic integrity amongst the different sets of data. The quality of the information was evaluated, and forty-five studies relevant to the problem domain of banditry logistics and intelligence barriers were identified. A PRISMA flow diagram (Figure 2) – henceforth referred to as the 'PRISMA flow diagram' – was used to select, filter and include studies for the systematic literature review.

3. DYNAMICS OF ASYMMETRIC WARFARE AND RURAL BANDITRY

In more recent literature, further attempts at interpreting rural banditry in the Northwest Nigeria region in a more recent fashion are in the form of 'asymmetric warfare' that is highly 'terrain adaptive'. As described by Ojo et al. (2023), the type of violence is a series of perpetrators targeting kidnappings and cattle rustling / resource theft. This is in agreement with Bello and Abdullahi (2021), which demonstrated that a deep-rooted farmers and herdsmen conflict is a direct catalyst for organised banditry that adversely affects the farmers' community in the rural zone. These armed groups are decentralised “syndicates”, rather than a single grievance.

They are not just grassroots groups, but they have a relatively strong logistics system which continues to sustain them. One of the economic tools for these gangs to use across the porous border of Niger and Nigeria is cattle herding and arms trading, as suggested by Ojewale (2024). In reaction, state actors have tried to disrupt the market, using logistical means of disruption, which are discussed in the article by Idris et al. (2024) as market warfare. But the shutting down of the rural markets brought about the reverse effect: civilian life was being lost and the bandits' supply line was not being severed. This is evidence that reactive and defensive military and/or economic responses don't thwart agile and asymmetric challenges.

Such studies present plenty of data on the level of violence that has occurred but have an important methodological flaw. The present study is mostly of a retrospective and qualitative nature and does not utilise structured data. All these studies do not provide a mathematical model of the logistical interface between these syndicates; all these studies do not bring objective factors of disruptions of logistical chains between these syndicates. In addition, they ignore requirements for infrastructure in these conflict zones, and there are no ways to obtain secure offline intelligence from the grassroots. Thus, the problem of class recognition and the evaluation criteria are still open problems, and the datasets are difficult to identify.

3.1 Barriers to Community Intelligence and Whistleblowing

The existing approaches called Intelligence-Led Policing (ILP), play down and disregard the significance of the citizen whistleblower, which is the bottom-up approach to getting data from the state. It is therefore logical to make the deduction that contemporary interventions are almost exclusively based on the built-in in-house spatial-temporal intelligence elaboration, following up on the large-scale review conducted by Khalfa and Hardyns (2023) to map the use of ILP evaluations.

Grassroots Informant Networks (GIN) are not a key driver of the evidence base of the ILP and are not necessarily assessed on the evidence of reduction of crime but rather on safety, quantity or protection of bottom-up civilian reporting (Khalfa & Hardyns, 2023). This institutional bias is compounded by a technology-centric, high-bandwidth type of solution with sensors, one that is simply not the right solution for the rural context of a conflict area. To give an example, Farion et al. (2022) introduced an intelligence extraction model for the border service which does not require manual data extraction from a variety of online sources, except for artificial intelligence classification. Similarly, Munir et al. (2022) believe that situational awareness is "dynamic and data-driven, and sensors are placed in the grey-zone warfare throughout. These models allow for simple measurement of the efficiency of the operation, but only those of digital platforms are considered to be capable of constructing intelligence of any kind. Focusing on both approaches does not account for the more typical scenario in offline and resource-limited areas: intelligence co-production with at-risk civilian informants, which are features of offline operations (Farion et al., 2022; Munir et al., 2022).

Concurrently, there are proactively maintained whistleblowing legions, which come with their own limiting factors at the structural level, as these datasets are defined. Despite having full access to what occurs after the incident, with no details of impending criminal acts, Cavallaro et al. (2020) can nevertheless model strategies of disruption using centrality measures. These paradigms imply that the raw community intelligence is 'noise' and not a potential source of intelligence that needs sentinel-like protection, such as a physical or cryptographic metric (Cavallaro et al. 2020 cite this). Together, this literature reveals an important research gap: while there are highly sophisticated and institution-orientated intelligence models, they are totally lacking in terms of conceptualising and addressing the infrastructural and safety constraints to grassroots whistleblowing. This open question sets the stage for tackling the issue of a low bandwidth at which to discuss the risks for systemic harm, most often going unaddressed namely the high risk of retaliation against civilian reporting.

3.2 Infrastructural Deficits in Low-Bandwidth Conflict Zones

Throughout the literature, telecommunication infrastructure has been established to be a systemic constraint that reduces the accessibility to digital reporting systems of actors safely and effectively. Salemink et al. (2017) refer to the rural-urban digital divide as something that is becoming both entrenched and problematic, as it pushes out villages and towns on the fringes of ICTs. The paradox exists among rural areas, as a growing need for them to rely on digital connectivity to replace capacity gaps in state security and public services is accompanied by a lag in the capacity of rural areas to reap benefits from that digital bridging (Salemink et al., 2017). This is a condition that exemplifies a “broadband bias” that is also intrinsic in the design of current digital systems. However, many large-scale data-driven architectures and mobile data architectures tacitly take for granted near-universal smartphone penetration and reliable connectivity and ignore all the issues related to degraded or unreliable telecommunications environments (Capponi et al., 2019).

This is further confirmed by empirical data. Research on digital participation in rural Europe (Stein et al., 2024) and digital village projects in emerging economies (Bai & Yang, 2025) shows that digital literacy and interest will not necessarily lead to meaningful participation and that there are factors beyond this to take into account. Instead, being reliable and getting access to functional devices become the core requirements. The results underlined a continuous lack of implementation where system architectures are used without considering the local constraints, such as infrastructural ones, in the actual context.

In war-torn contexts, these inequalities in the infrastructures are exacerbated and take on greater strategic importance. The development of a gap in intelligence collection between the state and non-state groups in low-bandwidth geographic areas has created a problem. Although citizens and formal institutions have limited access to reliable or strong telecommunications, military actors like ISWAP and bandits in rural areas are becoming more adept at taking advantage of communication asymmetries. Their activity and use of commercially available satellite broadband technology such as Starlink are reported to allow for mobile (and decentralised) command-and-control communications in remote and less well-connected areas. This has created a "significant gap" between state security agencies, which are still dependent on traditional communication infrastructure that is less resilient to the destruction of the communications system, and communities snubbed of access to such systems (Sahara Reporters, 2026). What is created is an enhanced intelligence/security threat where bad guys can thrive in or around infrastructure weaknesses.

The digital exclusion work has been done before and added important insights for understanding digital exclusion in the rural context; however, few of these works have good methodological backing in high-risk and conflict-sensitive areas. Generally, these are frameworks focused on the development of rural ICTs for customisation and on the implementation of urban-centric crowdsensing architectures that are not geared toward or implemented within conflict-affected hinterlands. Rural ICTs development for customisation (Salemink et al., 2017) and urban-orientated crowdsensing architectures (Capponi et al., 2019) are generally not applicable or usable in conflict-affected hinterlands with conflict.

Thus, the literature fails to theorise about the significance of infrastructure in the context of asymmetric warfare, in which connectivity is limited through the lack of development as well as disrupted or unevenly utilised by armed groups. This suggests there is a key missing research element underway – the development of a security-focused framework that is easily adaptable to situations of ongoing broadband shortcomings and malicious use of infrastructure. Solving this problem will involve integrating mini-mapping and reporting systems (like USSD) with degraded-connectivity communications to do threat mapping in low-connectivity space, as well as a rethinking of datasets as well as assessment metrics for law enforcement and security intelligence systems.

Current datasets on conflict and related evaluation indicators have many substantial measurement and structural shortcomings. Today, spatial forecasting and crime prediction are primarily dominated by historical data-based approaches using official police data in urban environments. The dependence on these approaches involves a limited perspective in applying them to more complex situations, such as kidnapping and banditry in situations of asymmetric conflict. As mentioned by Kounadi et al. (2020), most commonly used datasets are based on official reports of incidents that are generally binary and analysed using hotspot-based approaches. Consequently, most of the studies on spatial forecasting are based on these simplified concepts of the occurrence of crime. The effectiveness of the models is typically evaluated by using the standard evaluation metrics like prediction accuracy, Prediction Accuracy Index (PAI) and F1 scores. Yet these metrics tend to focus more on the proper representations of the past through patterns and leave out the more important aspects of the data being incomplete, structural bias and reporting time lag. Where monitoring is not very dense, there is high variability in data quality, sometimes missing or scarce. Moreover, there are more issues with the uniformity of experimental terms and poor reporting of experimental parameters like temperature distribution that all contribute to the lack of reproducibility and generalisability that Kounadi et al. (2020) point out.

This is a narrow metric culture, and it's also further compromised in computer systems applied to crime prediction, commonly referred to as 'machine learning' and 'deep learning' applications. Mandalapu et al. (2023) conducted a systematic review (150) of various evaluation practices and found that most of the evaluation practices are based on accuracy comparisons and use publicly available crime datasets. These datasets are typically considered to be ground truth and receive little attention in terms of any spatial, social or political biases built into the process of creating them. Most of these studies are also large-scale in nature, relying on urban data from well-established reporting systems and generally achieving high accuracy rates > 90% (Mandalapu et al., 2023; Shah et al., 2021). But these performance measures cannot capture issues like under-reporting, deliberate manipulation of data or lack of adequate reporting mechanisms in remote and conflict-torn areas (Shah et al., 2021). Therefore, these evaluation strategies are hard to implement and validate in low-visibility asymmetric conflicts.

From a more conceptual point of view, algorithmic bias and transparency problems are compounded by a strong reliance on large-scale spatial data and clearly defined risk labels in predictive policing (Berk, 2021). Furthermore, with modernity, the usage of digital traces and telecommunications data (Kang & Kang, 2017; Mandalapu et al., 2023) continues to gain traction, making multi-modal integration of data sources, like points of interest, population statistical data, and social media engagement, more possible within deep learning frameworks. These data-rich environments, however, are not common in low-bandwidth and rural environments affected by conflict where infrastructural limitations can cause significant data limitations. The majority of data analysis for evaluations is thus carried out assuming full and stable datasets; these are subject to possible ‘adversarial manipulation' from armed actors and are also impacted by infrastructural instability and data scarcity.

This leaves a huge research divide: lack of evaluation frameworks specifically developed for a conflict-sensitive context. Metrics based on the past, however, are more commonly related to retrospective, accurate measures that are based on well-structured urban datasets and therefore should be rethought. Subsequent assessment measures should include measures of structural bias, infrastructural disruption and missingness, especially in challenging or under-resourced settings where the assumption of predictions is not as valid.

RQ1: How are the logistical supply chain dependencies of kidnapping and banditry syndicates categorised

Anzoom et al. (2021) provide a comprehensive review of illicit supply chain networks and demonstrate that such systems can be understood along two primary dimensions: structural and functional. Structurally, illicit supply chains range from highly centralised configurations to decentralised, modular, and networked forms, with intermediate variations in formalisation, complexity, density, and central coordination. Functionally, they are organised into distinct operational stages, including sourcing, processing, transportation, distribution, and financial laundering.

These stages are often carried out by specialised actors linked through flexible arrangements such as brokerage, logistics coordination, and protection networks. In the context of kidnapping and banditry, these functional stages manifest as interconnected but operationally separated components, including abduction operations, hostage management, ransom negotiation, and proceeds laundering, which may be controlled by different units within the same criminal organisation (Azoom et al., 2021).

Building on this structural-functional distinction, El Baz et al. (2025) further refine the classification of illicit supply chains through an integrated framework that combines fraud-related behavioural dimensions (pressure, opportunity, rationalisation, and capability) with supply chain design characteristics (formalisation, centralisation, complexity, and density). Applied to the case of illegal grain trade in Ukraine, this approach produces a classification of illicit supply chains shaped by geopolitical instability and logistical conditions, resulting in adaptive configurations that may be opportunistic, embedded, or highly networked. Similarly, Idler (2020) examines the logistical organisation of violent non-state actors by mapping two key types of operational spaces: production nodes, where goods or materials are produced or processed, and transit nodes, where movement, coordination, and short-term exchanges occur. This distinction shows that long-term cooperative relationships tend to be concentrated at production sites, while more flexible and temporary interactions occur along trafficking routes. This spatial separation provides a useful framework for understanding the geography of illicit logistics and operational dependency.

Extending this line of analysis, Palma (2015) conceptualises commercial insurgency as a triadic system composed of political, military, and criminal dimensions. Each dimension operates through partially autonomous but interconnected networks. Within this structure, kidnapping and banditry logistics can be interpreted as consisting of political facilitation networks that enable operational space, military or tactical units responsible for execution and control of victims, and criminal-financial networks that manage ransom negotiation and money flows.

RQ2: What datasets are commonly utilised to map asymmetric warfare and criminal logistics

Several conflict and crime datasets that are widely used to map asymmetric warfare, armed non-state actors, and illicit or criminal logistics were identified. These resources underpin much empirical work on conflict patterns, rebel networks, and illicit supply chains. The datasets include ACLED, UCDP GED, GDELT, ICEWS, GTD, NSA, ANARD, Deep South Watch, Yemen Data Project, Micro Focus GPAS data, Colombian armed-actor event data, and various case-specific criminal network datasets.

The following data sets are often employed in mapping asymmetric warfare and criminal logistics:

1. ACLED (Armed Conflict Location & Event Data Project) is a very comprehensive event-based dataset that records organised political violence and protests, with in-depth actor coding, and is widely used as a benchmark to map instability and violence patterns across the globe (Raleigh et al., 2023).
2. UCDP Georeferenced Event Dataset (UCDP GED): Geocoded events of organised violence (state-based conflict, non-state conflict, and one-sided violence) are provided with date, location and linkage ID; the first version is for Africa, 1989–2010 (Sundberg & Melander, 2013).
3. Global Database of Events, Language, and Tone (GDELT) – A global, machine-coded event dataset based on news sources, capturing political events and violence; it is commonly used to compare with researcher-coded projects (Raleigh et al., 2023).
4. ICEWS (Integrated Crisis Early Warning System) – Machine-coded political event data for early warning and network research of insurgents and parties (Raleigh et al., 2023; Jäger, 2018).
5. GTD (Global Terrorism Database) – Event data on terrorism around the world; employed when conflict studies call for information on terrorism incidents (Raleigh et al., 2023).

6. NSA (Non-State Actors in Armed Conflict Dataset) – Actor-level dataset from UCDP containing information about state and rebel dyads to help analyse rebel actors and coalitions (Cunningham et al., 2013).
7. ANARD (Armed Nonstate Actor Rivalry Dataset) – Dyadic dataset of rivalries and militarised disputes among armed non-state actors in MENA, 1993–2018, built from ACLED, NSA and other sources (Powell & Florea, 2021).
8. Regional conflict datasets (for example, Deep South Watch and Yemen Data Project) – Highly resolved, country-specific event data that complement global series and that help reduce under-reporting (Raleigh et al., 2023; Jäger, 2018).
9. Colombian armed-actor event/NLP–GIS dataset – Geo-located events and actors (government, insurgents, paramilitaries, and criminal organisations) 1988–2017 (Osorio et al., 2019).
10. Data from Micro Focus Global Product Authentication Service (GPAS) – Spatio-temporal QR code authentication data to reconstruct legal and illegal supply chains and deduce illegal logistics flows (González Ordiano et al., 2020).
11. Case-based drug/illicit supply network datasets – Court records, police intelligence and surveillance-based networks documenting drug/illicit supply networks that are compared across multiple cases (Bichler et al., 2017; Anzoom et al., 2022; González Ordiano et al., 2020).
12. Together, these data sources make it possible to map insurgent violence, competition between non-state actors, terrorist activities, and illicit trade logistics in both space and time, and even often in ways that connect activities such as the location of events, actor features, and network structures.

RQ3: What are the evaluation metrics for the calculation of the performance of proactive threat detection and intelligence gathering?

It presents the primary metrics to evaluate the performance of proactive detection and cyber threat intelligence (CTI) systems in threat identification and classification. These metrics are mostly based on a confusion matrix of True Positives (TP), False Positives (FP), True Negatives (TN), and False Negatives (FN) (Alazab et al., 2024; Islam et al., 2024; Noman et al., 2022; Panigrahi et al., 2024). Table 2 shows the confusion matrix structure for threat detection evaluation.

Table 2: Confusion matrix structure for threat detection

	ACTUAL THREAT (Positive)	ACTUAL NORMAL (Negative)
PREDICTED THREAT	True Positive (TP): threat correctly detected	False Positive (FP): benign event flagged as threat
PREDICTED NORMAL	False Negative (FN): missed threat	True Negative (TN): normal correctly ignored

Table 3 shows common evaluation metrics in proactive detection/cyber threat intelligence.

Table 3: Common Evaluation Metrics in Proactive Detection / CTI

Metric	Typical Formula (from TP, FP, TN, FN)	Interpretation in proactive threat detection
Accuracy	(TP + TN) / (TP + TN + FP + FN)	Overall proportion of correctly classified events (threat + normal) (Alazab et al., 2024; Noman et al., 2022; Panigrahi et al., 2024)
Precision	TP / (TP + FP)	How many predicted threats are truly threats; important to control false alarms in hunting and CTI triage (Noor et al., 2025; Bai et al., 2024; Kilichev & Kim, 2023; Shaikhanova et al., 2025; Alazab et al., 2024; Ali et al., 2025; Islam et al., 2024; Fathima et al., 2023; Noman et al., 2022; Cue et al., 2025)
Recall / Detection Rate / TPR / Sensitivity	TP / (TP + FN)	Fraction of actual threats detected; critical for not missing attacks in proactive systems (Noor et al., 2025; Bai et al., 2024; Kilichev & Kim, 2023; Shaikhanova et al., 2025; Alazab et al., 2024; Ali et al., 2025; Islam et al., 2024; Fathima et al., 2023; Noman et al., 2022; Cue et al., 2025; Jayarin et al., 2024)
F1-score	2·Precision·Recall / (Precision + Recall)	Harmonic mean of precision and recall; widely used summary metric under class imbalance (Noor et al., 2025; Kilichev & Kim, 2023; Shaikhanova et al., 2025; Alazab et al., 2024; Ali et al., 2025; Islam et al., 2024; Fathima et al., 2023; Noman et al., 2022; Panigrahi et al., 2024; Cue et al., 2025; Jayarin et al., 2024)
False Positive Rate (FPR)	FP / (FP + TN)	Rate at which benign events are misclassified as threats; key for practical deployability (Alazab et al., 2024; Islam et al., 2024; Fathima et al., 2023; Panigrahi et al., 2024; Shen et al., 2024)
True Negative Rate (TNR / Specificity)	TN / (FP + TN) = 1 – FPR	Share of benign traffic correctly recognised as normal (Alazab et al., 2024)
False Negative Rate (FNR / Miss Rate)	FN / (TP + FN) = 1 – Recall	Proportion of threats missed; especially critical in proactive/early detection (Alazab et al., 2024; Fathima et al., 2023)
Error Rate	(FP + FN) / (TP + TN + FP + FN)	Overall misclassification rate (Alazab et al., 2024)
ROC curve & AUC	Plot TPR vs FPR; AUC ∈ [0,1]	Threshold-independent view of trade-off between detecting threats and raising false alarms (Alazab et al., 2024; López-Vizcaíno et al., 2024; Fathima et al., 2023

Metric	Typical Formula (from TP, FP, TN, FN)	Interpretation in proactive threat detection
Precision–Recall curve & PR-AUC	Precision vs Recall	More informative under heavy class imbalance typical in threat hunting (López-Vizcaíno et al., 2024; Fathima et al., 2023; Panigrahi et al., 2024)
Latency / Time to Detect	Detection time − attack start	Measures how early a system detects attacks; crucial for *proactive* detection (Alazab et al., 2024; Ali et al., 2025)
Time-aware F-score (TaF)	F1 penalised by detection delay	Jointly evaluates correctness and earliness of detection in streaming/early warning settings (Ali et al., 2025)
Weighted / Macro Averages	example., macro-F1 (mean per-class F1)	Capture performance across multiple attack types, including rare but critical threats (Alazab et al., 2024; Alkharabsheh et al., 2025; López-Vizcaíno et al., 2024; Fathima et al., 2023; Panigrahi et al., 2024; Jayarin et al., 2024)
Other CTI/assessment metrics	example., kappa, logistic loss, RMSD, risk scores	Used for multi-criteria SIEM/CTI evaluation beyond pure detection quality (Alkharabsheh et al., 2025; Bochner et al., 2023)

These metrics enable the assessment of proactive threat detection and intelligence systems by correctness, robustness in the face of imbalance, and timeliness, all of which are critical for cyber defence in the real world.

RQ4: How effective is intelligence-led policing in comparison to traditional, reactive, military responses?

Intelligence-led policing (ILP) is intended to address the shortcomings of traditional reactive policing and crime control strategies such as militarised responses by identifying and targeting resources in a proactive and efficient manner (Ratcliffe, 2025; Blair & Weintraub, 2023; Motsa, 2022). There are essentially only experimental and quasi-experimental examples, with the majority related to crime reduction and resource efficiency, and one large field experiment focusing on a reactive military-style deployment (Khalfa & Hardyns, 2023; Crous, 2010; Blair & Weintraub, 2023).

3.3 Overall Performance Comparison for Intelligence-led / proactive policing

Thirty-eight (quasi-)experimental ILP-style interventions are subject to a scoping review; most interventions demonstrate benefits in crime reduction when based on spatio-temporal intelligence to target hotspots or high-risk offenders (Khalfa & Hardyns, 2023). The use of ILP is linked to better use of resources, targeting high-harm offenders and issues, and decreased need for catch-all patrols (Ratcliffe, 2025; Blair & Weintraub, 2023; Motsa, 2022). There is a strong relationship between acceptance of ILP and the perception of policing effectiveness in Abu Dhabi Police (Alblooshi & Kassim, 2022). Contrary to the traditional reactive approach, case studies (e.g., the UK, the USA, and Serbia) present ILP as a means of achieving better outcomes with fewer resources (e.g., Ratcliffe 2025; Motsa, 2022; Berleze & Belinelli 2025).

Reactive military-style responses

- No credible drop in crime or an increase in the perceived safety of those residing in the crime hot spots, and possibly a rise in crime following the deployment, occurs during the deployment period in a large randomised trial of military policing in crime hot spots in Cali, Colombia (Blair & Weintraub, 2023).
- Human rights trends reveal rising incidents of violations, primarily from the police, indicating substantial legitimacy and rights trade-offs and few crime-control benefits (Blair & Weintraub, 2023).

Common Evaluation Metrics

Table 4 shows the evaluation metrics used in comparing ILP with military policing.

Table 4: Outcome metrics used to compare ILP and military policing

Outcome / Metric	Intelligence-led / Proactive Policing	Reactive Military Response
Crime level / counts	Often reduced in ILP-style hotspot and targeted interventions	No clear reduction; possible post-intervention rise
Crime disruption / harm concentration	Recommended as explicit ILP metric but rarely measured so far	Not explicitly measured
Perceptions of safety / fear of crime	Rarely evaluated; suggested future metric	No improvement; some evidence of deterioration
Human rights / abuses	Not central in ILP trials; flagged as necessary secondary metric	Evidence of increased abuses in surveys

Table 5 shows the evaluation performance metrics for ILP vs reactive models

Table 5: Process and Organisational Metrics performance metrics for ILP vs reactive models

Metric / Dimension	Intelligence-Led Policing	Traditional Reactive / Military Style
Resource efficiency	Prioritisation based on intelligence; better targeting	Saturation, high visible presence, low targeting
Use of data / analysis	Central (3i model: interpret–influence–impact)	Limited, often ad hoc
Officer/organisation effectiveness	ILP acceptance positively associated with perceived effectiveness	Not evaluated as such
Performance framework	Proposed multi-component ILP performance models (process + impact)	Traditional focus on recorded/resolved crimes

RQ5: What are the open issues that could arise in acquiring grassroots intelligence in a low-bandwidth, high-risk rural conflict zone environment?

This section focuses on some of the main constraints and difficulties in the gathering of grassroots intelligence in low-bandwidth, high-risk, rural, conflict situations.

Structural, Contextual Constraints

Fear and obstacles to access: Regular information collection is hampered by armed violence, continuing conflicts and threats faced by researchers, officials and informants that limit physical access to many areas (Rosenberg, 2024; Ayalew & Lema, 2025). The displacement and fragmentation of community structures further undermines the existing structures of local communities and the ability to rely on trustworthy sources (Osazuwa & Ugwukwu, 2025; Ayalew & Lema, 2025).

Poor and inadequate infrastructure and connectivity: Limited reporting upstream and downstream and the inability to get information in real time from the field are due to poor or damaged infrastructure, sparse communication networks and the absence of phones or data connectivity (Ayalew & Lema, 2025; Rosenberg, 2024). However, low-bandwidth modes also limit the use of advanced ISR or satellite tools, and thus coverage gaps exist (Ewuola, 2024; Kagai et al., 2024).

Community-Level and Human Factors: Communities are often hesitant to share information or give a full account of armed attacks by insurgents or state security forces due to mistrust and fears of reprisals (Osazuwa & Ugwukwu, 2025). Respondents in conflict settings often fear retribution against them, and it's a constant obstacle to honest reporting (Rosenberg, 2024).

Poor reading skills, language and cultural barriers: Lack of financing, old technology and lack of training affect HUMINT capacity, particularly in remote and risky rural areas (Osazuwa & Ugwukwu, 2025). Community-based intelligence frameworks can be marginalised by over-relying on centralised or militarised responses (Osazuwa & Ugwukwu, 2025).

Handling data quality, bias and validity concerns: Census data is often incomplete; the population is not stationary in conflict zones; and sampling is often ad hoc, resulting in population samples that are non-representative and have sampling bias (Rosenberg, 2024; Ayalew & Lema, 2025). Both the internal and external validity of grassroots intelligence are undermined by respondents' self-censorship or giving biased accounts (Rosenberg, 2024).

The major categories of challenges in collecting grassroots intelligence and descriptions are stated in Table 6

Table 6: Summary Table: Major Challenge Categories

Challenge Category	Brief Description
Insecurity & access	Physical danger, blocked areas, displacement
Connectivity limits	Sparse networks, low bandwidth, tool constraints
Trust & fear	Mistrust of authorities, fear of reprisals
Socio-cultural barriers	Illiteracy, language, hostility to research
Institutional gaps	Under-resourced HUMINT, bureaucratic hurdles
Data validity issues	Biased / incomplete samples and reporting

4. CONCLUSION

The purpose of this systematic literature review (SLR) is to investigate the problematic class of kidnapping and banditry captured in asymmetric warfare, the data that has been used and the measures of assessment suggested. The following are the key conclusions of the studies summarised:

1. The SLR shows how logistical support for kidnapping and banditry syndicates can be broken down into interrelated problem classes, including human intelligence networks, transportation and mobility chains, weapons procurement, supply procurement, safe havens and camps, financial flows and communication/coordination infrastructures.
2. Evidence shows that a mix of qualitative conflict reports, georeferenced incident databases, mobile phone/call detail records, satellite imagery, and open-source intelligence (OSINT) are the most commonly used datasets to map these supply chain dependencies.
3. The review shows that the success indicators for intelligence-led intervention are largely quantified by a variety of indicators that include the following, but are not limited to: Kinetic success measures, incident reduction rates, entities disrupted traversal, spatial–temporal clustering indices, network centrality measures, and proxy indicators of community safety and accessibility.
4. Due to the effect of intelligence-driven and logistics-based activities on decreasing the operational capability of kidnapping and banditry groups, the SLR suggests that these strategies are more effective than force-driven activities and reactive operations in the reduction of incidents, especially through the implementation of multi-source knowledge and community-based reporting.

Overall, the findings suggest a broad proposal that the materials and equipment exchanged under the auspices of kidnapping and banditry can be modelled as an adaptable supply chain that lacks a few elements, elements that can be detected and classified using organised data and evaluation concepts. Persistent data sparsity and underreporting, however, continue to be significant problems, and the difficulties of data flight and armed actors' reactions are still a very real concern. The primary objective of this SLR was to raise awareness for the design of asymmetric operations disruption strategies that rely on sensitive evidence (SE) and the need for a common set of data and metrics for future research on asymmetric criminal-insurgent.

REFERENCES

Al-Dhaqm, A., Ikuesan, R., Kebande, V., Razak, S., & Ghabban, F. (2021). Research Challenges and Opportunities in Drone Forensics Models. Electronics. https://doi.org/10.3390/electronics10131519

Alazab, M., Khurma, R., García-Arenas, M., Jatana, V., Baydoun, A., & Damaševičius, R. (2024). Enhanced threat intelligence framework for advanced cybersecurity resilience. Egyptian Informatics Journal. https://doi.org/10.1016/j.eij.2024.100521

Alblooshi, M., & Kassim, E. (2022). Intelligence-Led Policing Acceptance and Policing Effectiveness: The Roles of Organizational Change, Innovative Behavior and Knowledge Sharing. International Academic Symposium of Social Science 2022. https://doi.org/10.3390/proceedings2022082057

Ali, S., Razzaque, A., Yousaf, M., & Ali, S. (2025). A Novel AI-Based Integrated Cybersecurity Risk Assessment Framework and Resilience of National Critical Infrastructure. IEEE Access, 13, 12427–12446. https://doi.org/10.1109/access.2024.3524884

Alkharabsheh, A., Alhosani, F., Alameri, M., Alrashdi, A., Almenhali, F., & Alzaabi, A. (2025). AI-Driven Proactive Framework for Cybersecurity Threat Prediction, Detection, and Attack Classification. 2025 International Conference on Computer Science, Technology and Engineering (ICCSTE), 12–17. https://doi.org/10.1109/iccste65902.2025.11138235

Avtar, R., Kouser, A., Kumar, A., Singh, D., Misra, P., Gupta, A., Yunus, A., Kumar, P., Johnson, B., Dasgupta, R., Sahu, N., & Rimba, A. (2021). Remote Sensing for International Peace and Security: Its Role and Implications. Remote. Sens., 13, 439. https://doi.org/10.3390/rs13030439

Ayalew, N., & Lema, A. (2025). Conflict Risk Monitoring for Conflict Prevention in Ethiopia: The Case of Ataye Towen, North Shewa, Amhara Region. International Journal of Disaster Risk Management. https://doi.org/10.18485/ijdrm.2025.7.1.10

Bai, Y., Sun, M., Zhang, L., Wang, Y., Liu, S., Liu, Y., Tan, J., Yang, Y., & Lv, C. (2024). Enhancing Network Attack Detection Accuracy through the Integration of Large Language Models and Synchronized Attention Mechanism. Applied Sciences. https://doi.org/10.3390/app14093829

Berleze, JB., & Belinelli, AF. (2025). Qualified Operations Based on Military Police Intelligence: Advanced Strategies for the Preservation of Public Order and the Challenges of Contemporary Public Security. LUMEN ET VIRTUS, 16 (49), 6886-6909. https://doi.org/10.56238/levv16n49-052

Blair, R., & Weintraub, M. (2023). Little evidence that military policing reduces crime or improves human security. Nature Human Behaviour, 1–13. https://doi.org/10.1038/s41562-023-01600-1

Bochner, A., Makumbi, I., Aderinola, O., Abayneh, A., Jetoh, R., Yemanaberhan, R., Danjuma, J., Lazaro, F., Mahmoud, H., Yeabah, T., Nakiire, L., Yahaya, A., Teixeira, R., Lamorde, M., Nabukenya, I., Oladejo, J., Adetifa, I., Oliveira, W., Mcclelland, A., & Lee, C. (2023). Implementation of the 7-1-7 target for detection, notification, and response to public health threats in five countries: A retrospective, observational study. The Lancet. Global Health, 11, e871–e879. https://doi.org/10.1016/S2214-109X(23)00133-X

Crous, C. (2010). Conceptualising a performance framework for intelligence led policing. Australasian Policing: A Journal of Professional Practice and Research, *2*(1), 35–41.

Cue, H., Bourlai, T., & Lupo, M. (2025). Proactive Cyber Resilience: A Unified Assessment Methodology for Incident Forecasting With Cyber Threat Intelligence Integration. IEEE Access, 13, 139460–139478. https://doi.org/10.1109/access.2025.3596252

Ewuola, A. (2024). Developing Intelligence-Led Security Protocols for Multinational Pipeline Operations in Fragile Environments. International Journal of Multidisciplinary Research and Growth Evaluation. https://doi.org/10.54660/.ijmrge.2024.5.2.1086-1097

Fathima, A., Khan, A., Uddin, M., Waris, M., Ahmad, S., Sanín, C., & Szczerbicki, E. (2023). Performance Evaluation and Comparative Analysis of Machine Learning Models on the UNSW-NB15 Dataset: A Contemporary Approach to Cyber Threat Detection. Cybernetics and Systems, 56, 1160–1176. https://doi.org/10.1080/01969722.2023.2296246

Garcia, A., Britton, M., Doshi, D., Choudhury, M., & Dantec, C. (2021). Data Migrations. Proceedings of the ACM on Human-Computer Interaction, 4, 1–25. https://doi.org/10.1145/3434177

Guo, Y., Liu, F., Song, J., & Wang, S. (2024). Supply chain resilience: A review from the inventory management perspective. Fundamental Research, 5, 450–463. https://doi.org/10.1016/j.fmre.2024.08.002

Gundhus, H., Skjevrak, P., & Wathne, C. (2022). We Will Always Be Better Than a Spreadsheet. European Journal of Policing Studies. https://doi.org/10.5553/ejps/2034760x2022001009

Islam, M., Nasiruddin, M., Karmakar, M., Akter, R., Khan, M., Sayeed, A., & Amin, A. (2024). Leveraging Advanced Machine Learning Algorithms for Enhanced Cyberattack Detection on U.S. Business Networks. Journal of Business and Management Studies. https://doi.org/10.32996/jbms.2024.6.5.23

Jabbour, C., Sobreiro, V., De Sousa Jabbour, A., Campos, L., Mariano, E., & Renwick, D. (2019). An analysis of the literature on humanitarian logistics and supply chain management: paving the way for future studies. Annals of Operations Research, 1–19. https://doi.org/10.1007/s10479-017-2536-x

Jayarin, P., David, D., , J., Kumari, V., & Pillai, N. (2024). Enhancing Cybersecurity in the Digital Age with Machine Learning for Threat Detection and Prevention. 2024 International Conference on Recent Advances in Science and Engineering Technology (ICRASET), 1–5. https://doi.org/10.1109/ICRASET63057.2024.10895208

Kagai, F., Branch, P., But, J., Allen, R., & Rice, M. (2024). Rapidly Deployable Satellite-Based Emergency Communications Infrastructure. IEEE Access, 12, 139368–139410. https://doi.org/10.1109/access.2024.3465512

Khalfa, R., & Hardyns, W. (2023). 'Led by Intelligence': A Scoping Review on the Experimental Evaluation of Intelligence-Led Policing. Evaluation Review, 48, 797–847. https://doi.org/10.1177/0193841X231204588

Kilichev, D., & Kim, W. (2023). Hyperparameter Optimization for 1D-CNN-Based Network Intrusion Detection Using GA and PSO. Mathematics. https://doi.org/10.3390/math11173724

Lee, Y., Bradford, B., & Pósch, K. (2024). The Effectiveness of Big Data-Driven Predictive Policing: Systematic Review. Justice Evaluation Journal, 7, 127–160. https://doi.org/10.1080/24751979.2024.2371781

López-Vizcaíno, M., Nóvoa, F., Fernández, D., & Cacheda, F. (2024). Time Aware F-Score for Cybersecurity Early Detection Evaluation. Applied Sciences. https://doi.org/10.3390/app14020574

Mhanna, S., Halloran, L., Zwahlen, F., Asaad, A., & Brunner, P. (2023). Using machine learning and remote sensing to track land use/land cover changes due to armed conflict. The Science of the Total Environment, 165600. https://doi.org/10.1016/j.scitotenv.2023.165600

Motsa, V. (2022). Theoretical and methodological bases for the use of criminal analysis by operative units of law enforcement agencies in Ukraine. Uzhhorod National University Herald. Series: Law. https://doi.org/10.24144/2307-3322.2022.73.53

Noman, I., Bortty, J., Bishnu, K., Aziz, M., & Islam, M. (2022). Data-Driven Security: Improving Autonomous Systems through Data Analytics and Cybersecurity. Journal of Computer Science and Technology Studies. https://doi.org/10.32996/jcsts.2022.4.2.22

Noor, K., Imoize, A., Li, C., & Weng, C. (2025). A Review of Machine Learning and Transfer Learning Strategies for Intrusion Detection Systems in 5G and Beyond. Mathematics. https://doi.org/10.3390/math13071088

Ojo, J. (2020). Governing "Ungoverned Spaces" in the Foliage of Conspiracy: Toward (Re)ordering Terrorism, from Boko Haram Insurgency, Fulani Militancy to Banditry in Northern Nigeria. African Security, 13, 77–110. https://doi.org/10.1080/19392206.2020.1731109

Ojo, J., Oyewole, S., & Aina, F. (2023). Forces of Terror: Armed Banditry and Insecurity in North-west Nigeria. Democracy and Security, 19, 319–346. https://doi.org/10.1080/17419166.2023.2164924

Osazuwa, C., & Ugwukwu, V. (2025). Beyond the battlefield: the role of human intelligence (HUMINT) in addressing the socio-economic drivers of Boko haram in northeastern Nigeria. The American Journal of Political Science Law and Criminology. https://doi.org/10.37547/tajpslc/volume07issue05-09

Panigrahi, G., Sethy, P., Behera, S., Gupta, M., Alenizi, F., Suanpang, P., & Nanthaamornphong, A. (2024). Analytical Validation and Integration of CIC-Bell-DNS-EXF-2021 Dataset on Security Information and Event Management. IEEE Access, 12, 83043–83056. https://doi.org/10.1109/access.2024.3409413

Ratcliffe, J. (2005). The Effectiveness of Police Intelligence Management: A New Zealand Case Study. Police Practice and Research, 6, 435–451. https://doi.org/10.1080/15614260500433038

Ratcliffe, J. (2025). Intelligence-Led Policing (3rd ed.). Routledge. https://doi.org/10.1007/978-1-4614-5690-2_270

Rosenberg, W. (2024). Processes and Challenges Associated with Conducting Survey Research in Conflict Zones. Survey Practice. https://doi.org/10.29115/sp-2023-0032

Saminu, I., binYaacob, C., & Shukri, S. (2023). Bandits' Struggle for Survival and its Humanitarian Impacts in Zamfara State, Nigeria. Cogent Social Sciences, 9. https://doi.org/10.1080/23311886.2023.2241714

Sahara Reporters. (2026, May 12). https://saharareporters.com/2026/05/12/nigerian-military-intercepts-over-400-starlink-devces-linked-boko-haram-iswap-north

Shaikhanova, A., Kuznetsov, O., Tokkuliyeva, A., Ayapbergenov, K., Olzhas, S., & Danir, T. (2025). Security Audit of IoT Device Networks: A Reproducible Machine Learning Framework for Threat Detection and Performance Benchmarking. Sensors (Basel, Switzerland), 25. https://doi.org/10.3390/s25247519

Shen, X., Li, Z., Burleigh, G., Wang, L., & Chen, Y. (2024). Decoding the MITRE Engenuity ATT&CK Enterprise Evaluation: An Analysis of EDR Performance in Real-World Environments. Proceedings of the 19th ACM Asia Conference on Computer and Communications Security. https://doi.org/10.1145/3634737.3645012

Sticher, V., Wegner, J., & Pfeifle, B. (2023). Toward the remote monitoring of armed conflicts. PNAS Nexus, 2. https://doi.org/10.1093/pnasnexus/pgad181

Walther, O. J., Radil, S. M., Russell, D. G., & Trémolières, M. (2023). Introducing the Spatial Conflict Dynamics Indicator of Political Violence. Terrorism and Political Violence, 35(3), 533–552. https://doi.org/10.1080/09546553.2021.1957846

Xu, W., Lu, Y., & Proverbs, D. (2024). An evaluation of factors influencing the vulnerability of emergency logistics supply chains. International Journal of Logistics Research and Applications, 27(10), 1891–1924. https://doi.org/10.1080/13675567.2023.2209030