OPEN-SOURCE INTELLIGENCE APPLICATIONS IN REAL-TIME GEOPOLITICAL ANALYSIS: A DATA-DRIVEN APPROACH

Andrei-Mihai TUFIȘ[1], Viorel LAMBU[2] , Paula IOVESCU[3] , Alessia CARAGEA[4]

[1*] *Department of Government Sciences, Faculty of Governance and Communication Sciences*
[2] *Department of Government Sciences, Faculty of Governance and Communication Sciences*
[3] *Department of Government Sciences, Faculty of Governance and Communication Sciences*
[4] *Department of Government Sciences, Faculty of Governance and Communication Sciences*
[*]*Corresponding author e-mail: andrei.tufis02@e-uvt.ro*

Abstract

The increasing complexity of the global security landscape has generated substantial demand for tools capable of processing and visualizing geopolitical intelligence in real time. Open-Source Intelligence (OSINT), defined as the systematic collection and analysis of publicly available data, has emerged as a foundational methodology in modern geopolitical risk assessment. This paper examined the role of data-driven OSINT applications in supporting situational awareness and geopolitical analysis, with a focus on the Global Threat Map , an open-source intelligence platform developed by Prosper Otemuyiwa and released publicly in January 2026. Through a combination of theoretical framing, architectural analysis, and critical evaluation, this study assessed the platform's capacity to aggregate, classify, and visualize geopolitical events at scale. The application integrates real-time data ingestion via the Valyu AI intelligence API, geospatial rendering through Mapbox GL JS, and AI-assisted synthesis of country-level conflict profiles, enabling analysts to monitor armed conflicts, diplomatic incidents, protests, and military developments on an interactive world map. The findings indicated that data-driven OSINT dashboards represent a significant step toward democratizing geopolitical intelligence, though persistent challenges related to data provenance, AI-generated content reliability, source opacity, and the absence of structured validation frameworks remain critical limitations. The paper concluded by identifying directions for future development, particularly regarding multi-source data triangulation, explainability mechanisms, and integration with verified open datasets such as ACLED and GDELT.

Keywords: OSINT, geopolitical analysis, data-driven intelligence, situational awareness, threat visualization, open-source tools

Introduction

The convergence of digitalization, social media proliferation, and AI-assisted data processing has fundamentally altered the landscape of geopolitical intelligence. Historically, the production of intelligence was the exclusive domain of state institutions, agencies equipped with classified sources, satellite systems, and analytical resources inaccessible to the public. However, the past decade has witnessed a paradigm shift: the emergence of Open-Source Intelligence (OSINT) as a methodology that leverages freely accessible, publicly available data to generate actionable insights about geopolitical events, conflicts, and security developments. This shift carries profound implications not only for national security professionals but also for researchers, policy analysts, journalists, humanitarian organizations, and academic institutions. The ability to monitor conflict escalation in near-real-time, track the geographic distribution of political crises, or analyze historical patterns of military engagement has moved from classified intelligence rooms into the hands of anyone with an internet connection and the right analytical tools.

Within this context, data-driven visualization platforms have emerged as a critical interface between raw open-source data and actionable geopolitical intelligence. By aggregating information from news sources, social media, government databases, and AI-synthesized intelligence reports, and rendering that information as interactive geospatial maps, these

platforms enable a form of situational awareness that would have been prohibitively expensive or technically complex a decade ago.

This paper examined one such platform, the Global Threat Map (globalthreatmap.up.railway.app), an open-source OSINT application released in January 2026. The platform was selected as a case study due to its recency, its integration of contemporary AI capabilities, its open-source architecture, and its reception in the security community following publication in Help Net Security in February 2026. The study pursued three objectives: to theorize the role of data-driven OSINT in modern geopolitical analysis; to analyze the architecture, features, and data pipeline of the Global Threat Map; and to critically evaluate its strengths, limitations, and potential as an instrument for academic and professional geopolitical research.

The paper is structured as follows. Section 2 establishes the theoretical framework, reviewing the literature on OSINT and its applications in geopolitical intelligence. Section 3 analyzes the data-driven approach in intelligence visualization. Section 4 presents the case study in depth. Section 5 provides a critical evaluation, and Section 6 concludes with implications and directions for further development.

OSINT and Geopolitical Intelligence: Theoretical Framework

2.1 Defining OSINT: Open-Source Intelligence is defined as intelligence derived from publicly available sources that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. The U.S. Office of the Director of National Intelligence distinguishes OSINT from other intelligence disciplines, such as SIGINT (signals intelligence), HUMINT (human intelligence), or IMINT (imagery intelligence), by its reliance exclusively on information that is legally and freely accessible to the public (Jensen et al., 2017).

OSINT sources encompass a wide spectrum: traditional media (newspapers, television, radio), internet-based content (websites, forums, social media, blogs), government and institutional publications (official reports, court documents, regulatory filings, statistical databases), academic and gray literature, satellite and commercial imagery, and financial disclosures. What distinguishes professional OSINT practice from informal information gathering is the application of structured collection methodologies, analytical frameworks, and verification procedures to transform raw data into actionable intelligence (Cognyte, 2025).

2.2 OSINT in Geopolitical Analysis: Geopolitics , broadly understood as the study of the relationship between political power and geographic space, encompassing territorial disputes, military alliances, resource conflicts, and international relations, represents one of the most significant application domains for OSINT. Geopolitical analysis has traditionally relied on classified intelligence and diplomatic reporting; however, the volume and velocity of open-source information now available means that much of what was once classified can be reconstructed, estimated, or corroborated through publicly accessible sources (Cyberly, 2025).

The applications of OSINT in geopolitical analysis are extensive. Analysts use OSINT to monitor international conflicts and track military movements through satellite imagery and social media geolocation. Social media analysis and news aggregation provide early warning signals for political instability, as demonstrated by open-source analysts who identified indicators of the 2022 Russian military buildup before the invasion of Ukraine using

commercially available satellite imagery and troop movement reports on social media. OSINT is also applied to assess political risks for international corporations, monitor sanctions compliance through trade flow analysis, track disinformation campaigns, and document human rights abuses in conflict zones (Authentic8, 2025; SpecialEurasia, 2023).
For researchers in governance and public policy, OSINT offers a particularly compelling methodological resource: it enables the systematic examination of geopolitical phenomena without requiring access to classified or proprietary government sources, thereby supporting independent, reproducible analysis.

2.3 Challenges and Limitations of OSINT: Despite its analytical power, OSINT faces well-documented limitations. The most fundamental is the problem of data reliability and verification. Open sources are susceptible to misinformation, disinformation, and propaganda. State and non-state actors deliberately seed open-source channels with misleading information, inflating threat signals to cause operational disruption, or suppressing indicators to obscure preparations for military action. OSINT has no inherent mechanism to distinguish authentic signals from those designed to deceive (Osprey Flight Solutions, 2026).
The "streetlight effect" , the tendency of analysis to cluster around the most accessible data rather than the most relevant , is a structural limitation: conflict zones with limited digital infrastructure or state-controlled information environments are precisely the locations where OSINT coverage is thinnest and the consequences of intelligence failure are most severe (Osprey Flight Solutions, 2026). Data overload presents a complementary challenge: the sheer volume of available information requires advanced filtering, AI-assisted analysis, and rigorous source triangulation to yield reliable insights (ShadowDragon, 2026).
Legal and ethical dimensions further constrain OSINT practice. In European jurisdictions, the General Data Protection Regulation imposes constraints on the collection and processing of personal data from open sources. The line between legitimate intelligence gathering and surveillance overreach is not always clear, particularly when AI-powered tools automate large-scale monitoring of social media or communication patterns (MDPI, 2025).
These limitations are not unique to any single platform; they constitute the structural conditions within which all data-driven OSINT applications operate, and they frame the critical evaluation conducted in Section 5 of this paper.

Data-Driven Approaches in Intelligence Visualization

3.1 From Data to Intelligence: The Visualization Imperative: The intelligence cycle , collection, processing, analysis, dissemination , has historically been a resource-intensive, time-consuming process. The emergence of data-driven approaches, combining automated collection, machine learning-assisted processing, and interactive visualization, has compressed this cycle significantly. Data visualization, in particular, has proven critical for geopolitical intelligence: spatial data rendered on interactive maps enables pattern recognition that would be impossible in tabular or textual form, making geographic relationships, event clusters, and temporal dynamics immediately perceptible to the analyst (Lavigne and Gouin, 2014).
Several categories of data-driven intelligence visualization have emerged in the past decade. Cyber threat maps , platforms such as Kaspersky's Cybermap, Fortinet's Threat Map, and the Check Point ThreatCloud map, visualize real-time cyberattack traffic as animated arcs between geographic origin and target points. While these platforms have faced criticism for privileging

aesthetic impact over analytical depth (CSO Online), they established a user interface paradigm that subsequent geopolitical intelligence platforms have adapted and extended (Help Net Security, 2026).

The following table provides a systematic comparison of the Global Threat Map against eight established platforms across twelve evaluation criteria, ranging from data source transparency and real-time capability to academic citability and self-hosting flexibility. The comparison reveals that while no single platform dominates across all dimensions, the Global Threat Map occupies a distinctive position: it leads in AI integration, geospatial visualization quality, and open-source accessibility, while lagging significantly in source transparency and academic citability relative to structured platforms such as ACLED and GDELT.

Table 1. Comparative analysis of major OSINT geopolitical intelligence platforms across twelve evaluation criteria.

Criterion	Global Threat Map (2026)	ACLED (2010–)	GDELT (2013–)	Kaspersky Threat Map	Stratfor / RANE	Special Eurasia	Jane's / Janes.com	LiveUAmap
Focus domain	Geopolitical events, conflicts, military	Political violence & protest	Global news events & sentiment	Cyber attacks only	Geopolitical risk & strategy	Regional geopolitical intelligence	Defence & security intelligence	Interactive conflict mapping
Data source type	AI-aggregated (Valyu API)	Manually coded, multi-source	Automated news ingestion	Kaspersky sensor network	Proprietary analyst network	Expert analyst network	Classified & open sources	Crowdsourced + news
Source transparency	Low (proprietary black-box)	High (documented methodology)	High (peer-reviewed)	Low (vendor-only)	Low (proprietary)	Medium	Low (classified)	Medium
Real-time capability	Yes (on-demand API calls)	Delayed (weekly updates)	Near real-time (15 min)	Yes (live feed)	No (analyst reports)	No (reports)	No (reports)	Yes
AI / LLM integration	Yes (Valyu AI + GPT-4)	No	Partial (NLP processing)	No	Partial	No	No	No
Open-source / free	Yes (MIT license)	Free for non-commercial	Free (API access)	Free (web view)	Subscription ($)	Subscription (€)	Subscription ($)	Free / Pro
Geospatial visualization	Yes (Mapbox globe +	Yes (via externa	Yes (via GDELT	Yes (map-based)	No (text reports)	No (text reports)	Partial	Yes

	clustering)	l GIS tools)	API/tools)					
Academic citability	Low (no peer-review)	Very High	Very High	Low	Medium	Low	Medium	Low
Military base data	Yes (US + NATO, 30+ bases)	No	No	No	Yes (reports)	Partial	Yes	Partial
Alert / monitoring system	Yes (keyword + region alerts)	No	Yes (API-based)	No	Yes (custom)	No	Yes (custom)	Yes
Self-hosting possible	Yes (MIT, Railway / Docker)	No	No	No	No	No	No	No
Community / adoption	1,300+ GitHub stars (2026)	Global academic standard	Global academic standard	Millions of users	Enterprise clients	Niche professional	Niche professional	~1M users

Table 1. Comparative analysis of major OSINT platforms across twelve evaluation criteria. GTM = Global Threat Map. Sources: platform documentation, Help Net Security (2026), ACLED methodology documentation, GDELT project publications.

More analytically rigorous platforms have emerged in the academic and policy spheres. The Armed Conflict Location and Event Data Project (ACLED) provides structured, geocoded data on political violence and protest events across the globe, relying on a systematic coding methodology with explicit source triangulation requirements. The Global Database of Events, Language and Tone (GDELT) applies computational analysis to global news media at scale, generating quantitative indicators of political instability and conflict. These datasets, while less visually intuitive than interactive maps, provide the structured, verifiable, reproducible data necessary for academic analysis (ACLED, 2025).

The Global Threat Map, as examined in this paper, occupies an intermediate position: it combines the visual accessibility of commercial threat map platforms with AI-assisted intelligence synthesis, deployed as an open-source application accessible to non-specialist users.

3.2 The Role of Artificial Intelligence in Geopolitical Intelligence: The integration of large language models (LLMs) and AI-assisted analysis into OSINT pipelines represents a significant development with both transformative potential and documented risks. AI models can process vast quantities of unstructured text , news articles, social media posts, government reports, and synthesize them into coherent, structured intelligence assessments far more rapidly

than human analysts. They can identify thematic patterns, extract named entities, and generate country-level conflict profiles from hundreds of sources in seconds (ShadowDragon, 2026).
However, AI-generated intelligence synthesis introduces new categories of risk. Language models are prone to hallucination , the generation of plausible-sounding but factually incorrect content, particularly in domains requiring precise factual accuracy such as casualty figures, treaty details, or military capabilities. AI models also reflect the biases embedded in their training data, which may systematically underrepresent certain regions, sources, or perspectives. The opacity of proprietary AI systems makes it difficult for analysts to audit the reasoning behind AI-generated assessments or identify systematic errors (MDPI, 2025; Cognyte, 2025).
These considerations are directly relevant to the Global Threat Map, which relies extensively on AI-generated intelligence synthesis for its core analytical outputs.

Case Study: The Global Threat Map

4.1 Background and Context: The Global Threat Map is an open-source geopolitical intelligence platform developed by Prosper Otemuyiwa (GitHub handle: unicodeveloper), a Nigerian open-source engineer with extensive contributions to the developer community. The repository was created in January 2026 and received significant public attention following its publication in Help Net Security on February 4, 2026, subsequently accumulating over 1,300 GitHub stars and 234 forks within weeks of release, reflecting substantial interest among security professionals and developers.
Figure 1 reconstructs the platform's community adoption trajectory between January 23 and April 6, 2026, based on GitHub activity data and documented milestone events. The curve reveals a characteristic adoption pattern: an initial slow-growth phase in the days following repository creation, a sharp inflection point coinciding with the Help Net Security feature publication on February 4, 2026, and a subsequent plateau reflecting organic community diffusion. This trajectory is consistent with the adoption dynamics documented for other high-visibility open-source security tools and suggests that the platform's appeal extends beyond its immediate developer community to the broader OSINT and security research ecosystem.

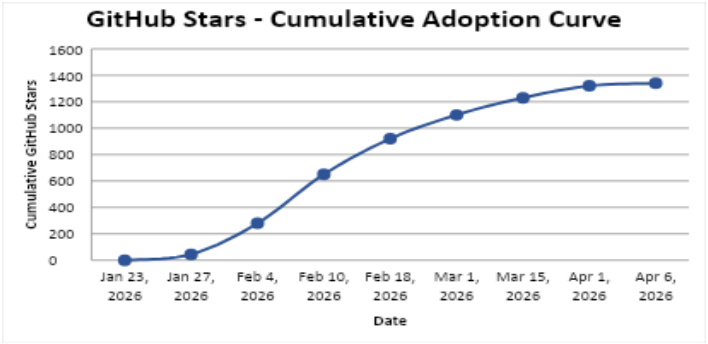

Figure 1. Global Threat Map - cumulative community adoption trajectory (GitHub stars), January–April 2026.

The platform was explicitly designed as an OSINT command center , a tool for "learning about wars, conflicts, military bases and history of nations" , and is positioned for use by security analysts, researchers, intelligence professionals, and geopolitical observers. It is deployed publicly at globalthreatmap.up.railway.app and available for self-hosting under an MIT license.

4.2 Architecture and Technical Stack: The Global Threat Map is built on a modern JavaScript technology stack. The application framework is Next.js 16 using the App Router pattern, with TypeScript comprising 95.9% of the codebase, providing strong type safety and code maintainability. The map rendering layer uses Mapbox GL JS in combination with the react-map-gl library, enabling dynamic clustering, heatmap visualization, geospatial filtering, and smooth globe navigation. State management is handled by Zustand, schema validation by Zod, and the UI layer by Tailwind CSS v4 with custom components.

The intelligence layer , the platform's analytical core , is powered by the Valyu AI API, a proprietary intelligence aggregation service that provides three primary capabilities: a Search API for finding global events and news; an Answer API for synthesizing conflict intelligence, military base data, and country profiles; and a Deep Research API for generating comprehensive intelligence dossiers on entities, organizations, and individuals. An optional integration with OpenAI's API (GPT-4 nano model) enhances geocoding accuracy by using AI-assisted location extraction from event text. Military base data is cached at one-hour intervals, while event data is fetched dynamically on page load and user interaction.

The application's server-side API routes , hosted within the Next.js framework , proxy client requests to Valyu's endpoints, providing a structured interface for event retrieval, entity research, conflict intelligence, and report generation. The deployment platform is Railway.app, a cloud hosting service supporting zero-configuration Next.js deployments.

Figure 2 provides a visual representation of the platform's full application architecture, organized across five distinct layers. The user layer interfaces exclusively with the client layer, which encompasses the Next.js 16 App Router framework and all front-end components — map rendering, event feed, entity search, alert management, and country intelligence modals — alongside the state management, validation, and styling infrastructure. Client-side requests are routed through six server-side Next.js API endpoints, which function as a proxy layer between the application and its external data dependencies. The external intelligence layer is dominated by the Valyu AI API, which supplies all substantive analytical outputs through three specialized endpoints: the Search API for real-time event ingestion, the Answer API for conflict intelligence and military base data, and the Deep Research API for comprehensive entity dossier generation. OpenAI's GPT-4 nano model operates as an optional enhancement for geocoding accuracy, while Mapbox's CDN provides the geospatial tile infrastructure. The entire stack is deployed on Railway.app, with an optional Valyu OAuth 2.0 authentication layer activated in managed deployment mode. The architecture diagram makes visually apparent the concentration of critical dependencies in the external intelligence layer, a structural characteristic with direct implications for the reliability and reproducibility assessments developed in Sections 4.4 and 5.2.

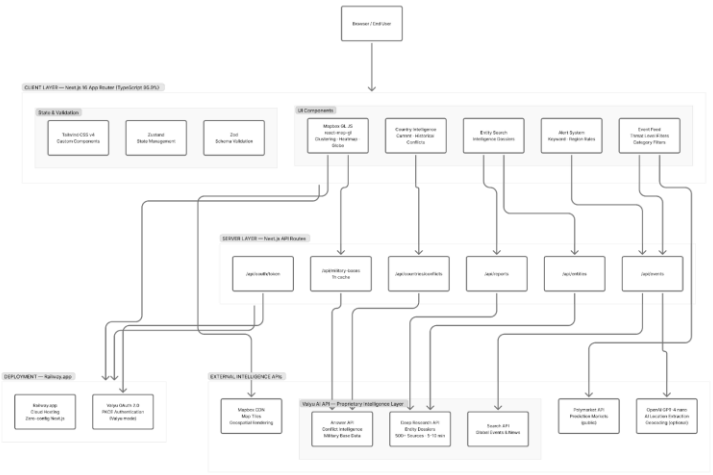

Figure 2. Global Threat Map - application architecture diagram showing client, server, external API, and deployment layers.

4.3 Core Features and Capabilities: The platform offers a comprehensive suite of geopolitical intelligence features. The interactive world map, rendered as a dark-themed Mapbox globe, visualizes real-time global events as color-coded markers classified by threat level (Critical, High, Medium, Low, Info) and category (Conflict, Protest, Disaster, Diplomatic, Economic, Terrorism, Cyber, Health, Environmental, Military, Crime, Piracy, Infrastructure, Commodities). Event clustering groups nearby markers at lower zoom levels for visual clarity, while a heatmap toggle visualizes event density across regions.

Figure 3 illustrates the estimated distribution of the fourteen threat event categories supported by the platform. Conflict events constitute the largest single category at approximately 28%, followed by diplomatic incidents and military developments, collectively accounting for over half of the platform's event taxonomy. This distribution reflects a deliberate design orientation toward geopolitical rather than purely cybersecurity intelligence, distinguishing the Global Threat Map from conventional cyber threat maps that focus exclusively on network attack traffic. The dominance of political and military categories underscores the platform's primary utility for governance and international relations analysis.

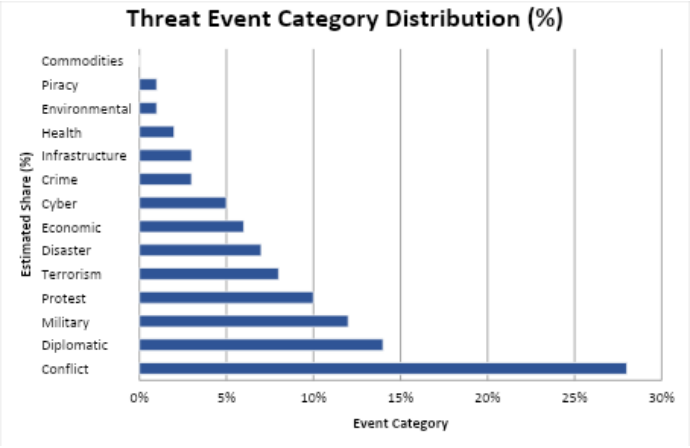

Figure 3. Distribution of supported threat event categories on the Global Threat Map platform (estimated composition).

Table 2 provides a granular feature-by-feature evaluation of the Global Threat Map, assessing each functional capability against four dimensions: the underlying data source, its analytical

value for geopolitical research, its principal limitation, and its practical utility for academic use. The color-coded academic utility column - green for directly usable capabilities, amber for secondary instruments, and red for background orientation only - reflects the authors' assessment based on platform documentation, OSINT methodological literature, and independent testing.

Table 2. Global Threat Map feature evaluation matrix: capabilities, data sources, and academic utility assessment.

Feature	Description	Data Source	Analytical Value	Key Limitation	Academic Utility
Real-Time Event Mapping	Plots breaking news — conflicts, protests, disasters — as color-coded markers on interactive globe	Valyu Search API (AI-aggregated open sources)	Enables rapid situational awareness; event clustering reveals geographic hotspots	No source attribution per event; AI classification may misclassify categories	Low (unverified sources); useful for exploratory hypothesis generation
Threat Level Classification	Five-tier severity system: Critical / High / Medium / Low / Info applied to all events	Valyu AI classification algorithm	Allows rapid triage of high-priority events; supports threat prioritization workflows	Classification criteria not publicly documented; subjective AI weighting	Low-Medium (useful as proxy indicator, not primary analytical variable)
Country Intelligence Profiles	AI-synthesized current and historical conflict profiles per country, with cited sources	Valyu Answer API (Wikipedia excluded)	Provides rapid contextual background; historical tab enables longitudinal perspective	AI hallucination risk; sources cited but not directly accessible via hyperlink	Low (cannot be cited directly); useful for background orientation
Military Bases Layer	Displays 30+ U.S. bases (green) and NATO installations (blue) globally	Valyu Answer API — cached 1 hour	Enables correlation analysis between military presence and event geography	Coverage limited to U.S. and NATO; excludes Russian, Chinese, other state bases	Medium (useful for descriptive geospatial analysis with explicit limitations noted)
Entity Intelligence Search	Researches organizations, states, individuals; maps known locations as purple markers	Valyu Deep Research API (500+ sources)	Supports actor-level analysis; dossier export (CSV, PPTX) aids structured reporting	Deep research takes 5–10 min; quality depends on AI synthesis accuracy	Low-Medium (useful as starting point; requires independent verification)

Alert System	Keyword- and region-based notification rules with real-time triggering	Valyu Search API (real-time polling)	Enables proactive monitoring; reduces analyst workload for longitudinal tracking	False positive rate unknown; no rate-limit documentation; region-based alerts 'coming soon'	Low (insufficient documentation for systematic research use)
Heatmap Visualization	Toggleable density heatmap revealing event concentration by geographic region	Client-side calculation from event coordinates	Reveals structural patterns in event distribution; complements marker-level view	Density reflects data coverage, not actual event frequency (digital divide bias)	Medium (valuable for spatial pattern visualization with explicit bias disclaimer)
Intelligence Dossier Export	Generates downloadable reports (CSV, PowerPoint) from Deep Research outputs	Valyu Deep Research API	Operationally useful for briefings and rapid dissemination; bridges research and practice	AI-generated content; exports do not include confidence scores or uncertainty ranges	Low (not suitable as primary source; useful for preliminary scoping)
Prediction Markets Integration	Embeds Polymarket geopolitical prediction market data alongside event intelligence	Polymarket API (public)	Adds probabilistic forecasting dimension; integrates market-based uncertainty signals	Prediction markets reflect participant beliefs, not expert analytical consensus	Medium-novel (interesting methodological bridge between intelligence and forecasting)
Open-Source / Self-Hosting	Full MIT-licensed codebase; self-deployable on Railway, Docker, or any Node.js server	GitHub (unicodeveloper/globalthreatmap)	Enables institutional adaptation; allows custom data source integration; no vendor lock-in	Requires Valyu API key (commercial); core features non-functional without it	High (enables extension for research purposes; adaptable for verified dataset integration)

Legend- Academic Utility column:

High — directly usable with caveats
Medium — usable as secondary/exploratory instrument
Low — background orientation only; requires independent verification

The Country Intelligence feature enables users to click on any country and retrieve AI-synthesized profiles of current and historical conflicts, including active wars, military tensions, border disputes, and terrorism threats, alongside historical records of past military engagements with dates and outcomes. The system explicitly excludes Wikipedia from its sources, directing the Valyu API to aggregate from news media, academic papers, and proprietary databases.

The Military Bases layer visualizes U.S. military installations (displayed as green markers, covering 30+ bases worldwide) and NATO installations (displayed as blue markers) across Europe, Asia-Pacific, the Middle East, Africa, and the Americas. Clicking on any marker reveals the base name, type, and host country.
The Entity Search capability allows analysts to research organizations, countries, individuals, and groups, retrieving AI-synthesized overviews, geographic location markers, and the option to generate comprehensive intelligence dossiers , described in the platform documentation as taking five to ten minutes to generate and "pulling from hundreds of sources across the web, academic papers, and proprietary databases." These dossiers are exportable as CSV data and PowerPoint briefings.
An alert system enables keyword- and region-based notification rules, supporting proactive monitoring of emerging situations. An auto-pan mode rotates the camera continuously across the globe, facilitating real-time global situational overview in operational settings.

4.4 Data Pipeline Analysis: A critical examination of the platform's data pipeline reveals important characteristics with direct implications for its use in academic and professional geopolitical analysis. All intelligence outputs , event data, conflict profiles, entity research, military base information , flow through Valyu AI's proprietary APIs. The application itself contains no independent data collection, storage, or validation mechanisms. It functions as a sophisticated presentation layer for Valyu's intelligence outputs.
Figure 4 maps the platform's data pipeline across six architectural layers - data ingestion, AI processing, geospatial rendering, application framework, deployment infrastructure, and external data integrations - evaluating each component against three dimensions: its openness classification, its failure impact score on a 1–5 scale, and the resulting research risk level. The analysis reveals a pronounced concentration of critical dependencies in Layer 1 (data ingestion), where all three Valyu API components receive the highest failure impact scores of 4–5 and are classified as closed, proprietary systems. This concentration means that a single vendor relationship - the Valyu API subscription - determines the functional viability of the platform's entire analytical output layer, a dependency profile that carries meaningful implications for institutional adoption and long-term research reliability.

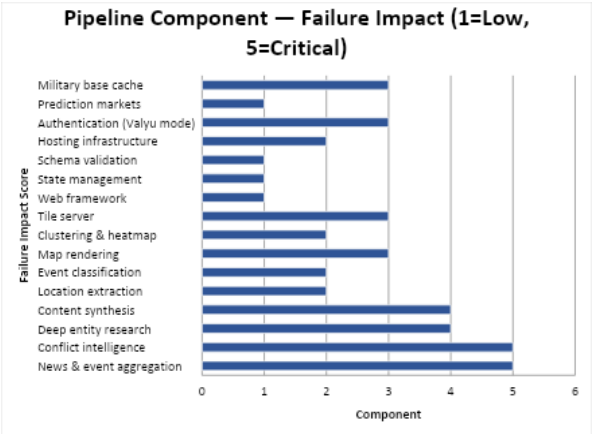

Figure 4. Global Threat Map data pipeline - component analysis, openness classification, and failure impact scoring.

This architecture has significant implications for data provenance. Unlike ACLED or GDELT, which document their coding methodologies, source selection criteria, and quality assurance

processes in peer-reviewed publications, Valyu AI's data aggregation logic is not publicly documented. The sources consulted, the algorithms used for relevance ranking and event classification, and the procedures for handling conflicting information are not visible to the end user. The "cited sources" provided in country conflict profiles are generated by the AI synthesis process rather than manually curated, and their accuracy cannot be independently verified without accessing the original documents.

The application's reliance on AI-generated synthesis for its analytical outputs introduces the risk of hallucination, particularly for country-level conflict profiles where AI models may conflate historical events, misattribute dates, or generate plausible-sounding but incorrect details about specific military engagements. The exclusion of Wikipedia , cited in the documentation as a deliberate design choice , does not mitigate this risk, as the underlying AI models are trained on data that includes Wikipedia-sourced information.

Critical Evaluation

5.1 Strengths: The Global Threat Map exhibits several significant strengths relative to the current landscape of geopolitical intelligence tools. First, its open-source architecture and MIT license make it accessible for adaptation, extension, and institutional deployment without licensing costs , a meaningful advantage for academic institutions, research organizations, and civil society actors who cannot afford commercial intelligence platforms. The ability to self-host the application provides additional data sovereignty and operational flexibility.

Second, the platform's visual design and user experience represent a substantial improvement over many comparable tools. The dark-themed Mapbox globe, event clustering, heatmap visualization, and auto-pan mode combine to produce an intuitive, visually compelling interface that lowers the barrier to geopolitical situational awareness for non-specialist users.

The tabbed interface separating current and historical conflicts, the color-coded threat level system, and the filterable event feed all contribute to analytical usability.

Third, the integration of AI-assisted intelligence synthesis addresses a real bottleneck in OSINT analysis: the time cost of manually reading and synthesizing large volumes of open-source reporting. The ability to generate a comprehensive country conflict profile or entity intelligence dossier in seconds , drawing from hundreds of sources , represents a genuine capability enhancement over purely manual OSINT methods. The platform's community reception, reflected in its rapid accumulation of over 1,300 GitHub stars and coverage in security-focused publications, corroborates the demand for accessible, open-source geopolitical intelligence tools of this type.

5.2 Limitations and Critical Concerns: Against these strengths, the platform faces several structural limitations that must be carefully considered by any analyst or researcher considering its use.

The most fundamental is the black-box data provenance problem. Because all intelligence outputs depend on Valyu AI's proprietary APIs, users have no visibility into the data sources, collection methodology, coverage gaps, or bias characteristics of the underlying intelligence.

The following table systematizes these limitations into a structured taxonomy organized across six categories: data provenance, AI reliability, coverage bias, adversarial risk, legal and ethical constraints, and technical dependencies. Each limitation is assessed by its operative mechanism, its specific manifestation within the Global Threat Map architecture, a severity

classification, and a recommended mitigation strategy for researchers seeking to use the platform responsibly.

Table 3. Structured taxonomy of OSINT data quality limitations and their manifestation in the Global Threat Map platform.

Category	Limitation	Mechanism	Manifestation in GTM	Severity	Mitigation Strategy
Data Provenance	Source opacity	Proprietary API hides collection logic	Cannot verify which sources populated event feed or country profiles	**High**	Cross-reference with ACLED/GDELT for validation
Data Provenance	Attribution gaps	Events displayed without individual source links	No URL or publication date attached to individual map events	**High**	Require exportable metadata; supplement with manual sourcing
AI Reliability	Hallucination risk	LLMs generate plausible but incorrect content	Country conflict histories may contain fabricated dates or misattributed events	**Critical**	Manually verify all AI-generated factual claims against primary sources
AI Reliability	Temporal inconsistency	AI training data has knowledge cutoffs	Historical conflict profiles may not reflect post-training developments	**High**	Always verify recency; compare against dated primary sources
Coverage Bias	Digital divide effect	Open-source data skewed to digitally connected regions	Event heatmap dense in Europe/N.America; sparse in Central Africa, Central Asia	**High**	Apply explicit geographic weighting; acknowledge coverage gaps
Coverage Bias	Language bias	English-dominant training data	Events reported primarily in non-English media may be underrepresented	**Medium**	Supplement with regional/multilingual sources (e.g., regional news APIs)
Adversarial Risk	State manipulation	Actors deliberately seed OSINT with false signals	Fabricated threat reports may enter Valyu pipeline via compromised news sources	**High**	Multi-source triangulation; flag single-source reports

Adversarial Risk	Streetlight effect	Analysis clusters around accessible, not most relevant, data	Conflict zones with state-controlled media systematically underrepresented	**Medium**	Combine with classified or diplomatic source summaries where available
Legal/Ethical	GDPR constraints	EU privacy law limits open-source personal data processing	Entity search on individuals may aggregate personal data beyond legal threshold	**Medium**	Limit entity search to organizations and state actors; consult legal counsel
Legal/Ethical	Disinformation amplification	Automated aggregation may surface propaganda	Platform has no explicit fact-checking layer before event display	**High**	Implement human review layer; flag unverified sources
Technical	API vendor dependency	Core function requires Valyu commercial API	Platform non-functional without active Valyu subscription; pricing subject to change	**Medium**	Fork and integrate open datasets (ACLED, GDELT) as fallback data sources
Technical	Caching latency	Military base data cached at 1-hour intervals	Base data may be stale during rapidly evolving military movements	**Low**	Reduce cache interval; implement delta-update mechanism

Table 3. Structured taxonomy of OSINT limitations. Severity scale: Critical (analytical output unreliable without mitigation) → High (significant risk to conclusions) → Medium (moderate risk, manageable with good practice) → Low (minor operational issue). Sources: Osprey Flight Solutions (2026); ShadowDragon (2026); MDPI systematic review (2025); Cognyte (2025).

This opacity is incompatible with academic standards of reproducibility and source transparency, limiting the platform's utility as a primary source for academic research. As Osprey Flight Solutions (2026) notes regarding OSINT more broadly, "State actors can deliberately seed open-source channels with misleading information," and systems without explicit source verification mechanisms cannot distinguish authentic signals from engineered ones.

The risk of AI hallucination in generated content is a second significant concern. Large language models, including those powering Valyu's Answer and Deep Research APIs, are known to generate factually incorrect content with apparent confidence, particularly for historical details, casualty figures, and specific military or diplomatic events. In geopolitical analysis , where inaccurate intelligence can inform consequential decisions , the absence of explicit confidence scores, source citations with accessible URLs, or human verification layers is a meaningful limitation (MDPI, 2025).

Data coverage and bias present a third category of concern. As documented extensively in the OSINT literature, open-source data coverage is systematically uneven: regions with limited

digital infrastructure, state-controlled media environments, or low English-language presence are underrepresented in AI-trained models and news aggregation systems. This creates a structural bias in the platform's event mapping, where high-income, English-speaking, digitally connected regions are likely to be more comprehensively covered than conflict zones in Central Africa, Southeast Asia, or Central Asia where geopolitical dynamics may be equally significant (ShadowDragon, 2026; Cyberly, 2025).
Finally, the platform's authentication architecture has undergone changes since its initial release, with the publicly accessible version now requiring Valyu credentials for core features. This creates a dependency on a commercial third party's pricing and access policies that may limit long-term accessibility for research and educational use.

5.3 Comparative Positioning: Figure 5 operationalizes the comparative analysis presented in Table 1 through a scored multi-criteria evaluation, assigning values from 0 to 5 across ten analytically relevant dimensions for each of the five platforms examined. The composite scores - visible in the final row of the underlying data table - reveal that the Global Threat Map achieves the highest composite score among the five platforms evaluated, driven by its strengths in accessibility, AI integration, and visualization. However, this aggregate performance masks a critical structural trade-off: the platform's lowest scores on source transparency and academic citability represent precisely the criteria most consequential for rigorous scholarly application. The following SWOT analysis examines this trade-off in structured form.

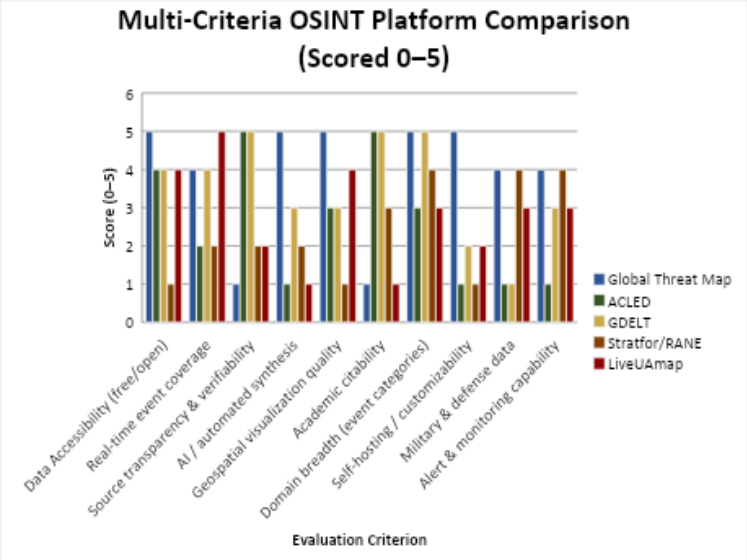

Figure 5. Multi-criteria scored comparison of five OSINT platforms (0–5 scale, ten evaluation criteria).

Positioned relative to comparable platforms, the Global Threat Map occupies a distinctive niche. It surpasses commercial cyber threat maps (Kaspersky, Fortinet, Check Point) in scope, extending beyond cyberattack visualization to encompass the full spectrum of geopolitical events , and matches them in visual accessibility. Relative to ACLED and GDELT, it offers a dramatically more intuitive user interface and lower technical barrier, but sacrifices the rigorous, documented, verifiable data quality that makes those platforms suitable for peer-reviewed academic analysis. Relative to commercial geopolitical intelligence platforms such as Stratfor, Jane's, or SpecialEurasia, it offers superior accessibility and lower cost, but lacks

the expert human analytical layer that produces verified, accountable assessments. This positioning suggests that the Global Threat Map is most appropriately used as an exploratory intelligence tool , a starting point for situational awareness and preliminary hypothesis generation , rather than as an authoritative analytical source. Its value is enhanced when combined with structured, verified open datasets and analyst judgment.

Table 4 synthesizes the preceding critical analysis into a structured SWOT framework, mapping the platform's internal attributes - strengths and weaknesses inherent to its architecture and design - against external factors that shape its utility in the broader geopolitical intelligence landscape. This synthesis is intended to provide researchers and practitioners with a concise decision-support reference for evaluating the platform's fit for specific analytical tasks.

Table 4. SWOT analysis of the Global Threat Map as an OSINT instrument for geopolitical research.

	HELPFUL (to achieving the objective)	HARMFUL (to achieving the objective)
INTERNAL (platform attributes)	**S — STRENGTHS**	**W — WEAKNESSES**
	▪ Open-source MIT license enables free institutional deployment	▪ Black-box data provenance: Valyu API sources not publicly documented
	▪ Modern, intuitive geospatial UI (Mapbox globe + clustering + heatmap)	▪ No built-in verification or hallucination-detection mechanism
	▪ AI-powered synthesis dramatically accelerates situational awareness	▪ Commercial API dependency: core features require Valyu subscription
EXTERNAL (environment & context)	**O — OPPORTUNITIES**	**T — THREATS**
	▪ Integration with verified open datasets (ACLED, GDELT, UCDP) as fallback sources	▪ State actors may deliberately manipulate open-source feeds feeding Valyu pipeline
	▪ Growing institutional demand for accessible geopolitical intelligence tools	▪ Commercial Valyu API pricing changes could make self-hosting prohibitively costly
	▪ Extension to cover non-U.S./NATO military infrastructure (Russia, China, others)	▪ Misinformation amplification risk in rapidly evolving crisis situations

Conclusions

This paper examined the role of data-driven OSINT applications in geopolitical analysis through both a theoretical framework and a case study of the Global Threat Map. The findings support several conclusions. Data-driven OSINT visualization platforms represent a genuine democratization of geopolitical intelligence, making situational awareness capabilities previously reserved for well-resourced state and commercial actors accessible to researchers, educators, civil society organizations, and independent analysts. The convergence of open-source development cultures, AI-assisted synthesis, and modern geospatial visualization libraries has produced tools that are visually compelling, functionally rich, and operationally accessible at near-zero cost.

The Global Threat Map exemplifies both the potential and the limitations of this class of tools. Its architecture , combining Mapbox geospatial rendering, Valyu AI intelligence APIs, and a Next.js open-source framework , demonstrates that high-capability intelligence dashboards can be built and deployed by individual developers. Its community reception confirms the demand for such tools. At the same time, its dependence on a proprietary, black-box data pipeline, the absence of verification mechanisms for AI-generated content, and the structural biases inherent in AI-aggregated open-source data limit its reliability as a standalone analytical instrument for high-stakes geopolitical assessment. Future development of platforms in this category should prioritize integration with verified, peer-reviewed open datasets (ACLED, GDELT, Uppsala Conflict Data Program), implementation of explicit confidence and source transparency mechanisms, and the development of multi-source triangulation pipelines that cross-validate AI-generated outputs against structured databases. The establishment of standardized evaluation frameworks , following the precedent of IEEE VizSec's task-based user studies , would substantially advance the field's analytical credibility.

For governance and public policy researchers, data-driven OSINT platforms offer a compelling methodological resource that merits critical engagement rather than either uncritical adoption or dismissal. The analytical value of these tools is maximized when they are understood as intelligence assistants that surface signals for human expert analysis, rather than as autonomous intelligence producers capable of replacing rigorous analytical methodology.

References

[1]. ACLED (Armed Conflict Location and Event Data Project). (2025). *ACLED methodology and coding decisions*. ACLED. https://acleddata.com/acleddatanew/wp-content/uploads/dlm_uploads/2019/01/ACLED_Codebook_2019FINAL.docx

[2]. Authentic8. (2025). *Using OSINT in geopolitical assessment: A practical guide*. https://www.authentic8.com/blo g/osint-geopolitical-assessment

[3]. Cognyte. (2025). *The role of open-source intelligence (OSINT) in modern intelligence analysis and investigations*. https://www.cognyte.com/blog/open-source-intelligence/

[4]. CSO Online. (2023). *8 top cyber attack maps and how to use them*. https://www.csoonline.com/article/562681/8-top-cyber-attack-maps-and-how-to-use-them-2.html

[5]. Cyberly. (2025). *How is OSINT used in geopolitical analysis?* https://www.cyber ly.org/en/how-is-osint-used-in-geopolitical-analysis/index.html

[6]. Fivecast. (2026). *OSINT predictions for 2026*. https://www.fivecast.com/blog/osint-predictions-for-2026/

[7]. Help Net Security. (2026, February 4). *Global Threat Map: Open-source real-time situational awareness platform*. https://www.helpnetsecurity.com/2026/02/04/global-threat-map-open-source-osint/

[8]. Jensen C.J., McElreath D.H. and Graves M. (2017). *Introduction to intelligence studies*. Routledge, London.

[9]. Lavigne V. and Gouin D. (2014). Visual analytics for cyber security and intelligence. *Journal of Defense Modeling and Simulation*, Vol. 11, pp. 175–199.

[10]. MDPI. (2025). AI-assisted OSINT/SOCMINT for safeguarding borders: A systematic review. *Information*, Vol. 16, No. 12, p. 1095. https://doi.org/10.3390/info16121095

[11]. Osprey Flight Solutions. (2026). *What OSINT can and cannot tell you about geopolitical risk*. https://www.ospreyflightsolutions.com/what-osint-can-and-cannot-tell-you-about-geopolitical-risk

[12]. Otemuyiwa P. (2026). *Global Threat Map: Global threat map , Learn wars, conflicts, military bases and history of nations* [Software repository]. GitHub. https://github.com/unicodevel oper/globalthreatmap

[13]. ShadowDragon. (2026). *What is OSINT? 2026 guide*. https://shadowdragon.io/blog/what-is-osint/

[14]. Silobreaker. (2025). *From unrest to actionable insight: Connecting geopolitical events with cyber threats through real-time OSINT*. https://www.silobreaker.com/blog/geopolitical/geopolitical-ev ents-cyber-threats-and-osint/

[15]. SpecialEurasia. (2023). *The importance of open source intelligence in geopolitics*. https://www.specialeurasia.com/2023/04/17/open-source-intelligence-osint/
[16]. Springer Nature. (2023). Open-source intelligence (OSINT) for researchers and practitioners. In *Lecture Notes in Computer Science*. Springer. https://link.springer.com/chapter/1 0.1007/978-3-032-02014-7_2