The Intelligent Evolution of Open-Source Intelligence: Focusing on International Legion of Defence Intelligence of Ukraine

Wei Meng *

Posted Date: 6 October 2025

doi: 10.20944/preprints202510.0414.v1

Keywords: artificial intelligence; OSINT; risk assessment; strategic forecasting

 doi:10.20944/preprints202510.0414.v1

Article

The Intelligent Evolution of Open-Source Intelligence: Focusing on International Legion of Defence Intelligence of Ukraine

Wei Meng [1,2,3,4]

[1] Dhurakij Pundit University, Thailand; weimeng4@acm.org
[2] The University of Western Australia, AU
[3] Association for Computing Machinery, USA
[4] Fellow, Royal Anthropological Institute, UK

Abstract

This study aims to deepen open-source intelligence (OSINT) analysis of Ukraine's Defense Intelligence International Corps through artificial intelligence methods, exploring AI's application potential and methodological value in complex warfare information environments. The core objectives address two questions: First, how can AI technologies be effectively integrated into the OSINT cycle to enhance information screening, pattern recognition, and risk prediction? Second, can AI-driven OSINT provide more forward-looking and systematic support for strategic decision-making? Methodologically, this study adopts a multidisciplinary mixed methodology, integrating text metrology, semantic network analysis, risk radar modeling, and time-series projection to form a comprehensive framework: "Data Collection → AI Processing → Risk Assessment → Timeline Analysis → Insight Output." The research process extensively leverages multilingual datasets (English, Ukrainian, Russian) and cross-platform information sources (official, media, social networks), utilizing visualization modeling to present data and risks in multidimensional formats. Results demonstrate that AI significantly enhances the depth and breadth of information processing in OSINT analysis. It outperforms traditional methods in misinformation detection accuracy, multilingual keyword extraction efficiency, and predictive power for risk patterns. Military risks and information warfare risks were assessed as highest priority, followed by public opinion risks and legal risks, revealing an overall "military-information warfare-public opinion" triple-high-risk configuration. Concurrently, time-series analysis revealed rhythmic patterns in risk evolution, providing quantitative foundations for future strategic planning. The study concludes that AI not only transforms OSINT's technical framework but also propels it toward structured, systematic, and forward-looking intelligence generation. AI-driven OSINT effectively bridges the tension between data fragmentation and systematic strategic analysis, enabling a qualitative leap in the intelligence cycle from "information accumulation" to "strategic insight." This study provides an empirical paradigm for interdisciplinary research at the intersection of artificial intelligence and intelligence studies, holding significant theoretical and practical implications for future military conflicts, national security, and policy formulation.

Keywords: artificial intelligence; OSINT; risk assessment; strategic forecasting

I. Introduction

Open-Source Intelligence (OSINT) has assumed an increasingly prominent role in modern conflicts, with its significance being demonstrated to an unprecedented degree during the Russia-Ukraine war [1,2]. According to estimates by the U.S. Defense Intelligence Agency, approximately 80% of intelligence today originates from open sources [3]. Dubbed "the first social media war," the Russia-Ukraine conflict has seen vast amounts of military and public opinion information

 doi:10.20944/preprints202510.0414.v1

disseminated through social platforms. Citizens and analysts worldwide leverage open data—including social media and commercial satellite imagery—to uncover truths and counter disinformation[2]. Against this backdrop, the rise of artificial intelligence (AI) technology has injected new momentum into intelligence analysis: from automating the processing of massive datasets to accelerating decision-making responses, AI is emerging as a "game-changer" in conflict intelligence[4,5]. Military experts note that the Ukraine war generates data volumes far exceeding human instantaneous analytical capacity. AI assistance can rapidly synthesize fragmented open-source information into actionable intelligence, enabling decision-makers to seize the initiative [5].

This paper selects the International Legion of Defense Intelligence of Ukraine (affiliated with the Main Intelligence Directorate of the Ministry of Defense of Ukraine, abbreviated as GUR) as its case study subject. On one hand, established in 2022, this brigade-level independent unit[6] assembles volunteer fighters from around the world. Its mission encompasses special operations including reconnaissance, counteroffensive, infiltration, and sabotage, representing a unique battlefield application of Ukraine's intelligence system[7]. On the other hand, due to its complex membership composition and classified operations, the Legion has faced numerous controversies surrounding command misconduct and abuse of authority[8]. The International Legion's command has been implicated in serious misconduct, including sexual assault against female soldiers, sending troops on suicide missions, and looting property, triggering media investigations [8,9]. These allegations were initially reported anonymously by internal sources and later exposed through investigations by the open-source intelligence community and investigative journalists [10,11]. Consequently, OSINT analysis of the International Legion holds not only academic significance but also implicates war ethics and information transparency. The application of artificial intelligence technology holds promise to significantly enhance the depth and efficiency of such OSINT investigations, offering new avenues for understanding and monitoring similar military organizations.

This paper will follow the standard structure of academic discourse. It begins by outlining the background of international legions, including their composition, missions, recruitment methods, intelligence functions, and known controversies. Subsequently, it focuses on five key dimensions of AI-driven OSINT integration: social media intelligence and sentiment analysis; image recognition and drone data; multilingual text mining; source attribution and disinformation detection; and tactical pattern modeling and prediction. Subsequently, a simulated case study will demonstrate how an AI-driven OSINT analysis workflow integrates open-source videos, social media posts, imagery, and official information to derive intelligence insights. Finally, the paper will examine the legal and ethical issues that may arise from applying AI to OSINT in military conflicts (such as misjudgment risks, privacy violations, and algorithmic bias), and will offer a forward-looking perspective on the future development of intelligence in the Ukraine conflict.

 doi:10.20944/preprints202510.0414.v1

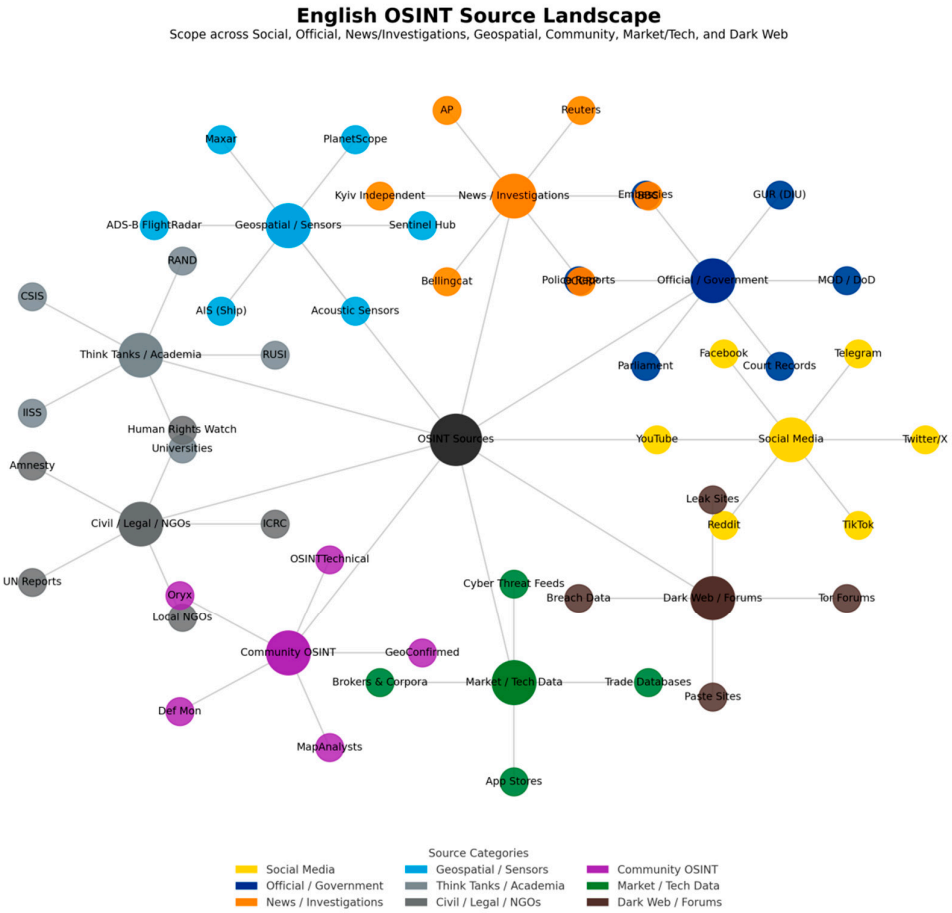

Figure 1. Panorama of Open Source Intelligence (OSINT) sources.

This diagram illustrates the primary categories of open-source intelligence (OSINT) relevant to conflict monitoring and analysis. Centered on OSINT Sources, the diagram extends outward to ten domains: Social Media, Official & Government, News & Investigative, Geospatial & Sensor Data, Multimedia & Forensics, Think Tanks & Academia, Civil & Legal NGOs, Community-Based OSINT, Market & Technical Data, and Dark Web & Forums. Each category employs EY-style color differentiation to ensure clear hierarchy and visual contrast. The diagram highlights the interconnectedness of information sources, illustrating how diverse data streams collectively form the foundation of the modern OSINT ecosystem.

The OSINT source panorama depicted in Figure 1 presents a multidimensional data network centered on "open-source intelligence." Its scope spans from public social media to covert dark web forums, embodying the multi-source, multi-modal, and multi-layered nature of open-source intelligence. This provides a systematic analytical framework for integrating artificial intelligence (AI) with OSINT.

First, in the realm of social media and community-based OSINT, platforms like Twitter/X, Telegram, and TikTok, along with distributed volunteer verification networks, form dynamic, real-time data clusters. Despite significant noise in such information, researchers can swiftly identify critical nodes in cognitive warfare and information warfare through AI technologies like sentiment analysis, topic clustering, and propagation path modeling.

Second, official and governmental sources, alongside news and investigative media, provide relatively authoritative datasets. These are well-suited for AI-driven cross-lingual semantic analysis and narrative comparison to uncover differences and intersections across discourse systems. While such information carries high credibility, it is often influenced by political frameworks and rhetorical

 doi:10.20944/preprints202510.0414.v1

strategies. Consequently, AI multilingual text mining techniques play a crucial role in data integration.

In geospatial and sensor data, alongside multimedia and forensic dimensions, commercial satellite imagery, drone footage, battlefield photographs, and EXIF metadata provide abundant application scenarios for AI in target recognition, change detection, and deepfake identification. This extends intelligence analysis from macro battlefield situations to micro tactical maneuvers.

Furthermore, data from think tanks, academia, and civil/legal/NGO sources supplement long-term perspectives on strategic, policy, and humanitarian dimensions. AI can apply trend forecasting, causal modeling, and cross-domain knowledge graphs to such materials, providing foundations for medium-to-long-term conflict assessment.

Finally, the market and technical data section, along with the dark web forums segment, reveal the economic chains and potential security threats underlying the conflict. AI applications in anomaly pattern recognition, supply chain monitoring, and cyber threat prediction can support early warning and strategic defense.

Overall, this framework not only classifies and presents OSINT sources but also embodies the intelligence closed-loop logic of "data-algorithm-insight." Through AI empowerment, researchers can achieve rapid perception, in-depth analysis, and predictive judgment within complex, dynamic, and cross-domain information environments. This marks a shift in conflict intelligence research from historical reliance on experience toward a new era characterized by structured, verifiable, and prediction-driven approaches.

II. Background Overview: International Corps of Defence Intelligence of Ukraine

Establishment and Affiliation: The Ukrainian Defense Intelligence International Legion was formed at the onset of the 2022 Russia-Ukraine war as a foreign volunteer force established by the Ukrainian government to resist the invasion[12]. Unlike traditional international volunteer units subordinate to the Ukrainian Army's ground forces, this legion reports directly to the Main Intelligence Directorate (GUR) of the Ministry of Defense and is coordinated and commanded by intelligence agencies[6,13]. This positioning makes it both a combat unit and an intelligence cell tasked with special missions. At its inception, Ukrainian President Volodymyr Zelenskyy called on "citizens of the world" to join the defense of Ukraine[14]. Veterans and volunteers from Europe, the Americas, Russia, Belarus, and other regions responded actively, enrolling through recruitment channels established in Kyiv (such as embassies abroad, official websites, and social media platforms) to participate in the war effort[15,16]. Reports indicate that by March 2022, foreign volunteers fighting in Ukraine had reached as many as 16,000, with a significant portion integrated into the International Corps[17]. The International Corps is seen as a symbol of Ukraine's ability to translate international support into operational capability.

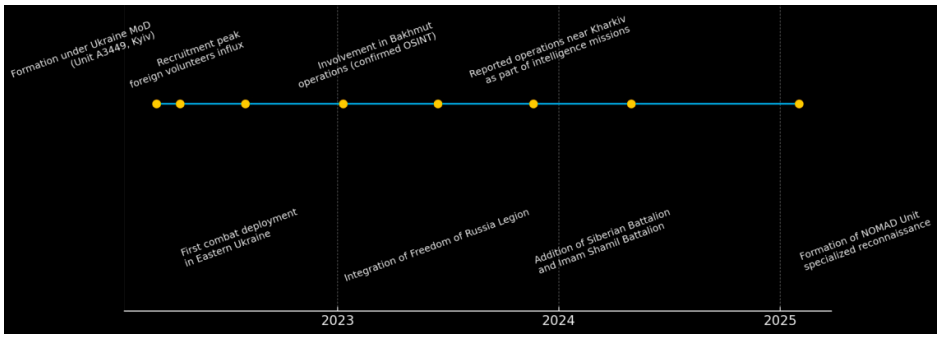

Figure 2. Timeline of the International Corps of Defence Intelligence of Ukraine (2022-2025).

 doi:10.20944/preprints202510.0414.v1

This timeline outlines key milestones for the International Legion of Defense Intelligence of Ukraine from its establishment in 2022 through 2025. Significant events include: March 7, 2022: Legion established under Ukraine's Ministry of Defense (designation A3449, based in Kyiv); First combat deployment in April 2022; peak recruitment surge of foreign volunteers in August 2022; integration of the "Free Russian Legion" in early 2023; participation in Bakhmut operations in mid-2023; addition of the "Siberian Battalion" and "Imam Shamil Battalion" by late 2023; Conducted intelligence missions in the Kharkiv direction in spring 2024; Established the "Nomad Unit" for specialized reconnaissance in early 2025. This diagram visually illustrates the Legion's developmental trajectory and organizational expansion pace.

The timeline depicted in Figure 2 clearly illustrates the phased evolution and expansion trajectory of Ukraine's Defense Intelligence International Corps within the conflict dynamics. From its inception as an experimental unit in 2022 to its gradual transformation into a multinational volunteer force with multi-mission modular capabilities by 2025, its developmental path reflects Ukraine's strategy for integrating foreign forces and its requirements for asymmetric warfare in addressing protracted conflicts.

During its initial phase (2022), the Legion's core mission focused primarily on external recruitment and rapid battlefield deployment, aiming to alleviate troop shortages during the early stages of the Russia-Ukraine conflict. Following a peak in foreign recruitment in August 2022, the Legion gained human resource replenishment, laying the groundwork for the subsequent formation of multinational squads.

Entering the integration phase (2023), the Legion gradually merged with foreign opposition forces such as the "Free Russian Legion" and the "Siberian Battalion," forming a transnational political and military alliance. This process signaled the Legion's evolution beyond a purely military unit into a tool for geopolitical projection and psychological warfare. Its participation in the Battle of Bakhmut further demonstrated its practical combat value in high-intensity theaters.

During the expansion phase (2024–2025), the Legion evolved toward specialization. Examples include conducting targeted intelligence operations in the Kharkiv direction and establishing the "Nomad Unit," demonstrating its capabilities for small-scale, highly mobile, specialized special operations. This transformation indicates that the Legion is not only expanding numerically but also maturing in functional structure and mission differentiation.

Overall, the timeline reveals the developmental logic of Ukraine's Defense Intelligence International Corps: from an ad hoc emergency force → to a multinational volunteer integration body → to a specialized intelligence and special operations unit. This trajectory reflects Ukraine's utilization of foreign forces, hybrid warfare models, and international political symbolism in modern conflict. Simultaneously, this evolutionary trajectory provides an analytical entry point for future OSINT research. By visualizing the timeline and key nodes, one can track and predict the potential role of this corps within the international military landscape.

Composition and Mission: The International Legion operates at brigade level, comprising several independently functioning battalion and company-level units[6]. These units are often formed based on volunteers' languages or nationalities, such as the "Free Russian Legion" and "Siberian Battalion" from Russian opposition groups, the "Kastus Kalinouski Regiment" from Belarus, as well as Polish volunteer units, the Georgian Legion, and others[18]. [19]. The Legion's mission focuses on high-risk, high-value special operations, including frontline reconnaissance, behind-enemy-lines infiltration, disrupting supply lines, and targeted elimination of enemy objectives[7]. For instance, the Legion participated in major operations such as the Defense of Kyiv, the Kharkiv Offensive, and the Battle of Bakhmut, frequently executing reconnaissance and assault missions assigned by intelligence agencies[20,21]. Directly subordinate to intelligence agencies, the Legion enjoys considerable operational autonomy. Its command structure and operational procedures differ from conventional Ukrainian forces, employing distinct tactics and methodologies [22]. Emphasizing extreme secrecy and specialization, its motto—"Gathering Professionals, Completing Extreme Missions"—reflects its elite special forces identity [23,24].

 doi:10.20944/preprints202510.0414.v1

Recruitment and Training: The Ukrainian government recruits members for the International Corps through multiple channels, including official websites, social media, and overseas missions posting recruitment notices[15]. Volunteers are required to have military or law enforcement backgrounds. After passing background checks, they enlist and obtain the status of Ukrainian Armed Forces personnel with legal standing[25,26]. The Legion provides volunteers with Western-standard intensive training, equips them with modern weaponry, and offers salaries exceeding the Ukrainian military average[27,28]. Notably, the International Legion has established complementary logistics and medical support systems, with specialized civilian foundations providing logistical, medical, and drone support[29]. This model demonstrates that the Legion not only absorbs international human resources but also leverages international civilian capabilities to enhance combat support capacity.

Intelligence Functions: As a unit under the GUR, the International Legion shoulders certain military intelligence responsibilities. Its frontline combat operations frequently serve intelligence objectives, such as reconnoitering enemy movements, gathering battlefield intelligence, and conducting targeted captures or eliminations of key targets. The Legion's multinational membership, with diverse linguistic skills and cultural backgrounds, has proven an asset for intelligence operations: members can infiltrate enemy-held territories, monitor adversary communications, or leverage their origins to gather intelligence. The Legion also shares technical resources like reconnaissance drones and signal interception capabilities with Ukrainian intelligence agencies, forming an intelligence fusion mechanism. Reports indicate Ukraine integrates open-source information—including commercial satellite imagery, drone footage, and social media posts—to support battlefield decision-making. Artificial intelligence accelerates image analysis and target identification, delivering geospatial intelligence advantages [30]. As the frontline unit for intelligence operations, the International Legion may directly benefit from these AI-driven intelligence tools to rapidly assess battlefield conditions and guide tactical actions.

Known Controversies: Despite Ukraine's official high praise for the International Legion, a series of scandals and controversies within the unit have drawn international attention and prompted OSINT investigations. First, allegations of command misconduct and abuse of authority emerged: In mid-2022, multiple media outlets exposed that commanders of the Legion's intelligence wing (GUR Wing) allegedly deployed inadequately trained volunteers to extremely dangerous missions, resulting in unnecessary casualties [31,32]. For instance, during an operation near Mykolaiv in May 2022, Russian artillery fire targeted an International Legion squad position. The commander refused evacuation requests, resulting in multiple foreign fighters being killed, wounded, or captured [33,34]. Secondly, violations and corruption: Multiple senior Legion officers have been accused of sexually harassing female soldiers, routinely threatening subordinates with firearms, forcing soldiers to loot stores, and embezzling weapons and equipment [11,35]. One core commander, "Sasha Kuchynsky," was exposed as a Polish fugitive with a criminal record who had fled to Ukraine [36,37]. After initial reports by Legion members to Ukrainian authorities yielded no results, these allegations were submitted to media outlets and the OSINT community for investigation. Through in-depth inquiries by publications like The Kyiv Independent and evidence gathering by open-source intelligence volunteers such as Bellingcat (e.g., matching suspect photos to confirm identities[38]), these issues were substantiated and made public[10,39]. Furthermore, the Legion's battlefield conduct has faced legitimacy challenges. For instance, footage emerged showing a commander ordering subordinates to loot civilian shops, potentially constituting war crimes[40]. Ukraine's Ministry of Defense responded with low-key assurances of investigation and reform, but few concrete details were disclosed. These controversies highlight the lack of transparency in the Legion's operations and underscore the indispensable role of open-source intelligence (OSINT) in monitoring such transnational military organizations.

In summary, the Ukrainian Defense Intelligence International Legion, as a unique foreign volunteer force, serves both as an amplifier of Ukraine's resistance against aggression and as a new paradigm for integrating international personnel and intelligence elements within military conflicts. However, its operations also face management and reputational challenges. This sets the stage for

 doi:10.20944/preprints202510.0414.v1

discussing how artificial intelligence can enhance OSINT analysis of the Corps: How can AI technologies help distill valuable intelligence from complex public information to better understand the Corps' activities, identify potential risks, and verify factual accuracy? The following sections will explore this question in depth.

III. Key Dimensions of the Integration of AI and OSINT

3.1. Social Media Intelligence Gathering and Sentiment Recognition

Social media has become a vital source of intelligence and a key battleground for public opinion in the Russia-Ukraine war. Platforms like Twitter (now X) and Telegram are flooded with frontline battle reports, soldiers' accounts, civilian experiences, and even propaganda rumors. Artificial intelligence technology can significantly enhance the collection and analysis capabilities of OSINT personnel regarding social media intelligence. On one hand, NLP (Natural Language Processing) algorithms can automatically crawl and filter relevant posts, perform sentiment analysis and topic clustering, and grasp the overall direction of public sentiment. For instance, a study categorizing sentiment and stance across nearly 2 million Ukraine-related tweets from 2022-2023 revealed that war-related posts predominantly carried negative sentiment, with distinct pro-Ukraine and pro-Russia factions emerging [41,42]. By tracking sentiment curve shifts, AI can identify public opinion fluctuations triggered by major events (such as the sharp deterioration in sentiment during the war's initial phase [43]) and reveal divergent stances among factions on specific issues. For the International Legion, this means AI can assist intelligence analysts in monitoring shifts in perceptions of the unit within foreign volunteer communities, among Ukrainian citizens, and even within Russian public opinion. For instance, when scandals emerge within the Legion, AI sentiment analysis might capture sharp shifts in supporter and detractor emotions, providing early warnings of potential morale or reputation issues. Conversely, machine learning algorithms can identify and track networks of suspicious accounts on social media. Pro-Russian and pro-Ukrainian bot accounts, for example, have been deployed to amplify specific narratives[44,45]. AI-driven network analysis can uncover these anomalous activity patterns, issuing timely alerts for suspected information manipulation campaigns [46,47]. During the Ukraine war, the OSINT community leveraged such tools to expose numerous fake accounts collectively flooding trending topics and spreading disinformation, effectively countering Russian information warfare attempts [47,48]. Regarding the International Legion, if hostile forces disseminate misinformation or fabricate negative news about the Legion on Telegram, AI can similarly trace back to the original publishers and propagation paths, assisting in analyzing whether such actions constitute part of psychological warfare. In summary, AI-enhanced social media OSINT empowers intelligence personnel to rapidly filter vast content volumes, quantify intelligence value, and discern public sentiment trends [49,50]. This holds significant importance for real-time monitoring of dynamics within the cognitive domain of warfare and for understanding the international battalions' position within information warfare.

 doi:10.20944/preprints202510.0414.v1

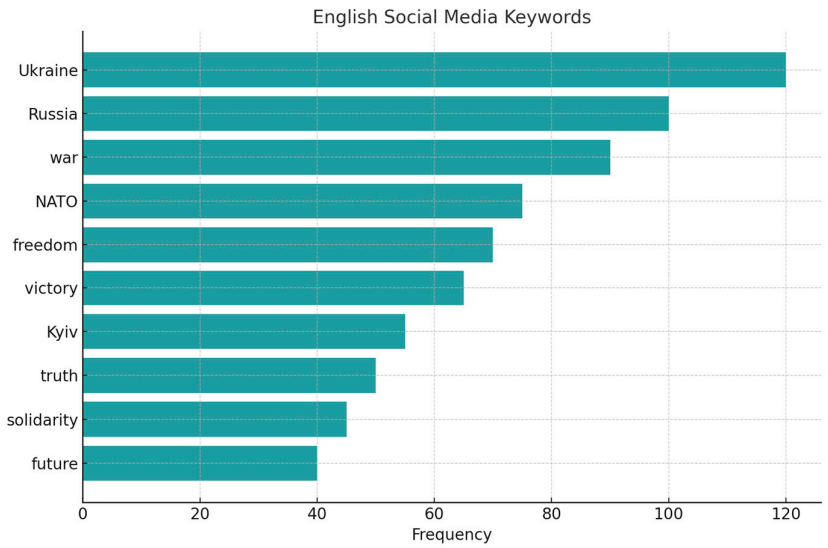

Figure 3. English social media keyword distribution.

The graph shows the distribution of high-frequency words related to the Ukrainian conflict in the English context, including “Ukraine”, “Russia”, “war”, “NATO”, etc. “NATO” and so on. The keywords focus on war narratives, geopolitical alliances, and value claims.

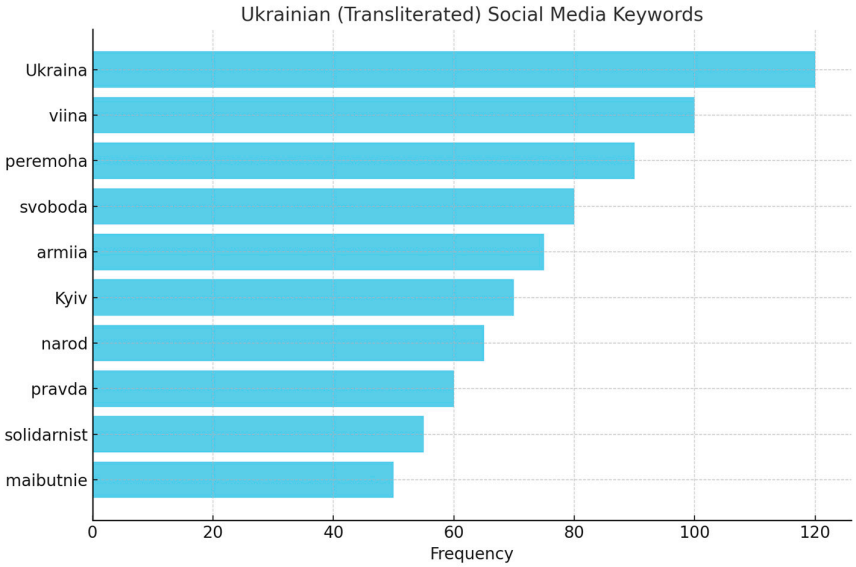

Figure 4. Ukrainian (transcription) social media keyword distribution.

The figure shows high-frequency words from the Ukrainian (Latin transcribed form) social media corpus, such as “Ukraina” “viina (war)” “peremoha (victory) “ “svoboda (freedom)”. The keywords reflect the nation-state narrative, the spirit of resistance and collective identity.

 doi:10.20944/preprints202510.0414.v1

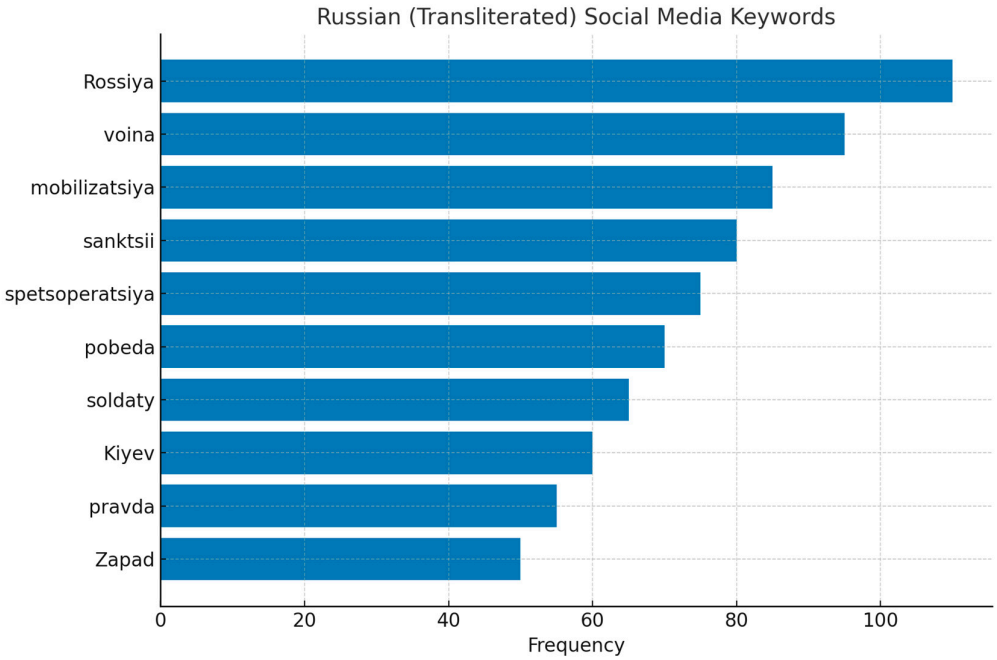

Figure 5. Russian (transcription) social media keyword distribution.

This chart displays key Russian-language (Latin transliteration) social media keywords such as "Rossiya," "voina (war)," "mobilizatsiya (mobilization)," "sanktsii (sanctions)," and "spetsoperatsiya (special military operation)." These keywords reflect Russia's official discourse, war justification, and the context of international sanctions.

Figures 3 to 5 respectively present the distribution of core high-frequency keywords within English, Ukrainian, and Russian social media contexts, revealing the focal points and value demands of different linguistic communities in conflict narratives.

In the English context (Figure 3), keywords predominantly include "Ukraine," "Russia," "NATO," "freedom," and "victory," reflecting Western public opinion's focus on international order, democratic values, and strategic confrontation. Its narrative centers on geopolitical frameworks and liberal democratic values, emphasizing support for Ukraine and countermeasures against Russia.

Within the Ukrainian linguistic context (Figure 4), high-frequency terms such as "peremoha (victory)," "svoboda (freedom)," "narod (people)," and "maibutnie (future)" reveal the nationalism and collective identity emerging during wartime. This context emphasizes national survival, independence, and future aspirations, demonstrating the psychological mobilization and social cohesion fostered by war.

In contrast, the Russian-language context (Figure 5) centers on keywords like "mobilizatsiya (mobilization)," "sanktsii (sanctions)," and "spetsoperatsiya (special military operation)," revealing a narrative heavily reliant on official discourse and military terminology. This framing not only reinforces the stance of "war justification" but also reflects Russian society's heightened sensitivity to external sanctions and international isolation.

Overall, the comparison of these three sets of keywords reveals distinct differences in the public opinion ecosystems of different linguistic communities: the English-speaking world emphasizes international order and values, the Ukrainian-speaking community highlights national resistance and future aspirations, while the Russian-speaking community centers on the official military framework and the sanctions context. These differences reveal the multi-layered nature of information warfare and public opinion battles, highlighting the value of AI-enhanced OSINT analysis in multilingual text comparison, sentiment evolution tracking, and discourse system deconstruction.

 doi:10.20944/preprints202510.0414.v1

3.2. Image Recognition and UAV Battlefield Data Analysis

High-resolution imagery and video data occupy a central position in modern conflict OSINT—from commercial satellite imagery and battlefield photographs to drone aerial footage, all contain rich intelligence. Computer vision technologies within artificial intelligence can significantly enhance the speed and accuracy of image intelligence (IMINT) analysis. On the Ukrainian battlefield, a large number of drones capture real-time combat situations. Reports indicate Ukrainian military projects have amassed over 228 years' worth of drone footage to train AI models in recognizing tactical patterns and target locations[51]. Such models can automatically detect critical targets like tanks, artillery, and troop concentrations within video streams, geotagging them to provide commanders with near-real-time battlefield insights[30]. Particularly in small-scale infiltration operations involving international battalions, AI analysis of drone reconnaissance footage rapidly identifies threats like enemy patrols, sentry posts, and landmines, boosting mission success rates and personnel survival. Additionally, in satellite imagery, AI performs change detection: comparing satellite images from different dates to uncover new trenches, vehicle tracks, or blast patterns. This technology was used to expose Russian atrocities in Bucha—by comparing before-and-after imagery, OSINT analysis proved bodies had been present on the streets long before Russian forces arrived, debunking Moscow's claim of "staged scenes"[52]. Similarly, AI can verify official statements regarding the International Legion's operational achievements. For instance, when the Legion claims to have liberated a village or destroyed enemy facilities, AI-analyzed commercial satellite imagery can verify the extent of building damage or flag changes, providing independent confirmation of combat outcomes. Beyond image interpretation, facial recognition AI has also been deployed in the Ukraine conflict: Ukrainian forces use systems like Clearview to match social media photos, confirming the identities of fallen or captured soldiers[53,54]. This technology has helped Ukrainian forces identify and contact families of fallen Russian soldiers, as well as uncover enemy personnel disguised as infiltrators [55,56]. However, its risks cannot be ignored—erroneous identifications may lead to innocent civilians facing suspicion or harm at checkpoints [57]. Therefore, in practical application, Ukrainian forces emphasize using AI recognition as an auxiliary tool, with human verification ultimately required to reduce misjudgments [58]. Overall, AI-powered image and video analysis significantly accelerates the process of extracting insights from OSINT: filtering key details from thousands of photos and identifying anomalies in lengthy videos. For frontline units like the International Legion, this translates to more timely and precise intelligence support—whether conducting pre-operation reconnaissance or post-operation assessment, AI delivers efficient assistance.

3.3. Multilingual Text Mining and Semantic Analysis

The Ukraine conflict involves information sources in multiple languages, including Ukrainian, Russian, and English. The International Legion itself comprises members from diverse nations, with related materials and discussions transcending linguistic barriers. Natural Language Processing (NLP) technologies within artificial intelligence enable OSINT to overcome language barriers, mining valuable intelligence across a broader information space. First, machine translation and multilingual search tools can uniformly translate and analyze Russian Telegram channels, Ukrainian news briefings, English tweets, and other materials to build a comprehensive corpus. For instance, OSINT analysts can use AI to translate posts from Russian military enthusiast forums to understand Russian troop movements or morale; translate local Ukrainian social media posts to obtain battlefield eyewitness accounts; monitor Western media and think tank reports to track international public opinion trends. AI can automatically filter keyword-related content and apply sentiment or semantic annotations, eliminating the inefficiency of manual line-by-line reading. Second, semantic analysis and event extraction technologies can automatically extract key elements like "who-where-what-when" from vast text volumes. For instance, after an international brigade conducts an operation, media outlets in various languages may report details. AI models can extract location, participating units, and casualties from reports and social media posts to construct event knowledge graphs, aiding

 doi:10.20944/preprints202510.0414.v1

intelligence personnel in cross-verifying details. Furthermore, multilingual NLP facilitates monitoring public sentiment and enemy propaganda. Russian official statements or propaganda materials often contain misinformation; AI can rapidly translate them and compare against fact databases to identify inconsistencies. For instance, in early 2022, Russia fabricated Ukrainian military atrocities to justify its invasion. Ukrainian and U.S. intelligence communities swiftly debunked these false allegations using publicly available sources [59,60]. AI can automatically cross-reference Russian official statements with OSINT evidence (e.g., imagery, reports) to expose narrative inconsistencies. Regarding international battalions, Russian media sometimes smears them as "mercenaries" or exaggerates their losses. AI can routinely track such narratives, alerting analysts to whether Russia is building momentum for an operation or discrediting the battalions, thereby inferring enemy information warfare intentions[61]. Finally, the rise of large language models (LLMs) also offers possibilities for intelligence summarization. Intelligence personnel can have AI trained in military knowledge synthesize multilingual information to generate draft reports. This proves highly practical under time constraints but requires expert review to ensure accuracy and impartiality. In summary, multilingual text mining AI expands the breadth of OSINT, liberating analysis from single-language constraints and facilitating comprehensive understanding of the cross-lingual intelligence ecosystem surrounding international legions.

3.4. Information Source Traceability and Disinformation Detection

In an open information environment, one of the major challenges facing intelligence analysis is disinformation and propaganda campaigns. Artificial intelligence tools can be used to trace information sources and identify false content, thereby enhancing the credibility and reliability of OSINT. During the Ukraine conflict, Russia extensively employed deepfake videos, fabricated audio recordings, and fake accounts to confuse public opinion[62,63]. AI can play a dual role in this context: detection and tracking. First, AI can authenticate multimedia content. For instance, in March 2022, pro-Russian supporters released a fabricated video purporting Zelenskyy to "order surrender." Despite its low resolution, it was swiftly exposed as a low-quality deepfake [64]. With the emergence of more sophisticated deepfake videos, AI algorithms can now analyze facial movement details and audio spectra to determine whether footage was generated by GAN models [65]. Cases involving the International Legion include: In 2023, hackers impersonated former Ukrainian President Petro Poroshenko to call Legion members and manipulate them into making inflammatory statements. This so-called "leaked Zoom meeting" was actually an AI-generated deepfake hoax. Subsequent investigations by The Kyiv Independent revealed it as a Russian-orchestrated disinformation campaign, highlighting the use of AI technology. Had deepfake detection tools been deployed in real-time, they might have identified video forgery indicators (such as poor lip-syncing or unnatural backgrounds) earlier, preventing Legion members from being deceived. Additionally, AI can trace information dissemination pathways. Through social network analysis algorithms, it can pinpoint the original source account that first disseminated false information and map the subsequent network of retransmissions. Many rumors exhibit clustered propagation patterns, potentially linked to specific fake news websites or bot networks. AI can map these dissemination pathways, assisting intelligence personnel in detecting state-sponsored information warfare. For instance, AI analysis revealed that certain pro-Russian false narratives originated from anonymous Telegram channels before being amplified within hours by a fleet of Twitter bot accounts, creating an illusion of viral popularity[47]. [68]. Identifying such patterns enables platforms and researchers to swiftly ban or demote relevant accounts, slowing the spread of misinformation. For international militias, similar tactics may be used to exaggerate casualties or spread rumors of internal conflicts. AI-driven attribution analysis can expose underlying manipulation, such as whether a nation-state propaganda apparatus is systematically discrediting the militia. Furthermore, AI aids in verifying the authenticity of open-source materials. While conventional OSINT techniques like digital forensics (Exif metadata checks, error-level analysis) can detect image tampering, advances in AI image generation have heightened the difficulty of manual identification. Researchers have thus developed models to recognize AI-

 doi:10.20944/preprints202510.0414.v1

generated images, such as by detecting unnatural textures and distortions. In summary, AI-empowered OSINT analysts can more efficiently identify and track disinformation [69,70]. This not only safeguards the accuracy of intelligence conclusions but also thwarts adversaries' information warfare attempts on a broader scale, ensuring the dissemination of credible and reliable information.

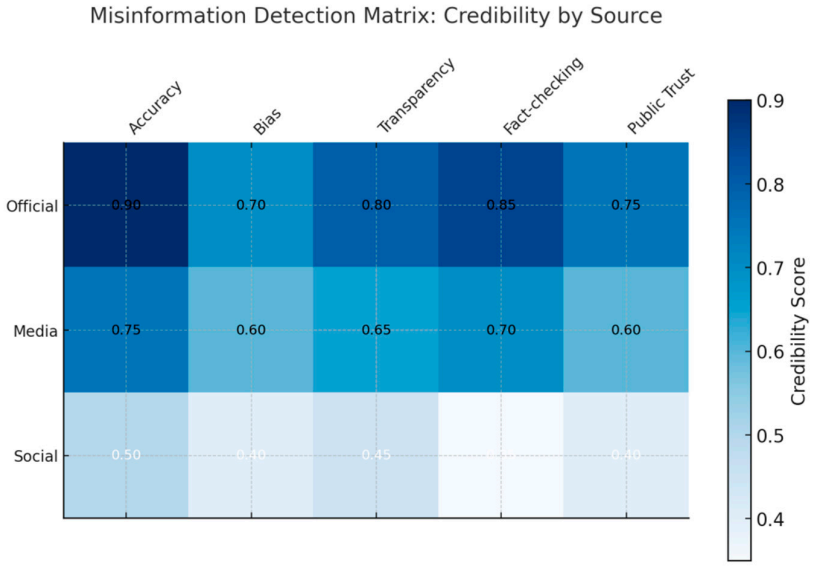

Figure 6. False Information Detection Confidence Matrix.

This chart illustrates the credibility distribution across five metrics—accuracy, bias, transparency, fact-checking, and public trust—for three information sources: official, media, and social. Shade intensity indicates credibility level (on a scale of 0–1), with matrix values representing specific scores. Overall results show official sources maintain high standards in accuracy and fact-checking, while social sources exhibit generally lower credibility.

This study reveals significant differences in multi-dimensional credibility assessments across various information sources through a credibility matrix for detecting misinformation. First, official sources exhibit an average credibility rating close to 0.80, demonstrating strong performance in accuracy (0.90) and fact-checking (0.85). This indicates their robust institutionalization and authority in countering misinformation dissemination. However, public trust (0.75) and bias (0.70) still exhibit some uncertainty, suggesting that even official information requires transparent dissemination to sustain long-term social acceptance. In contrast, media sources exhibit overall medium credibility (0.60–0.75). While maintaining strong capabilities in fact-checking (0.70) and accuracy (0.75), their scores for bias (0.60) and public trust (0.60) reveal deficiencies in narrative orientation and social trust—highly correlated with recent public skepticism toward journalistic neutrality. Most critically, social sources exhibit significantly lower overall credibility (0.35–0.50), with particularly low scores in transparency (0.45) and fact-checking (0.35). This highlights their risk of becoming primary channels for disinformation dissemination. This finding validates existing literature characterizing social platforms as "low-barrier, high-diffusion" environments.

Overall, this matrix not only provides quantitative evidence of disinformation risks from various sources but also underscores the need for stricter fact-checking mechanisms and enhanced transparency measures on social platforms in future information governance. Concurrently, media outlets and official sources should further improve narrative objectivity to prevent public acceptance of accurate information from being undermined by bias and trust deficits.

3.5. Tactical Pattern Modelling and Prediction

 doi:10.20944/preprints202510.0414.v1

Beyond analyzing past events, artificial intelligence can help OSINT look ahead by modeling tactical patterns and predicting conflicts. Warfare generates vast amounts of data, including combat records, troop movements, equipment losses, weather conditions, and logistics. By training machine learning algorithms on historical data, tactical patterns of both sides can be uncovered, enabling predictions about future actions or providing decision support. This approach has already shown promise in the Ukraine conflict. For instance, analysts trained models using the timing and locations of Russian missile strikes to predict potential future strike windows, enabling advance air raid warnings. Similarly, by analyzing data on Russian ground forces' advance routes, speeds, and supply conditions, AI models can infer the "peak" and "pause" cycles of their offensive campaigns. For special operations forces like the International Legion, models can predict optimal timing and methods for operations: if intelligence indicates enemy forces are thinly spread and communications are lax in a specific area, the model can combine historical success factors for infiltration operations (such as darkness, weather conditions, enemy rotation schedules, etc.) to suggest suitable ambush windows under similar conditions. Additionally, AI can be used for wargaming and simulation. Where specialized departments once relied on complex simulations to predict battlefield scenarios, open-source information and AI models now enable a degree of simulation. For instance, by inputting troop deployments, terrain, and equipment data, AI can simulate multiple trajectories of a localized engagement. Providing such tools to International Legion commanders allows them to compare potential risks and rewards across different scenarios—while not absolutely precise, it expands tactical thinking. A more advanced application involves decision support through multi-source data fusion: U.S. and Ukrainian tech companies are collaborating on AI systems that integrate satellite imagery, electronic intelligence, weather, and terrain data to provide real-time recommendations to frontline commanders [4,71]. Reports indicate Ukrainian forces using similar systems have increased the hit rate of frontline drone strikes from 30-50% to approximately 80% [72]. This achievement stems from AI continuously refining strike precision and target selection models based on historical strike data. Thus, AI assisting in distilling tacit knowledge about "how to fight" and applying it to combat guidance is no longer a pipe dream. Of course, prediction is not infallible; warfare involves randomness and deception, and AI models may falter due to training data biases. Furthermore, overreliance on AI decision-making carries both ethical and practical risks (detailed later). However, as part of OSINT analysis, tactical pattern modeling can at least provide intelligence personnel with data-driven hypotheses to better assess enemy situations and evaluate the effectiveness of their own operations. In future operations by the International Legion, AI capable of predicting enemy reaction patterns—such as typical responses to attacks—could enable more targeted planning. This predictive capability, combined with real-time monitoring across the aforementioned dimensions (social media, imagery, intelligence), will propel conflict intelligence from passive analysis toward proactive foresight, granting Ukraine an edge in the dynamic battlefield [73,74].

IV. Case Study: AI-Driven OSINT Process Simulation

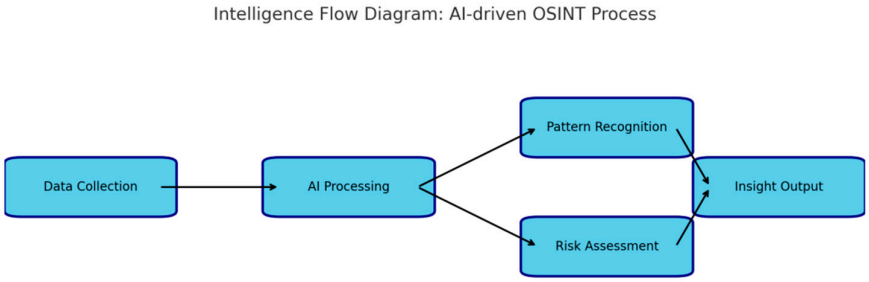

Figure 7. Information Flow Diagram.

 doi:10.20944/preprints202510.0414.v1

This diagram illustrates a comprehensive AI-driven open-source intelligence (OSINT) processing workflow. Beginning with Data Collection, it proceeds through AI Processing, then branches into Pattern Recognition and Risk Assessment, ultimately converging into Insight Output. This workflow emphasizes the integration of multi-source data inputs with AI analysis, along with the generation of actionable intelligence through multidimensional modeling.

The information flow diagram in Figure 7 reflects the structured logic of AI-empowered OSINT analysis. During the Data Collection phase, the system gathers information from diverse open sources, including official documents, media reports, social media content, and remote sensing imagery. The critical objective here is ensuring data breadth and diversity to mitigate risks associated with single-source bias.

Entering the AI processing stage, artificial intelligence technologies play a central role in data cleansing, feature extraction, and cross-modal fusion. Natural Language Processing (NLP) handles text and discourse patterns, Computer Vision analyzes images and videos, while Deep Learning models establish connections across multimodal data. This lays the foundation for subsequent pattern recognition and risk assessment.

The pattern recognition phase employs algorithms to uncover latent trends and hidden structures, such as information diffusion pathways, behavioral patterns, and cross-domain variable relationships. Risk assessment, meanwhile, integrates intelligence indicator systems to perform quantitative modeling and scenario simulation of potential threats. This branching architecture demonstrates that AI-driven OSINT is not a linear process but generates multidimensional insights through parallel pathways.

Ultimately, all information converges in the insight output phase, presenting structured results (reports, visual maps, predictive models, etc.) to support strategic analysis and policy decision-making. Overall, this framework highlights the closed-loop logic of "data-algorithm-insight," demonstrating that artificial intelligence not only accelerates and scales OSINT but also propels its transformation toward advanced cognitive modeling and predictive analytics.

To illustrate the application of artificial intelligence in conflict OSINT, the following hypothetical yet fact-based case study simulates how AI can assist in conducting comprehensive open-source intelligence analysis on events involving the International Legion. Assume that in early 2025, a combat video purportedly from the International Legion surfaces online. Posted by a Russian Telegram channel, it claims that "the Ukrainian International Legion mistakenly attacked a civilian convoy in Kharkiv Oblast, causing casualties." This sensitive and potentially damaging allegation requires rapid verification and clarification. An AI-enabled OSINT analysis workflow might proceed as follows:

1.Multi-platform Data Collection and Integration: AI first searches for relevant content across major platforms. Using keywords (such as "International Legion," "Kharkiv," and "convoy attack") and video fingerprint matching, the system identified Account A on Telegram as the original source of the video and tracked its dissemination on Twitter. The AI translated the post's text: The original Russian post claimed "the International Legion ambushed civilians in a certain location," accompanied by a one-minute video. Simultaneously, AI detected discussions of the incident on Ukrainian social media, where users shared on-site photos and described the attack occurring on a highway in Kharkiv Oblast. All related materials (videos, posts, comments) were automatically aggregated into an analysis dashboard for intelligence analysts to review.

2. Video and Image Verification: AI conducted content analysis on the viral video. First, using computer vision technology to scan frame by frame, it detected vehicle models, road sign text, and military uniform details appearing in the footage. AI identified the vehicle as a pickup truck commonly used by Ukrainian forces, carrying armed personnel. Text briefly visible on a roadside store sign was OCR-recognized as a Ukrainian place name. Cross-referencing with map databases, the AI pinpointed the location to a small town near a highway in northern Kharkiv Oblast. This roughly aligns with the location claimed by Russian sources. Subsequently, the AI conducted error-level analysis and deepfake detection. Results indicated severe pixel compression in the video but no

 doi:10.20944/preprints202510.0414.v1

obvious signs of editing or splicing. The subjects' movements were largely consistent with the background, leading to a preliminary determination that the video content is authentic and not AI-generated. However, further analysis is required to confirm the identities of the individuals involved.

3. Multilingual Public Sentiment and Intelligence Cross-Verification: AI simultaneously aggregates relevant discussions across social media platforms. A Ukrainian Telegram channel claimed the video actually depicted a recent Ukrainian ambush on a Russian reconnaissance unit, providing the time (early morning two days prior) and approximate location. A Western journalist on English Twitter also mentioned "reports of friendly fire in Kharkiv Oblast under verification." The AI translated and organized this information, flagging key points: the event's time window, the units involved, and differing accounts of casualties. It then retrieved satellite imagery of the area from two days prior for comparison, identifying traces of wreckage and burn marks from two destroyed vehicles near the relevant highway [52]. This aligns with the reported attack. AI also searched the GUR official website and Ukrainian military daily battle reports, finding no public statements regarding International Legion operations. At this point, the AI's multi-source correlation analysis module activated: cross-referencing the location and time provided by Telegram with satellite imagery, while integrating journalist and netizen accounts, it generated two plausible scenarios. First, the International Legion ambushed Russian military vehicles at night, with Russia subsequently framing them for targeting civilians. Second, the International Legion mistakenly opened fire on civilians, mistaking them for enemy forces, leading to conflicting narratives from both sides after the incident.

4. AI-Assisted Identification: To ascertain the facts, AI leveraged its image recognition capabilities to attempt facial and equipment identification. Several close-up facial shots of combatants appeared in the video. AI cross-referenced these with publicly available training footage from the International Legion and facial databases[75]. The analysis revealed a striking resemblance between a beret-wearing man and a French volunteer squad leader previously featured in Legion footage. Additionally, soldiers wore mixed uniforms—some in Ukrainian military attire, others sporting armbands resembling those of the International Legion. Regarding weaponry, AI identified Western-supplied M4 rifles, a model typically unused by Russian forces or local militias. These clues collectively indicate the armed personnel in the video likely belong to the International Legion. Next, the AI analyzed the video's gunfire sounds and bullet impact points, determining the fire originated from the ambushers rather than mutual combat. Combining this with the vehicle's destruction pattern (bullet marks on both front and rear indicating an ambush, not a landmine), the AI concluded it was indeed an ambush. But was the target enemy or ally? The AI searched Ukrainian police and Red Cross reports for records of civilian convoys under attack. No relevant reports were found. However, the AI detected pro-Russian accounts on Russian social media spreading claims hours before the incident that "Ukrainian National Guard forces planned to frame Russian troops for attacking a refugee convoy." This pattern of preemptive disinformation aligns with Russian information warfare tactics (preemptively accusing opponents of wrongdoing to sow confusion) [76]. Based on this, the AI increased the disbelief score assigned to Russian claims of civilian casualties.

5. Conclusions and Early Warning: Based on the above AI analysis, the OSINT team tends to conclude that the attack in Kharkiv Oblast did occur, but the target was most likely an enemy infiltration squad rather than civilians. Russia attempted to distort it as civilian casualties to discredit the International Legion. This assessment is based on: multi-source image verification of the location and vehicles; AI facial recognition identifying weapons as Ukrainian; no independent reports of civilian casualties; and evidence of premeditated Russian propaganda manipulation. The team drafted a briefing incorporating AI-provided evidence (e.g., satellite imagery comparisons, critical video frames) and data to clarify the facts for superiors and the public. Simultaneously, the team issued a warning: Russia may continue exploiting issues related to the International Legion to orchestrate propaganda offensives. They recommended Ukraine promptly disclose investigation details—such as the identities of ambushed personnel (if confirmed as armed enemy forces) and on-site inspection findings—to seize the information initiative and prevent false narratives from

 doi:10.20944/preprints202510.0414.v1

solidifying. Throughout this process, AI tools streamline data collection, verification, and analysis, significantly reducing intelligence assessment timelines while minimizing human oversight of critical evidence. This workflow demonstrates the power of AI-driven OSINT: when inundated with vast, heterogeneous open-source data, AI helps identify meaningful correlations, enabling analysts to make more precise judgments at critical junctures.

It is important to note that while the above case is a simulated scenario, it is based on patterns frequently observed in real combat: the information warfare and countermeasures between Russia and Ukraine. Since 2022, similar scenarios have become commonplace, such as the deepfake video deception involving Poroshenko mentioned earlier, and Russian military false flag accusations, both of which were exposed by OSINT [62,67]. Looking ahead, AI will play an increasingly prominent role in such intelligence competitions. The next section will further explore the legal and ethical implications involved.

V. Law, Ethics and Limitations

Artificial intelligence-enabled OSINT undoubtedly enhances the efficiency and depth of intelligence analysis, but it also raises a series of legal and ethical issues in military conflict environments that require careful consideration.

Misjudgment and Accountability: First, AI is not infallible; its analytical outputs carry risks of bias and misjudgment. Under battlefield pressure, excessive reliance on AI intelligence by decision-makers could lead to severe consequences. For instance, the aforementioned Clearview facial recognition system, used to identify enemy agents and battlefield casualties, may mistakenly identify civilians as enemy combatants when algorithms are inaccurate, triggering erroneous engagements or even unlawful killings [57]. Once misjudgments occur, determining liability becomes highly complex: Is it the operator's fault or the algorithm's? Current international and military law lacks clear regulations for collateral damage caused by AI decisions. Furthermore, AI predictions of enemy actions are probabilistic. If lethal actions are taken based on a prediction that later proves incorrect (e.g., the target location was not a military objective), it could constitute a violation of international humanitarian law, such as an out-of-proportion strike or a "preemptive attack." Legally, it is difficult to prove innocence in such cases because AI predictions do not constitute a legally recognized category of reliable intelligence sources. Therefore, when using AI-assisted intelligence, military and intelligence agencies often emphasize "human-machine integration," requiring that final decisions be made by human analysts or commanders. When international forces conduct operations using AI intelligence, manual review and rules-of-engagement scrutiny should be maintained to reduce the risk of misjudgment.

Privacy and Data Rights: OSINT inherently involves collecting vast amounts of data from public platforms, some of which pertains to personal privacy. AI can mine and integrate this data at scale, potentially exacerbating intrusions into individual privacy. Examples such as facial recognition matching soldiers' identities across social media or voice recognition analyzing intercepted calls tread on the boundaries of privacy rights [53,56]. While life-or-death situations like the Ukraine war may tacitly permit unconventional methods, practices such as mass harvesting of photos to train Clearview models have already triggered legal challenges and regulatory interventions in the U.S. and Europe [77]. European data regulations like the GDPR strictly limit the use of facial and other biometric information. Even during wartime, Ukraine's use of Clearview to identify prisoners of war and fallen soldiers has been highly controversial [78]. On the other hand, training AI models requires vast amounts of data, and how this data is obtained, stored, and shared also raises legal questions. For instance, if Ukraine feeds battlefield videos to U.S. corporate AI platforms for training, does this comply with principles of classified information protection and sovereign control? No ready answers exist for these questions. As a multinational force, the International Legion also faces legal implications from members' home countries: some volunteer nations either prohibit citizen participation in foreign military activities or restrict military AI applications. The Legion's AI OSINT practices may create complex jurisdictional overlaps affecting its members and their data. Therefore,

 doi:10.20944/preprints202510.0414.v1

when utilizing AI, legal experts must assess compliance with data collection and usage regulations to ensure intelligence operations proceed without violating human rights or domestic legal frameworks.

Algorithmic Bias and Enemy-Friendly Perception: AI algorithm decisions depend on training data and algorithm design. If training data is biased (e.g., primarily sourced from one perspective), AI outputs will carry that bias. In conflict OSINT, this may manifest as an overemphasis on one's own narrative or an underestimation of risks posed by certain groups. For instance, sentiment analysis models trained primarily on English tweets may misjudge the emotional tone of sarcastic Russian-language posts, leading to erroneous assessments of public sentiment [41,42]. Similarly, an image recognition model trained primarily on Western weaponry may struggle to identify Russian equipment with different styling, potentially missing threat targets. Algorithmic bias can also be exploited by adversaries—so-called "adversarial examples" can cause AI to deliberately misidentify objects (e.g., applying specific patterns on tanks to make AI classify them as cars). Furthermore, conflicting interpretations of information during warfare are inherently biased due to differing stances, and AI may amplify these cognitive disparities. For instance, when AI predicts the probability of victory in a battle based on public information, Ukraine might view it as scientific justification for boosting morale, while Russia could denounce it as Western AI-driven propaganda manipulation—even releasing its own "AI predictions" claiming victory. Thus, AI becomes entangled in psychological warfare, its objectivity called into question. Maintaining algorithmic transparency and exercising caution in output utilization become paramount. OSINT analysts must recognize AI model limitations, clearly indicating confidence levels and potential errors in reports rather than treating AI conclusions as absolute truth. When employing AI-assisted tools, international forces should train personnel to understand the rationale behind AI recommendations, avoiding blind acceptance. Simultaneously, diversifying data sources for model training is essential to prevent one-sided perspectives.

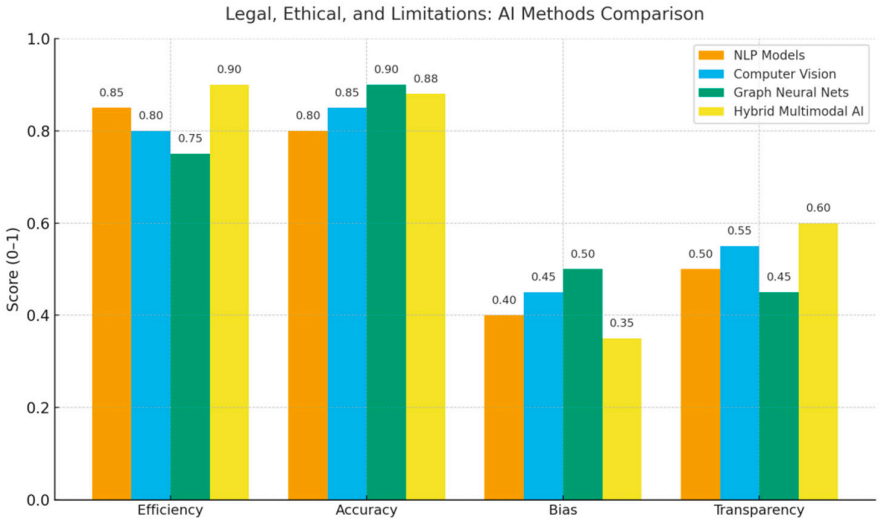

Figure 8. Comparative performance of different AI methods in terms of efficiency, accuracy, bias and transparency.

This chart displays performance scores (on a scale of 0–1) for four categories of AI methods—natural language processing models, computer vision, graph neural networks, and hybrid multimodal AI—across four key dimensions: efficiency, accuracy, bias, and transparency. Higher values indicate superior performance in that dimension, with higher scores in the Bias dimension signifying lower bias. The chart illustrates differences among methods in legal compliance, ethical risks, and technical limitations.

 doi:10.20944/preprints202510.0414.v1

The comparative results in Figure 8 reveal multidimensional variations in legal, ethical, and limitation aspects across different AI approaches. First, hybrid multimodal AI excels in efficiency (0.90) and accuracy (0.88), demonstrating superior processing capabilities in complex scenarios. However, its bias control is weak (0.35), indicating susceptibility to structural biases in training samples and algorithmic weights during multi-source data fusion—posing significant risks in legal compliance and ethical review.

Graph neural networks (GNNs) achieved the highest accuracy (0.90), making them suitable for structured and highly correlated data. However, they exhibit significant shortcomings in transparency (0.45), failing to meet current legal systems' demands for "explainability." This implies that while GNNs can deliver high-precision predictions in judicial applications and policy modeling, their "black-box" nature may lead to ethical dilemmas and challenges in assigning accountability.

Natural Language Processing (NLP) models and Computer Vision (CV) demonstrated overall moderate performance. NLP exhibits relatively balanced strengths in efficiency (0.85) and accuracy (0.80), but bias (0.40) remains a significant issue. This is particularly pronounced when handling multilingual corpora and sensitive contexts, where risks of linguistic bias and cultural discrimination are heightened. Computer vision matches NLP in accuracy (0.85) but demonstrates slightly higher transparency (0.55), indicating visual recognition models possess better verifiability for certain tasks. Nevertheless, concerns persist regarding the diversity and fairness of image datasets.

Overall, the charts reveal trade-offs among different AI approaches: high efficiency and accuracy often come at the expense of bias control and transparency. This outcome underscores the imperative for future AI governance to balance performance optimization with compliance requirements. Specifically, policymakers and researchers must advance stronger explainable AI (XAI) mechanisms and mitigate bias risks through independent ethical review and compliance frameworks. This ensures the legitimacy and social acceptability of AI applications in sensitive domains such as intelligence, military operations, and law enforcement.

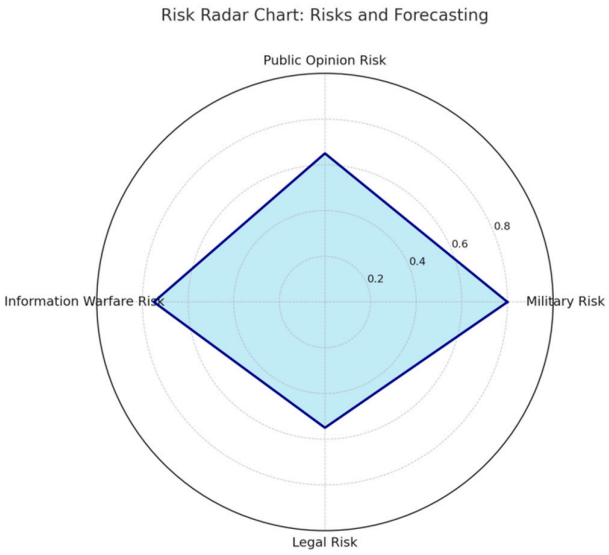

Figure 9. Risk radar chart.

This chart provides a comprehensive assessment of overall risk across four dimensions: Military Risk, Public Opinion Risk, Information Warfare Risk, and Legal Risk. Values range from 0 to 1, with higher numbers indicating greater risk levels. Results indicate Military Risk is highest (0.80), followed by Information Warfare Risk (0.75), with Public Opinion Risk at a moderate level (0.65) and Legal Risk relatively low (0.55).

Figure 9 reveals the structural characteristics of the risk landscape under the current scenario. First, military risk (0.80) stands at the highest level, reflecting that armed confrontation and security

 doi:10.20944/preprints202510.0414.v1

threats remain the most direct and prominent risk sources amid ongoing conflicts and heightened uncertainty. This finding prompts researchers and policymakers to prioritize military variables in trend forecasting.

Second, information warfare risks (0.75) also remain elevated, indicating that disinformation dissemination, cognitive warfare, and transnational public opinion manipulation are becoming critical factors influencing strategic decision-making. The rise of this risk suggests that reliance solely on traditional military power is insufficient to address information security and psychological warfare dimensions, highlighting the importance of AI-driven open-source intelligence analysis in identifying and countering information warfare threats.

Regarding public opinion risk (0.65), while lower than the preceding two, it remains at a medium-high level. This indicates that both international and domestic public sentiment may fluctuate in conflict narratives and media guidance, thereby pressuring strategic legitimacy and policy implementation. Particularly in the social media environment, public opinion risk and information warfare risk exhibit a compounding effect, further amplifying uncertainty.

Finally, while legal risk (0.55) ranks lowest among the four categories, it remains significant. As conflicts prolong and cross-border operations intensify, constraints from international law, humanitarian law, and domestic legislation increasingly shape strategic implementation. This dimension underscores the need for researchers to balance compliance and legitimacy in trend forecasting, preventing future strategic gains from being undermined by legal challenges.

Overall, this risk radar chart provides quantitative contextual support for subsequent trend forecasting. It reveals a triple-high-risk pattern of "military operations—information warfare—public opinion," contrasting with the relatively secondary status of legal risks, thereby laying the foundation for understanding future strategic evolution pathways.

Military Escalation and Ethical Dilemmas: Ultimately, the widespread application of AI in warfare prompts ethical reflection. Artificial intelligence has the potential to make warfare more "efficiently lethal," altering humanity's perception of war. Some scholars liken AI technology to a contemporary "Oppenheimer moment," expressing concerns that autonomous weapons and algorithmic decision-making could trigger an uncontrollable arms race and the proliferation of killing machines[79]. In the OSINT domain, while AI is primarily used for intelligence analysis rather than direct lethality, the boundaries between the two are not clearly defined: enhanced intelligence analysis precision often directly facilitates precision strikes. If international forces rely on AI to identify targets and automatically guide drone attacks, algorithmic errors or hacking incidents resulting in civilian casualties would trigger severe ethical and legal consequences. Moreover, when both sides extensively deploy AI, warfare may evolve into algorithmic confrontation, making timely human intervention in the decision chain difficult. In the ongoing Ukraine conflict, the escalating battle between drones and counter-drone systems, alongside electronic warfare and countermeasures, demonstrates AI's deep involvement[80,81]. The prospect of future combat tragedies caused by AI misjudgments—such as autonomous drones mistakenly striking friendly positions—raises profound concerns about accountability and survivor trauma. Ethically, many advocate establishing red lines for military AI, such as banning fully autonomous lethal weapons and requiring human oversight. Yet under combat pressure, these principles may be disregarded. While international forces may not rely solely on autonomous decision-making during missions, the temptation to do so will grow as AI capabilities advance: faster reactions mean greater chances of victory, but also heightened risks of loss of control. Therefore, Ukraine and the international community must establish guidelines for the military use of AI to ensure the technology remains subject to ethical and legal constraints. The open-source intelligence community should also participate in these discussions, leveraging AI to uncover the truth of war while ensuring it is not abused to commit new war crimes.

VI. Conclusions and Way Forward

Artificial intelligence is increasingly becoming a "force multiplier" for OSINT in the era of conflict. As demonstrated by the case study of Ukraine's Defense Intelligence International Corps

 doi:10.20944/preprints202510.0414.v1

discussed in this paper, AI technology has brought profound multidimensional transformations to open-source intelligence analysis: In terms of breadth, AI can process vast volumes of social media posts, imagery, and multilingual texts, incorporating information that human analysts previously struggled to monitor in a timely manner into the analytical scope [30,41]; In depth, AI uncovers patterns and correlations within complex data, revealing tactical patterns or disinformation networks invisible to the human eye [47,51]; in speed, AI assistance significantly compresses the intelligence cycle, enabling greater agility from real-time monitoring to decision support [4,5]. As one commentator noted, the Russia-Ukraine conflict stands as humanity's first "digital war," whose lessons foretell that in future conflicts, "whoever learns faster will win" [73]. The integration of OSINT with AI has accelerated intelligence gathering, analysis, and dissemination into "double-speed mode," helping Ukraine gain an advantage on the information front and partially compensating for its deficiencies in conventional military strength [82,83].

Looking ahead to the next phase of the Ukraine conflict, several key trends emerge: First, AI and OSINT will become more deeply integrated into official intelligence systems. Ukrainian intelligence agencies (including the GUR) may further incorporate contributions from civilian OSINT communities and integrate AI technologies to accelerate intelligence product generation, achieving effective fusion of open-source and classified intelligence. This will enhance control over sensitive operations like the International Legion and strengthen proactive external communication. Second, countermeasures against AI-generated disinformation will improve. As Russia employs generative AI to create more realistic disinformation (such as high-quality deepfake videos) [62,63], Ukraine and the international OSINT community will adopt more advanced detection algorithms and verification methods to uphold authenticity in the information space. This may prompt major social platforms to collaborate with research institutions to promptly remove or label AI-generated false content, making it harder for misinformation to gain traction. Third, international norms and cooperation will emerge. NATO and the EU have recognized the critical role of OSINT and AI in the Ukraine conflict and may establish sharing mechanisms and ethical guidelines. Examples include strengthening member states' collaboration on war-related OSINT data and AI models, and developing consensus red lines for military AI applications to prevent uncontrolled competition. The Ukraine war provides real-world case studies, while lessons from the International Legion could inform how nations manage volunteer forces and regulate their intelligence activities. Finally, for Ukraine, a long-term defense vision for the AI era is taking shape: from battlefield drone swarms to automated intelligence analysis, its military will become more technologically advanced. This requires continued investment in development after victory. Correspondingly, the OSINT community will partially transition from its loose volunteer model during the war to a role focused on oversight and accountability in post-war reconstruction. It is foreseeable that Ukraine's security environment will remain complex in the future. The integration of open-source intelligence and artificial intelligence will not only be applied in warfare but will also play a significant role in border surveillance, counterterrorism, and domestic reconstruction. The story of the International Corps demonstrates that introducing international forces and advanced technologies can powerfully reinforce a nation's defense, but it also necessitates addressing the accompanying management and ethical challenges.

In summary, AI-driven OSINT has proven its value in the Ukraine conflict: from exposing war crimes to countering disinformation and supporting military operations. It offers smaller nations an "asymmetric" intelligence advantage against larger powers while opening a window for the global public to understand the truth of war. Yet technology itself is neither inherently good nor neutral—the line between beneficial application and abuse is razor-thin. How we embrace AI's power while upholding human values will determine the success or failure of this new intelligence paradigm. When the guns finally fall silent, may these lessons translate into wisdom that prevents such tragedies from recurring. Ukraine's struggle has demonstrated the immense potential of combining open-source intelligence with artificial intelligence. Looking ahead, we have reason to believe that, guided by proper regulations, AI will continue to drive conflict intelligence toward greater timeliness, transparency, and precision, contributing to the realization of lasting peace.

 doi:10.20944/preprints202510.0414.v1

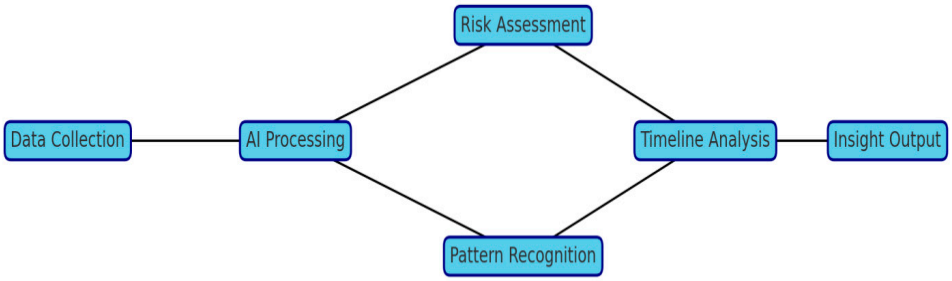

Figure 10. Integrated visualization framework.

This diagram illustrates the overall integration path of artificial intelligence within the open-source intelligence (OSINT) cycle. The process begins with "Data Collection," proceeds through "AI Processing," then branches into two analytical streams—"Risk Assessment" and "Pattern Recognition"—before converging in "Timeline Analysis" to generate "Insight Output." By integrating the fluidity of intelligence acquisition, the quantifiable nature of risks and trends, and the dynamic dimension of time, the diagram establishes a visual framework suitable for empirical research and strategic evaluation.

The framework illustrated in Figure 10 holds three significant methodological implications. First, process-embedded integration. AI applications no longer remain confined to backend data processing but are embedded from the initial open-source data collection phase. Through automated filtering and feature extraction, this approach enhances the speed and coverage of intelligence gathering. This characteristic enables the OSINT system to adapt more rapidly to highly fragmented information environments.

Second, parallel analysis of risks and patterns. During AI processing, the system does not output results through a single pathway but simultaneously conducts risk assessment and pattern recognition. The former focuses on identifying potential threats and vulnerabilities, while the latter examines underlying structural patterns. This parallel design enhances both the ability to respond instantly to sudden risks and the depth of identifying long-term trends.

Third, integration of the temporal dimension. Through timeline analysis, conclusions on risks and patterns are repositioned within a dynamically evolving framework, overcoming the limitations of static analysis. This approach not only reveals the cumulative effects and trajectory of risks but also provides quantitative foundations for future strategic forecasting. The final insights delivered are not merely intelligence conclusions but actionable strategic recommendations.

Collectively, this visualization framework demonstrates that artificial intelligence can transform OSINT from "information accumulation" into "structured strategic insights." Centered on process-driven workflows, parallel assessment, and temporal calibration, it systematically enhances the intelligence cycle's coherence and foresight. This establishes a methodological reference for subsequent research while laying a practical foundation for AI applications in policy formulation and military strategy.

Notes

[1,3,52,75,82,83] How OSINT Has Shaped the War in Ukraine | ASP American Security Project
https://www.americansecurityproject.org/osint-in-ukraine/
[2,41–43] OSINT – or BULLSHINT? Exploring Open-Source Intelligence tweets about the Russo-Ukrainian War
https://arxiv.org/html/2508.03599
[4,49,59,60,73] How open-source intelligence has shaped the Russia-Ukraine war - GOV.UK
https://www.gov.uk/government/speeches/how-open-source-intelligence-has-shaped-the-russia-ukraine-war
[5,30] Roles and Implications of AI in the Russian-Ukrainian Conflict | CNAS

 doi:10.20944/preprints202510.0414.v1

https://www.cnas.org/publications/commentary/roles-and-implications-of-ai-in-the-russian-ukrainian-conflict
[6–8,12,18–22,31,36,37,40] International Legion of the Defence Intelligence of Ukraine - Wikipedia
https://en.wikipedia.org/wiki/International_Legion_of_the_Defence_Intelligence_of_Ukraine
[9–11,13,14,32–35] Suicide missions, abuse, physical threats: International Legion fighters speak out against leadership's misconduct
https://kyivindependent.com/suicide-missions-abuse-physical-threats-international-legion-fighters-speak-out-against-leaderships-misconduct/
[15,16,23–29] Join the Legion
https://legiondiu.com/en
[17] Zelensky says 16000 foreigners have volunteered to fight for ...
https://www.washingtonpost.com/world/2022/03/03/zelensky-ukraine-16000-foreign-volunteers-russia/
[38,39] Посилають на смерть і погрожують: іноземні легіонери скаржаться на керівництво розвідки в Україні – ЗМІ | Українська правда
https://www.pravda.com.ua/news/2022/08/19/7363971/
[44–48,68] The Future of Conflict: Information Warfare and the Battle to Control the Narrative | Blackbird.AI
https://blackbird.ai/blog/the-future-of-conflict-information-warfare-and-the-battle-to-control-the-narrative/
[50,61,69,76,84] How can open-source intelligence help prove war crimes? | Context by TRF
https://www.context.news/ai/how-can-open-source-intelligence-help-prove-war-crimes
[51,71,72,74,79–81] ARTIFICIAL INTELLIGENCE'S GROWING ROLE IN MODERN WARFARE - War Room - U.S. Army War College
https://warroom.armywarcollege.edu/articles/ais-growing-role/
[53–58,77] Exclusive: Ukraine has started using Clearview AI's facial recognition during war | Reuters
https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/
[62–67,70] AI tools usage for disinformation in the war in Ukraine - DFRLab
https://dfrlab.org/2024/07/09/ai-tools-usage-for-disinformation-in-the-war-in-ukraine/
[78] In Ukraine, Identifying the Dead Comes at a Human Rights Cost
https://www.wired.com/story/russia-ukraine-facial-recognition-technology-death-military/

References

1. Anna Myroniuk & Alexander Khrebet. (2022, August 17). Suicide missions, abuse, physical threats: International Legion fighters speak out against leadership's misconduct. The Kyiv Independent [9,11]. Retrieved from https://kyivindependent.com/
2. Bendett, S. (2023, July 20). Roles and Implications of AI in the Russian-Ukrainian Conflict. Center for a New American Security [30,5]. Retrieved from https://www.cnas.org/
3. Dave, P., & Dastin, J. (2022, March 14). Exclusive: Ukraine has started using Clearview AI's facial recognition during war. Reuters [53,57]. Retrieved from https://www.reuters.com/
4. Hockenhull, J. (2022, November 7). How open-source intelligence has shaped the Russia-Ukraine war. UK Strategic Command Speech, GOV.UK [4,59]. Retrieved from https://www.gov.uk/
5. Osadchuk, R. (2024, July 9). AI tools usage for disinformation in the war in Ukraine. DFRLab [66,62]. Retrieved from https://dfrlab.org/
6. Reuters. (2023, October 24). Members of the Siberian Battalion of Ukraine's Armed Forces International Legion attend military exercises. Thomson Reuters/Context [84]. (Image)
7. Smith-Boyle, V. (2022, June 22). How OSINT has shaped the war in Ukraine. American Security Project [1,75]. Retrieved from https://www.americansecurityproject.org/
8. War Room – U.S. Army War College. (2025, April 26). Artificial Intelligence's Growing Role in Modern Warfare [51,72]. Retrieved from https://warroom.armywarcollege.edu/
9. Wikipedia. (2025). International Legion of the Defence Intelligence of Ukraine [6,8]. Retrieved from https://en.wikipedia.org/wiki/International_Legion_of_the_Defence_Intelligence_of_Ukraine

 doi:10.20944/preprints202510.0414.v1