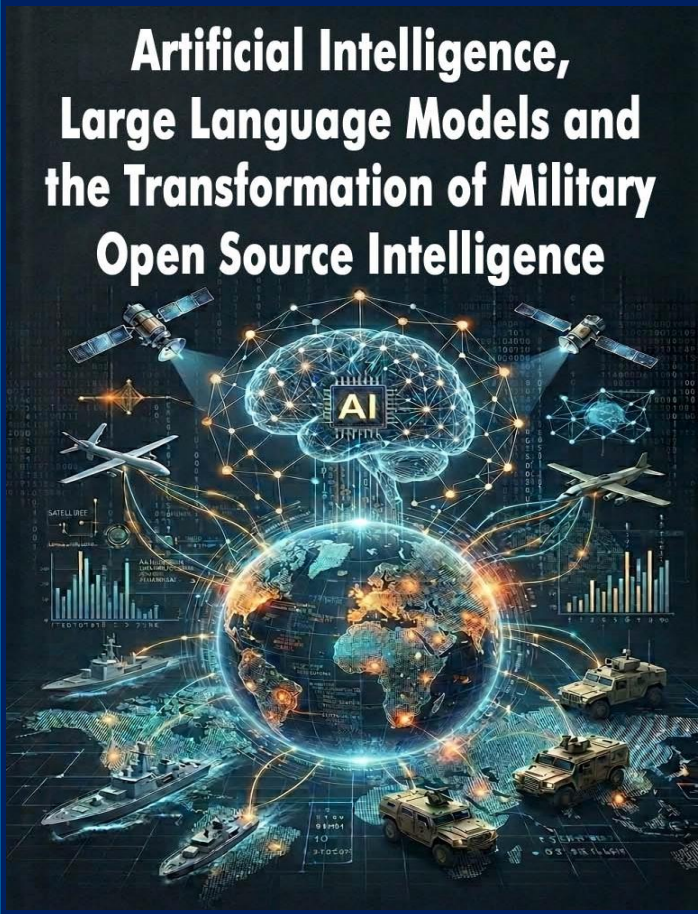
USI Occasional Paper

No 5 - 2026

(Estd. 1870)

Artificial Intelligence, Large Language Models and the Transformation of Military Open Source Intelligence



Major General PK Mallick, VSM (Retd)

About the Occasional Paper

This occasional paper examines the joint United States-Israel air campaigns-Operations Epic Fury and Roaring Lion-against Iran and analyses their strategic, operational, and doctrinal implications for contemporary warfare. The study explores the political and military objectives of the campaigns, the pursuit of air superiority through intelligence-led targeting, the role of integrated air and missile defence systems, and the increasing influence of Artificial Intelligence (AI) in planning and execution. It assesses the effectiveness and limitations of air power, intelligence, and manned–unmanned teaming, while highlighting the evolving character of conflict in an era of multi-domain operations. Drawing lessons from the successes and shortcomings of all participants, this paper identifies critical implications for India's air defence architecture, command and control systems, intelligence integration, force protection, and theatre command structures. It argues that future military advantage will depend increasingly on networked systems, doctrinal coherence, AI-enabled decision support, and anticipatory adaptation.

Introduction

Open-Source Intelligence (OSINT) has long been a major source of intelligence for the Intelligence Community (IC). OSINT refers to the collection, analysis and dissemination of intelligence derived from publicly available information sources. This includes newspapers, television broadcasts, academic publications, government reports, satellite imagery, social media platforms, blogs, podcasts, online forums and commercial databases. In the digital age, the exponential growth of online information has transformed OSINT from a supplementary intelligence discipline into a central pillar of national security, military strategy, law enforcement, cybersecurity and geopolitical analysis.

The advent of Large Language Models (LLMs) has transformed OSINT with far more advanced and dynamic intelligence capabilities. The challenge for intelligence agencies is no longer the lack of information but rather the overwhelming volume of data. This is where LLMs have become revolutionary.

The military implications of this transformation are immense. Modern warfare increasingly depends on information superiority rather than merely kinetic superiority. Recent conflicts demonstrate that the battlefield awareness is now shaped as much by social media feeds, satellite

imagery, commercial drone footage and online narratives as by classified intelligence systems. LLMs enable militaries to fuse disparate streams of open-source information into coherent situational awareness in near real time.

Today, OSINT accounts for between 70 and 90 per cent of all contemporary intelligence material.[1]

This paper examines how LLMs are fundamentally transforming the OSINT cycle—from collection and processing to analysis and dissemination—with particular focus on military intelligence applications.

The Evolution of Open-Source Intelligence

OSINT is not a new phenomenon. Military commanders throughout history have relied on publicly observable information to understand adversaries.

During the Second World War, governments systematically exploited open and available information through monitoring foreign broadcasts and publications. During the Cold War, OSINT expanded to include academic, commercial and satellite-derived information. The internet revolution remodelled OSINT by making information globally accessible in real-time. Social media platforms and commercial satellite imagery further enhanced

intelligence collection, enabling both state and non-state actors to conduct sophisticated analysis.

Why Large Language Models Matter

Traditional OSINT workflows relied on Boolean searches, keyword alerts, scraping scripts, web scrapers, Really Simple Syndication feeds and traditional Application Programming Interfaces (APIs). It produces vast but raw, unstructured datasets from open sources, social media, darknet forums and registries. This labour-intensive process created latency, often delaying tactical insights. Thus, critical localised open-source chatter from conflict zones may remain unreviewed for hours or days.

LLMs are advanced Artificial Intelligence (AI) systems trained on massive datasets containing books, articles, websites, social media content, code repositories and other textual information.

Pre-LLM Bottlenecks.

- **Scale**. Analysts overwhelmed by excessive volume of material beyond processing capabilities.
- **Language Barriers**. With reliance on English sources; foreign-language monitoring required scarce specialists or is prone to poor-quality machine translation.

- **Slow Synthesis**. Connecting disparate signals (cargo records, satellite data, social media posts) demands time-intensive human effort.
- **Tacit Knowledge**. Analyst intuition is valuable but hard to scale or systematise.

LLMs overcome these constraints as the models are trained on massive datasets, they can translate across dozens of languages, detect patterns, track disinformation and extract structured insights from unstructured sources. LLM-enabled systems can process very large document collections far faster than human analysts, generate near real-time alerts and automate relationship mapping—matching operational tempo in ways human analysts alone cannot.

The comparative table below illustrates the shift clearly: from manual, English-biased, slow synthesis to automated, multilingual, and real-time analysis.

Aspect	Traditi-onal OSINT	LLM-Enhanced OSINT	Key Benefit
Scale	Limited by analyst hours	Processes millions of documents in minutes	Handles data deluge
Language Coverage	Heavy English bias; specialist-dependent	Real-time multilingual translation and analysis	Broader source access
Speed	Hours to days for synthesis	Near real-time alerts and reports	Matches operational tempo
Synthesis	Manual cross-referencing	Automated pattern detection and relationship mapping	Better insight extraction
Unstructured Data	Labor-intensive reading	Automated extraction and structuring	Reduced analyst burden
Hypothesis Testing	Limited by time	Rapid generation and evidence evaluation	Improved decision support
Risks	Human fatigue, bias	Hallucinations, model bias, adversarial gaming	Requires human oversight

Table 1: Traditional vs Large Language Models Open Source Intelligence

Source: Created by author

Transformation of the Intelligence Cycle

Figure 1: The Intelligence Analysis Workflow

Source: The Future of Intelligence Analysis: US-Australia Project on AI and Human Machine Teaming, Special Competitive Studies Project, Sep 2024

Process of Intelligence Analysis. Analysts follow a cyclical workflow in which new information is collected, synthesised and transformed into assessments for decision-makers. AI, particularly LLM models, has the potential to automate many stages of this process.

The Black Box Challenge. A major challenge is the opacity of LLM outputs. Because LLMs function largely as 'Black Boxes', their reasoning is often

difficult to trace. This lack of transparency can undermine accountability, credibility and trust if policymakers cannot understand how conclusions were reached. While foundational models are black boxes, prompt engineering techniques like the chain-of-thought prompting force the model to output its step-by-step reasoning, making it easier for a human analyst to audit the logic.[2]

Retrieval-Augmented Generation. This anchors LLMs by forcing them to cite specific, verifiable vector-database documents. Instead of hallucinating facts from static training data, the model acts as an advanced search-and-synthesis engine, retrieving precise information to ground its responses in verifiable truth.[3,4]

How LLMs Are Transforming the OSINT Intelligence Cycle

Intelligence Cycle Transformation. LLMs are reshaping the intelligence cycle by accelerating every stage—collection, processing, analysis and dissemination. They expand source coverage, ingest and translate data in real time, detect anomalies and generate tailored reports for different audiences. This shifts OSINT from a periodic activity into a continuous intelligence function, strengthening military warning and monitoring.

Key enhancements.

- **Collection**. Persistent monitoring of state media, shipping databases, satellite feeds and social chatter aligned with priority requirements.
- **Processing**. Automated extraction and structuring of unstructured data (emails, chat logs, social media threads) into queryable formats.
- **Analysis**. Pattern discovery, change detection and hypothesis testing across fragmented signals, enabling faster situational awareness.
- **Dissemination**. Rapid report generation, customised for policymakers or specialists, reducing analyst workload.

Practical Integration Architectures

- **Analyst-Augmentation Model**. LLMs act as research assistants for summarisation, translation, extraction and drafting — accelerating workflows while analysts retain control over requirements, evaluation and judgments.

- **Integrated Analysis Environments.** LLMs connect to the knowledge bases and historical data, flagging contradictions providing a thus contextual synthesis.

Human-Machine Teaming

Human-Machine Teaming (HMT) combines human, machines and interdependencies between them. HMT can significantly enhance intelligence collection through OSINT by combining the speed and scale of automated systems with the judgment and contextual understanding of human analysts.

Machines can monitor vast amounts of publicly available information across news media, social platforms, imagery and online forums, quickly filtering noise and identifying patterns, anomalies and emerging trends. Human analysts then assess credibility, interpret intent and distinguish genuine signals from misinformation or deception. Augmenting human weaknesses with machine strengths and vice versa, can form human-machine teams that outperform both humans and machines across many tasks.

HMT makes OSINT more efficient, accurate and actionable, thus enabling the IC to turn fragmented public data into timely and reliable intelligence.[5]

HMT is about designing human-centric systems that acknowledge the capabilities and limitations of both human and technology and achieved the appropriate balance. Trust, transparency and usability are essential for adoption and effectiveness. [6]

HMT involves several models of interaction which are as follows:

Human-in-the-Loop	Human-on-the-Loop	Human-out-of-the-Loop
Humans retain full control over key decisions, with AI offering recommendations or processing support. Common in targeting and surveillance systems. No intelligence report is generated or escalated without strict human analysis and approval.	AI executes certain tasks independently, while humans monitor and retain the ability to intervene. Suitable for time-critical or high-tempo missions.	AI operates autonomously without real-time human supervision, usually in tightly bounded, pre-approved scenarios.

Table 1: Human Control in Artificial Intelligence Systems

Source: Created by author

Enhancing human capability in HMT requires careful balancing of human and technological strengths. While humans excel at dynamic interpretation and decision-making, they are

fallible. AI and autonomous systems offer superior data processing, assimilation and speed, significantly improving accuracy, efficiency and reducing cognitive load when properly integrated.

Perspectives.

- **United States (US)**. Department of Defense integrates HMT into decision-making.
- **China**. Pursues 'Itelligentised Warfare' with AI-enabled platforms.[7]
- **Russia**. Incorporates AI assistants in aircraft like the MiG-35.

Emerging changes in the association between humans and machines have the potential to alter how wars are fought and won, from the tactical to the strategic level. The private sector's research into HMT generates numerous opportunities to accelerate change through dual-use technologies.[8]

No matter how quickly HMT changes warfare, many of the challenges will persist. War fighters still rely on their teammates and will experiences of the fear of failure and death. Adapting more quickly than opponents will remain critical. Achieving political outcomes will still require eliminating a human actor's options or forcing them to change their risk calculus. Comprehensively,

military and political leaders will still have to understand human nature, human decision-making and outcomes created by humanity.

For now, AI should not be a total replacement of human analysts. The 'Expert Intuition' of human analysts in identifying novel connections between disparate pieces of information and in explaining the meaning and potential implications of those connections is currently beyond AI's current capabilities.

As the volume of publicly available information continues to expand, successful intelligence organisations will be those that effectively integrate human expertise with advanced AI systems, creating a synergistic partnership that enhances rather than replaces human judgment.

Military Applications

LLMs in Military Intelligence. The rapid deployment of specialised LLM pipelines has completely re-engineered command-and-control assumptions. LLMs addresses the fundamental bottleneck that has historically limited OSINT's contribution to military intelligence: the gap between the volume of available information and the capacity of human analysts to exploit it.[9] This has created the conditions for AI and LLMs to emerge as essential tools. For military intelligence, these capabilities offer

rapid multilingual processing of massive datasets, automated reporting, real-time monitoring, pattern detection and predictive analysis.[10]

OSINT in Modern Conflict. Recent conflicts in Ukraine and Iran have demonstrated OSINT's transformative potential. It has highlighted the role of independent analysts using satellite imagery, geolocation techniques and social media to track troop movements, identify equipment losses and verify battlefield events, often faster than official intelligence channels. This democratised intelligence production, enabling civilians and researchers to contribute meaningfully to battlefield awareness. Smaller states and non-state actors can now also access tools once exclusive to major intelligence agencies, fundamentally redistributing intelligence power.

Operation Epic Fury. According to open-source reporting during the first twenty-four hours of Operation Epic Fury, US forces struck more than 1,000 discrete targets across the Islamic Republic of Iran. This unprecedented scale and tempo of destruction was made possible by the US military's Maven Smart System, overseen by Palantir and powered by Anthropic's Claude AI. By simultaneously processing massive volumes of drone footage, commercial satellite imagery, telemetry pings and Human Intelligence (HUMINT) reports, the AI

identified hundreds of targets, issued precise geographic coordinates and prioritised them based on strategic value and immediate threat.[11]

Speed Implications. LLM-enabled OSINT dramatically accelerates intelligence production, generating actionable insights from open sources within minutes. This speed enhances targeting and crisis response but also challenges traditional command-and-control processes, requiring commanders and staffs to rapidly absorb, assess and act on intelligence products in fast-moving operational environments.

Real-Time Battlefield Awareness. AI-enhanced OSINT combines data from civilians, soldiers, drones and satellites to identify targets, assess damage, track logistics and geolocate imagery, enabling dynamic battlefield mapping and near real-time situational awareness for commanders.

Predictive Intelligence. By analysing historical data, social media activities, economic indicators, shipping patterns, satellite imagery and political discourse, AI may identify indicators associated with increased likelihood of military activity. Indicators such as increased logistics activity, fuel stockpiling, troop leave cancellations and rising nationalist rhetoric can be linked to provide early warning of escalation.

Large Language Models at Tactical, Operational and Strategic Level

Tactical Applications. At the tactical level, LLM-enabled OSINT systems can monitor battlefield developments, analyse adversary narratives, detect troop movements through publicly shared imagery and identify emerging threats through digital chatter. Brigade and battalion headquarters previously dependent on higher-echelon intelligence products for OSINT-derived information can now conduct organic, real-time open-source collection relevant to their areas of interest. This holds particular significance for operations in complex information environments—urban terrain, operations among populations, hybrid or grey-zone operations—where locally generated open-source material is often more operationally relevant than products derived from national-level collection systems.

Operational Applications. At the operational level, AI-driven OSINT supports strategic planning by identifying trends in geopolitical behaviour, economic vulnerabilities, technological developments and public sentiment.

Strategic Applications. At the strategic level, LLMs enable nations to conduct information warfare and narrative management with unprecedented precision and scale.

The Command Dilemma. If a tactical battalion is running its own organic LLM-OSINT pipeline, how can the 'Analytical Drift' be prevented—where a tactical commander acts on locally generated AI insights that contradict the broader strategic assessment produced by higher-echelon agency systems?

Bandwidth and Edge Computing. In a contested electronic warfare environment, cloud-reliant commercial AI may break down. There is a vital need for edge-deployed, lightweight, quantised LLMs that can run locally on ruggedised tactical hardware without an internet connection.

Strategic Implications. At every level—tactical, operational and strategic—LLMs reshape how militaries achieve information superiority. Yet significant risks accompany these gains: hallucinated assessments, amplified bias, deepfakes, synthetic information operations and the erosion of human judgement through over-reliance on AI outputs. Ethical and legal questions concerning privacy, surveillance and accountability remain unresolved, demanding careful governance as these capabilities mature.

How OSINT has been utilised in the current conflicts is given in Appendix.

Risks, Failure Modes and AI-Enabled Deception

Failure Modes. LLM-enabled OSINT introduces critical failure modes that can compromise intelligence accuracy and operational security.

Automation Bias. This bias leads analysts to over-trust AI-generated intelligence because it appears objective and authoritative without adequate verification. LLMs can amplify confirmation bias by preferentially generating outputs that align with an analyst's preconceptions.

Source Laundering. It exploits LLMs' ability to synthesise information from many sources, making it impossible to trace final claims back to primary sources.

False Confidence. This emerges from LLMs' confident presentation style—even when entirely wrong, they deliver answers with unwavering certainty, misleading analysts about reliability.

Adversarial Prompt Injection. It exploits hidden instructions embedded in open-source content to manipulate LLM behaviour, potentially bypassing safeguards, distorting intelligence assessments, exposing sensitive information and undermining AI-assisted collection and analysis systems.

Data Poisoning. It involves attackers injecting malicious training data and false information into the information environment, systematically corrupting LLM intelligence outputs over time and creating persistent vulnerabilities that remain undetected until critical operations fail.

Human Oversight. LLMs should be viewed as intelligence-support tools rather than autonomous analysts. Effective OSINT will continue to require human judgment, source validation, cross-checking and structured analytic techniques to mitigate these failure modes.

Artificial Intelligence-Enabled Deception in the Open Source Intelligence Era

AI-Enabled Deception. LLMs have fundamentally transformed OSINT by enabling sophisticated, scalable deception operations that previously required large human teams. AI can generate fake documents, manipulated imagery, synthetic social media activity and fabricated data patterns. These deceptive artefacts can mislead intelligence collectors and distort analytical conclusions.[12] This AI-enabled deception ecosystem now poses critical challenges for intelligence analysts attempting to distinguish genuine information from manufactured narratives.

Synthetic Personas. LLMs now generate realistic online identities with photographs, biographies, posting histories and social media interactions. These personas can infiltrate online communities, build credibility over time and influence discussions. They can be used to spread misleading narratives and manipulate public opinion while appearing authentic.[13]

Deepfake Operations. Generative adversarial networks can now generate videos, audio recordings and images that convincingly depict events that may have never occurred. Visual deepfakes (audio, photos and videos) are increasingly used to legitimise fake accounts.[14]

Narrative Flooding. Adversaries can generate massive volumes of AI-produced content to overwhelm the information environment. Analysts are increasingly struggling to distinguish reliable information from noise.[15]

Automated Disinformation. Generative AI creates thousands of customised phishing emails tailored to individual targets' interests extracted from social media. This significantly expands the reach and effectiveness of influence operations.[16]

Implications for Intelligence. The intelligence challenge is now undergoing a shift from information collection to information verification. Future OSINT

effectiveness will depend on source authentication, provenance tracking and deception-detection capabilities. The competition between AI-enabled intelligence collection and AI-enabled deception is likely to become a defining feature of future intelligence operations.

Multimodal Intelligence and All-Source Fusion

All-Source Intelligence Fusion. The true significance of LLMs lies not merely in their ability to enhance OSINT, but in their potential to serve as integrative platforms for all-source intelligence fusion. Future intelligence systems will increasingly combine information from multiple intelligence disciplines, with AI acting as the tool for synthesising, processing and connective layer that correlates diverse data streams into coherent assessments.

Intelligence Disciplines. Intelligence is often described in terms of the methods used in its collection, the gathering of different kinds of data through a variety of methods.

HUMINT. This includes running agents and interrogations. This is the most ancient form of espionage, but it can also support or be supported by Technical Intelligence (TECHINT).[17]

Signals Intelligence (SIGINT). It includes communications intelligence from radios, phones and digital networks and electronic intelligence from radars and other emissions.

Geospatial Intelligence (GEOINT). It combines imagery intelligence from satellites and aircraft with cartographic analysis.

Measurement and Signature Intelligence (MASINT). It is the scientific analysis of acoustic, geophysical, chemical, biological, radiological, nuclear and electromagnetic signals.

Cyber Intelligence and Social Media Intelligence. They further expand the information ecosystem by providing insights into cyber activities, online behaviour and digital influence operations.

Financial Intelligence and TECHINT. LLMs analyse financial open-source data alongside classified financial intelligence and process technical intelligence from equipment captures using open-source technical manuals.

AI as the Integrator. LLMs serve as a connective layer across all intelligence disciplines — correlating SIGINT intercepts with open-source reporting, grounding GEOINT imagery analysis in social media geolocation, cross-referencing HUMINT debriefs against publicly available information and processing MASINT signatures against open technical literature.

The Agentic AI Workflow. This automatically chains specialised agents across all Intelligence, delivering fused operational pictures from single prompts with auditable source trails.[18]

The Future of Intelligence. In this environment, LLMs function as cognitive integrators that connect disparate intelligence sources, identify hidden relationships and generate actionable insights. The future of military intelligence is not simply 'LLMs and OSINT' but, AI-enabled all-source intelligence fusion, where machine-assisted synthesis provides a comprehensive and dynamic understanding of the operational environment.

Agentic Artificial Intelligence Systems

The next evolution beyond LLM-assisted OSINT is the emergence of Agentic AI systems. By combining reasoning, planning, memory and tool-use capabilities, agentic AI can operate as a semi-autonomous intelligence assistant that continuously monitors information environments and adapts collection strategies in response to emerging developments. Agentic AI can produce contextualised, hypothesis-driven assessments tailored to decision-maker timelines and risk tolerance, enabling faster, more adaptive situational awareness across domains.[19]

Frameworks such as Google's Agent2Agent architecture and tools like GeoSeer demonstrate the growing use of multi-agent AI systems that autonomously coordinate tasks, analyse data and accelerate intelligence workflows. Although fully autonomous military intelligence systems remain limited and require substantial human oversight, the trend is toward increasingly automated pipelines in which analysts' transition from intelligence producers to supervisors who are responsible for validation, oversight and final judgment.

However, the increasing autonomy of these systems also raises concerns regarding transparency, accountability, reliability and the risk of automated errors influencing operational decision-making. Agentic AI systems demand robust audit trails, explainability mechanisms and secure architectures to prevent manipulation or compromise.

Most defence and intelligence organisations are expected to adopt a human-on-the-loop model, in which agentic AI performs routine collection and analysis tasks while human analysts retain responsibility for oversight, validation and final intelligence judgments.[20]

The Technologies Used for Intelligence Integration

While LLMs have transformed the exploitation of textual information, modern battlefields generate vast quantities of imagery, video, audio, geospatial and sensor data that cannot be effectively analysed through text alone. Modern military intelligence is transitioning from text-centric OSINT to multimodal intelligence fusion, integrating diverse AI modalities for comprehensive operational pictures. This convergence enhances situational awareness while reducing analyst cognitive overload.[21]

LLMs act as the cognitive layer that synthesises intelligence from disparate sources, generating natural language summaries and enabling conversational intelligence queries. Multimodal LLMs combine natural language understanding with spatial reasoning for geospatial tasks.[22]

Computer vision automates detection and classification of military assets in satellite imagery and drone footage. AI algorithms analyse images for object detection, facial recognition and military vehicle identification. This eliminates the limits of review and counters manual image review bottlenecks.[23]

Geospatial AI combines satellite data with machine learning to detect temporal changes in terrain, infrastructure development, troop deployments and activities across space and time.[24]

Speech-to-text systems convert broadcasts, intercepted communications, speeches and social media videos into searchable text. They facilitate rapid linguistic analysis and real-time intelligence extraction.[25]

Video analytics processes live surveillance feeds, automatically tracking targets, identifying behaviours, detecting operational indicators within vast volumes of footage and detecting anomalies.

This integration creates synergistic intelligence. Computer vision identifies tank formations, geospatial AI tracks movement routes, speech-to-text transcribes communications, processes video analytics for monitoring destinations and LLMs synthesise coherent assessments. This transforms military command architectures for real-time decision-making. The future of military OSINT lies in multimodal AI systems capable of delivering comprehensive, and near-real-time situational awareness across the battlespace.

Strategic Implications

The adoption of LLMs in OSINT is reshaping military competition by significantly lowering the barriers to intelligence exploitation. The growing role of commercial technology firms in satellite imagery, cybersecurity and AI analytics is also blurring the distinction between civilian and military intelligence capabilities.

The gap between open source and classified intelligence is shrinking. The meaning of unclassified must be reassessed. It is significant for an environment in which publicly available data, aggregated and processed at large scale, can generate intelligence effects traditionally associated with classified collection. Intelligence now is being built lawfully, commercially and outside the frameworks designed to govern it.

The widespread use of LLMs introduces significant challenges. Security concerns arise when sensitive intelligence-related data is processed through commercial AI platforms that may retain or use submitted information. Consequently, many defence organisations are developing sovereign or air-gapped AI systems. This large-scale aggregation of publicly available data can create detailed personalised profiles. This raises important concerns as privacy, legal and human rights issues despite the information being publicly accessible.[26]

The recent restriction of commercial satellite imagery during an active conflict and the US response to its use, are two public signs that the market now produces significant intelligence inputs that were once associated primarily with state controlled systems.

If commercial imagery providers are already delaying or restricting the release of conflict-zone imagery to reduce adversary exploitation, commanders should assume that the observable signature of operations is itself part of the contested battlespace. Commanders and their staff should treat aggregation risk as a core planning consideration. Legal review must be given due importance. The questions must be raised about data sourcing, vendor reliance, analytic methods and integration into operational workflows.[27]

The US imposed sanctions on three Chinese firms for allegedly providing satellite imagery and related support to Iran, which enabled Iran's military strikes on American forces in the Middle East, as Washington ramps up efforts to restrict technological support for Tehran in the conflict.

China's Meentropy Technology (Hangzhou) Co., The Earth Eye and Chang Guang Satellite Technology Co., were named by the US in its list of entities and individuals assisting Iran, a few of which were based in Belarus and the United Arab Emirates.

Meentropy Technology, known as MizarVision, published open-source images detailing US military activity during Operation Epic Fury, while The Earth Eye provided satellite imagery to Iran. Chang Guang collected data on US and allied military forces at Tehran's request, according to the public statement.[28]

Information Warfare

Modern conflict now significantly extends into the information domain. LLMs enable information warfare by generating or shaping strategic narratives, analysing public sentiment, detecting hostile disinformation and countering adversary messaging. At the same time, adversaries can exploit the same technologies for propaganda, psychological operations and influence campaigns, making the information domain an increasingly contested battlespace.

Ukraine used OSINT to develop anticipatory intelligence; shift public sentiment, counter Russian propaganda, provide a platform for the population to actively participate in passing battlefield information, and offer alternative views through crowdsourced information and fill in missing pieces. All this was likely corroborating intelligence collected from sensitive sources.

Operation Epic Fury demonstrated that modern warfare extends beyond physical battlefields into the cyber and cognitive domains, where the objective is to influence perceptions, decision-making and public behaviour. In the conflict's opening phase, Iran experienced near-total internet disruption, severely restricting communications which created an information vacuum. Exploiting this environment, US and allied cyber forces reportedly conducted psychological operations aimed at undermining regime authority. Some open-source reports alleged that the Iran's BadeSaba religious application was hacked and compromised to disseminate messages encouraging military defections and civilian resistance to deliver directly to millions of users. Simultaneously, Iranian state media platforms were reportedly disrupted and their broadcasts manipulated to disseminate adversarial narratives.

Geospatial AI enhanced these operations by analysing app telemetry and location data to identify concentrations of regime supporters and military personnel, thus, enabling synchronised cyber, cognitive and kinetic effects. Iran's weakened response relied largely on decentralised cyber proxies and hacktivist groups, which used AI-assisted tools to conduct low-level cyberattacks, illustrating how AI has lowered barriers for pursuing cyber warfare and information operations.

Ethical and Legal Issues

The integration of AI and autonomous systems into defence systems must comply with legal obligations, ethical standards and International Humanitarian Law. Central to this approach is the principle of Meaningful Human Control (MHC), which ensures that humans remain responsible and accountable for decisions, including the use of lethal force. Achieving MHC requires transparent AI design, rigorous testing and validation, effective human oversight and clear command structures. Its objectives include maintaining safety, precision, accountability, human dignity, democratic legitimacy and institutional stability. The United Kingdom Ministry of Defence's Joint Service Publication 936 provides guiding principles for the responsible use of AI tools and uphold autonomy, emphasising transparency, accountability and human supervision.

Defence organisations must address challenges such as biases in training data, adversarial manipulation and the risk of unintended escalation to ensure AI systems operate safely, ethically and in accordance with established norms and laws.[29]

The organisations that will derive the greatest operational benefit from LLM-enabled OSINT will be those that integrate these capabilities thoughtfully, preserving human judgement at the critical points in the analytical cycle where it remains indispensable,

while leveraging machine-speed processing for the collection and synthesis tasks that have historically constrained the OSINT function.

Role of Private Sector

The Economist stated on the possibilities from OSINT: 'There are websites which track all sorts of useful goings-on, including the routes taken by aircraft and ships. There are vast searchable databases. Terabytes of footage from phones are uploaded to social media sites every day, much of it handily tagged'.[30]

States increasingly rely on commercial organisations for satellite imagery to monitor hostile troop movements, assess adversaries' military capabilities, evaluate damage from munitions and analyse environmental changes for tactical and strategic advantage.

The private sector plays an increasingly important role. Private space companies are now capable of performing tasks previously exclusive to governments. Commercial satellite companies like Maxar, Planet or BlackSky are not just launching satellites into space but also collecting from around the world and producing analyses from their imagery and data.

The satellite constellation provides frequent revisits of much of the Earth's surface. This vast amount of data is uploaded to the cloud and processed using sophisticated computer algorithms. These algorithms can analyse images, identify changes over time and extract valuable insights, such as patterns and trends.

OSINT has become a major high-tech industry. Private sector companies have capitalised on the growth of smartphones, advances in deep learning and affordable cloud computing. However, OSINT pricing models have become prohibitively expensive for large-scale government use across intelligence and defence agencies.

Governments worldwide are increasingly purchasing commercial satellite data. It includes the effective utilisation of commercial satellite images from Maxar for Battle Damage Assessments and information warfare during Operation Sindoor. It must also be noted that Public data may not be sufficient enough to answer all questions.

Comparative National Approaches

US.

- The Office of the Director of National Intelligence and the Central Intelligence Agency (CIA) released their IC OSINT Strategy in Mar 2024[31] reflecting the growing intelligence value of public and commercial data and emphasising data acquisition, collection management, innovation and workforce/tradecraft development**.**

- The Defence Intelligence Agency OSINT Strategy 2024–28 explicitly calls for integrating AI/ML into OSINT collection, processing and reporting. It promotes a unified, enterprise-wide approach to maximise the value of OSINT across the defence ecosystem. By integrating diverse open-source data—such as social media, commercial imagery and public reports—the strategy aims to enhance decision-making for policymakers and military leaders. The initiative underscores innovation, interoperability and workforce development to ensure timely, actionable intelligence.[32]

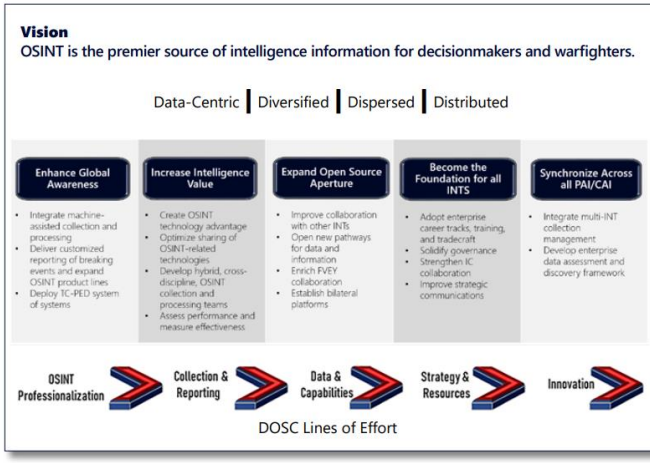


Figure 2: Defence OSINT Strategy 2024-28

Source: OSINT STRATEGY 2024–28, US DoD, 23 Oct 2023 available at: https://www.dia.mil/Portals/110/Documents/OSINT-Strategy.pdf

China: Civil-Military Integration and Technical Exploitation.

- China's approach to LLM-enhanced OSINT is closely integrated with its Military-Civil Fusion strategy, which combines the efforts of the military, government, academia, state-owned enterprises and private technology firms. The People's Liberation Army (PLA) leverages a vast Science and Technology Intelligence network and a growing ecosystem of research organisations, universities and commercial companies to collect process and analyse open-source

information. The PLA views OSINT as a critical intelligence discipline and employs advanced technologies to exploit massive volumes of publicly available data. [33,34]

- Chinese military researchers have developed concepts and patents for systems that fuse OSINT with traditional intelligence disciplines, including HUMINT, SIGINT, GEOINT, TECHINT and MASINT, enabling comprehensive intelligence support across the entire intelligence cycle. The PLA extracts information from foreign governments, militaries, universities, think tanks, defence industries, media organisations, social media platforms, commercial databases, satellites and online forums. This information provides insights into foreign military capabilities, doctrines, technologies, force structures, exercises, deployments and decision-making processes.[35]

- OSINT supports PLA activities at the strategic, operational and tactical levels. Strategically, it informs about assessments of political, economic, technological and military trends. Operationally, it assists in understanding adversary intentions, command structures and force coordination.

Tactically, it provides information on deployments, order of battle, weapons systems and battlefield conditions. Beyond intelligence analysis, OSINT contributes to long-range maritime surveillance, crisis warning, precision strike support, counter-propaganda efforts, military training and technological innovation.

- The PLA has already integrated generative AI models, including DeepSeek AI, across a range of non-combat functions. According to an analysis by the cybersecurity and intelligence company called Recorded Future, patents show that the PLA is deploying models for various intelligence tasks, including OSINT report generation, processing of SIGINT data and event extraction.[36]

- The PLA's collection priorities include AI, hypersonics, quantum technologies, cyber and electromagnetic warfare, unmanned systems, foreign naval capabilities and armoured platforms. Attention is devoted to the military capabilities of countries such as the US, Taiwan, India, Japan, Australia, South Korea, Germany, the United Kingdom, France and Russia. Through diverse procurement

methods and extensive institutional participation, China has developed one of the world's most comprehensive military OSINT ecosystems.

Russia. Russian doctrine views information environments as an asymmetric battlespace. Rather than focusing heavily on processing technical data, Russia's use of LLMs is heavily optimised for Active Measures—cognitive warfare, psychological operations and narrative disruption.[37] Russia has shifted from traditional social media propaganda to 'LLM Grooming'—flooding the internet with low-quality disinformation designed to be scraped by AI.

Israel.

- According to media reports, the Israel Defence Forces—specifically its elite cyber and SIGINT wing, Unit 8200—approaches AI and LLMs as direct tactical decision-support tools. Israel's focus is on integrating LLMs into mass surveillance architectures to drastically compress the time between data collection and target acquisition.[38]
    - Israel's Unit 8200 is running custom ChatGPT-style models on live intercepts, trained on vast collections of Palestinian communications to understand spoken Arabic, with reservists from

Google/Meta/Microsoft leading development.[39]

All the three nations recognise generative AI as a double-edged sword. While it enhances their OSINT capabilities, they also fear adversaries using AI to create convincing inauthentic content that degrades intelligence value.[40]

China, Russia and Israel approach this technology through entirely different doctrines, aligning LLMs with their distinct national security priorities: China focuses on scale, technical intelligence and civil-military data harvesting; Russia leverages LLMs for cognitive warfare and large-scale narrative manipulation, while Israel employs specialised AI pipelines for target generation and multi-sensor intelligence fusion.

Indian Context

There is little information available in the open domain about the Indian IC's use of OSINT. Indian intelligence agencies are remarkably coy about their activities, including OSINT. It is not known which intelligence agencies are using OSINT for their intelligence purposes. OSINT is not about using apps, googling, or commercially available OSINT engines.

US IC is exploiting OSINT. The Indian IC would do well to study those and create its own organisation, lead agency and sharing mechanism.

For example, several Intelligence agencies would require OSINT. They are: The Research and Analysis Wing, National Investigation Agency, Intelligence Bureau (IB), National Technical Research Organisation (NTRO), Defence Intelligence Agency, Central Bureau of Investigation, Narcotics Control Bureau, Financial Intelligence Unit, Enforcement Directorate, Central Board of Direct Taxes, Central Board of Indirect Taxes and Customs, Directorate of Revenue Intelligence, and Directorate General of Goods and Services Tax Intelligence.

The leading agency may be NTRO or IB. An organisation like Open-Source Enterprise of the US may be created under the OSINT Functional Manager, directly under the supervision of NTRO or IB, as the case may be. The chain of information sharing and the procedures can be worked out subsequently.

Issues on Integration of Large Language Models into Military Intelligence

Military intelligence cannot fully rely on commercial AI for classified operations due to fundamental security and operational limitations. Commercial

LLMs trained on public OSINT excel at open-source analysis, but using external APIs risks exposure of classified data through excessive data exposure vulnerabilities and traffic sniffing. The questions that arise are[41]:

Can military Intelligence Rely on Commercial AI? Only with strict safety measures. Civilian commercial models may exhibit behaviours, especially those unwanted in the military context, such as hallucinations or political bias. The military must develop its own LLMs rather than adopt commercial ones if generative AI is truly to be embraced, while addressing concerns over protecting sensitive information and preventing model tampering.

Can Classified Data be Exposed Through External APIs? Yes, it is a critical vulnerability. Routing sensitive queries through commercial APIs exposes inference patterns, metadata and potentially content to foreign-hosted infrastructure, creating unacceptable counterintelligence risks. The National Telecommunications and Information Administration report of the US identifies dual-use foundation models as posing serious security risks.[42]

Should Countries Develop National Foundation Models? Strongly recommended. Defence deployments often occur in highly restricted environments where sovereign control over data and

infrastructure is maintained. Military and intelligence agencies are increasingly exploring sovereign AI architectures based on nationally controlled foundation models operating within secure, air-gapped environments. Such systems allow governments to retain control over training data, model updates, security standards and legal accountability while reducing dependence on foreign technology providers.[43]

Both the US and China are developing military-specific or sovereign LLMs for defence applications, including OSINT, intelligence analysis and secure military communications.

Both the US (Defence LLAMA) and China (ChatBIT) have adapted military LLMs for OSINT and secure military communication.

What should be Air-gapped or Sovereign? All classified information, such as Intelligence, Surveillance, and Reconnaissance feeds, operational orders, raw intelligence and mission logs, must remain air-gapped. Commercial LLMs lack native access control and zero-trust features for classified environments. Air-gapped LLMs deployed on classified networks can support intelligence analysis without transmitting data outside secure environments. At the same time, sovereign AI does not imply complete technological isolation; commercial models may still be useful for

unclassified research and OSINT exploitation. The strategic challenge is therefore to establish a layered architecture in which sensitive intelligence processing remains sovereign and protected, while less-sensitive analytical tasks can benefit from the innovation and scale of commercial AI ecosystems.[44]

Recommendations

For military intelligence communities, the central challenge is now institutional rather than conceptual. The technology and data exist and the requirement is evident. What remains is to build doctrine, training, validation standards and technical pipelines that allow LLMs to accelerate open-source collection without eroding the evidentiary discipline on which reliable intelligence ultimately depends.

Key recommendations includes:

Technical.

- **Invest in Verification Mechanisms.** Robust validation systems are essential to counter misinformation and AI hallucinations. Human review mechanisms must remain embedded within intelligence workflows.

- **Enforce source attribution disciplines.** All intelligence products derived from LLM synthesis must maintain explicit

linkage to the source material from which they were generated. Retrieval-augmented generation architectures should be the standard for operational OSINT systems, ensuring that analytical outputs can be traced to and verified against specific source documents.

- **Strengthen Cybersecurity.** AI systems themselves will become strategic targets. Protecting training data, algorithms and intelligence networks is essential.

- **Formal methods and neuro-symbolic hybrids.** Pairing LLM intuition with symbolic reasoning, constraint solvers and knowledge bases will reduce hallucinations and improve explain ability for high-stakes assessments.

- **Foundational Models.** Nation states must develop their own foundation models operating within secure, air-gapped environment.

Doctrinal.

- **Develop Adversarial Resilience**. Doctrine and training should explicitly address the vulnerabilities of LLM-dependent OSINT architectures to

adversarial manipulation, information poisoning and prompt injection. If an LLM automatically scrapes a hostile forum, a hidden piece of text on that forum could execute an injection attack, blinding the model or manipulating its summarisation output. Red team exercises should routinely test the susceptibility of operational LLM pipelines to these attack vectors.

Training.

- **Preserve Foundational Tradecraft**. LLM adoption should not be permitted to result in the attrition of manual OSINT skills in the analyst workforce. Training programmes should maintain proficiency in manual source identification, evaluation, translation and synthesis as a baseline capability, recognising that LLM-dependent workflows will be degraded or unavailable in some operational contexts.

- **Enhance AI Literacy**. Military leaders and intelligence personnel must understand AI capabilities and limitations to make informed operational decisions.

Organisation.

- **Invest in Sovereign LLM Capability**. Commercial LLM services are inappropriate for military OSINT processing. Defence establishments should invest in developing and deploying classified-network LLM infrastructure, operated under appropriate security protocols, to support the full range of OSINT collection tasks without creating data-handling vulnerabilities.

- **Unified AI-enabled Intelligence Ecosystems**. Military organisations should establish unified AI-enabled intelligence ecosystems integrating OSINT, SIGINT, GEOINT and cyber intelligence into interoperable platforms.

- **Promote International Norms**. Global discussions on military AI governance should address misinformation, autonomous systems and AI-enabled influence operations.

Legal and Ethical.

- **Update Legal and Ethical Frameworks**. Governments should create legal and ethical guidelines governing AI-enabled intelligence collection, surveillance and information operations. Legal review processes for

intelligence collection and targeting must be updated to explicitly address LLM-generated analytical products. Data protection impact assessments should be carried out for OSINT collection systems incorporating LLM processing capabilities.

Conclusion

Clausewitz said: "A great part of information obtained in war is contradictory, a still greater part is false and by far the greatest part is somewhat doubtful. What is required of an officer in this case is a certain power of discrimination". Clausewitz warned against attempting to reduce warfare to a crude 'Algebra of Action'. One should resist all attempts to reduce intelligence to formulaic calculation. Intelligence is not Boolean algebra. Intelligence analysis is fundamentally uncertain, characterised by incomplete, ambiguous and often contradictory snippets of partial, unreliable information.[45]

Former National Security Agency and CIA Director Michael Hayden once said, "If it were a fact, it wouldn't be intelligence". Intelligence analysis operates in a realm of uncertainty, focusing less on facts and more on assessing competing claims, assumptions and probabilities. Analysts interpret ambiguous and incomplete information to understand complex realities. It is impossible to fill

every so-called intelligence gap. Intelligence analysts are more concerned with nuance, judgment and with hunches, intuition or a 'Gut Feeling', or what we might call tacit or implicit knowledge.[46]

These nuanced judgments, which lie between certainty and speculation, remain difficult for generative AI systems to evaluate reliably.

Intelligence is adversarial. Intelligence analysis is not a neutral field of academic research. Intelligence is a deeply adversarial political activity directed primarily against rival states. Because of its inherently antagonistic nature, intelligence is a discipline mired in lies.

Despite technological advances, intelligence remains fundamentally a human endeavour. AI systems lack intuition, cultural understanding, moral judgment and strategic wisdom. Human analysts provide contextual interpretation, challenge assumptions and understand political nuance in ways machines cannot fully replicate.

Intelligence analysis is inherently vulnerable to deception, as adversaries actively conceal, distort and manipulate information. Analysts must distinguish genuine information from false or misleading data, much like solving a puzzle with missing and counterfeit pieces. It is not data science, where accurate information can often be obtained

through sound methodology. The rise of AI-generated content further increases the risk of deception and complicates accurate assessments.

Intelligence is also uniquely focused on understanding the decisions of a small number of key political and military leaders. Predicting individual behaviour is difficult because human decisions are shaped by personal experiences, cultural influences, biases, fears and irrational factors. Effective intelligence analysis depends not only on data but also on deep expertise in the history, language, culture and psychology of foreign actors and societies.

OSINT has long been regarded as a major contributor to intelligence production. Developments in machine learning, data mining, visual forensics and the growing computing power available for commercial use have enabled OSINT practitioners to speed up and sometimes even automate, intelligence collection and analysis, obtaining more accurate results more quickly. As the infosphere expands to accommodate ever-increasing online presence, so does the pool of actionable OSINT. These developments raise important concerns regarding governance, ethical, legal and social implications. New and crucial oversight concerns appear alongside standard privacy concerns, as some of the more advanced data analysis tools require little to no supervision. [47]

The most significant consequence of LLM-enabled OSINT may not be faster intelligence production but the erosion of traditional intelligence monopolies. Capabilities once restricted to major intelligence services are increasingly available to smaller states, private companies, non-state actors and even individuals. As barriers to intelligence exploitation continue to fall, competitive advantage will depend less on access to information and more on the ability to validate, fuse and act upon it faster than adversaries.

The future of intelligence is not human versus machine, but human-machine collaboration. Successful intelligence agencies will combine Human expertise, AI-enhanced LLM-driven automation, verification, Domain knowledge, Ethical oversight and human decision-making.

Training future intelligence professionals will require hybrid skills combining data science, geopolitics, psychology, linguistics and military strategy. Intelligence agencies will possess a decisive advantage in the rapidly evolving information environment of the 21st Century. In an era of information abundance, that combination of machine scale and human insight is what separates noise from signal, data from intelligence.

Appendix

OSINT in Ukraine War

The Russia-Ukraine War has highlighted the importance and impact of OSINT within wider intelligence and security analysis, the benefits of weaponising intelligence to wage information warfare and the criticality of multisensor or intelligence Processing, Exploitation and Dissemination supported by AI.

OSINT has been pivotal in the Russia-Ukraine War, supporting conflict tracking, intelligence gathering and de-mining efforts. Before the invasion, investigators used OSINT to monitor the Russian military build-up. OSINT provided Russia's military build-up before the invasion of Ukraine in 2022. Ukraine has effectively leveraged social media platforms like Instagram and TikTok to locate Russian forces and track naval deployments and hardware losses, aided by civilian and formal groups. Crowdsourced reporting, combined with commercial satellite imagery and computer vision models, has enabled near real-time situational awareness. Geographic Information System software has guided de-mining by identifying unexploded ordnance zones.

Satellite imagery, including Synthetic Aperture Radar technology, has been instrumental in observing Russian activities, such as pontoon bridges during the Kherson retreat and new defensive positions along the M14 highway. High-resolution images also exposed the damage from Ukrainian drone strikes inside Russia.

However, only states have access to the most compeling evidence, such as intercepts of Russian war plans and indicators that Russia was moving blood plasma to the front lines at a crucial moment in mid-Jan 2022.

It is misleading to regard open and classified sources as entire separate intelligence domain. Public estimates of losses of Russian military equipment in Ukraine appear to be pretty accurate. But public data is often most useful and revealing when it is fused with non-public or secret information. Bridging the unclassified and the classified data is both technically and institutionally difficult.

Ukraine used OSINT to develop anticipatory intelligence; shift public sentiment; counter Russian propaganda; provide a platform for the population to actively participate in passing battlefield information, offer alternative views through crowdsourced information and fill in missing pieces, likely corroborating intelligence collected from sensitive sources.

Beyond mobilising Ukrainians, Ukrainian President Volodymyr Zelenskyy's digital strategy reached a global audience, transforming Ukraine into a symbol of resistance. This global sympathy reshaped political priorities worldwide, influencing policy shifts even in distant nations like Japan and Australia. Germany's decision to send tanks to Ukraine, breaking 75 years of foreign policy tradition, underscores the profound international impact of Ukraine's narrative.[48]

The single most important repository of data during the war has been Telegram. In early 2022, Telegram experienced a significant surge in users due to Russia's restrictions on Western-owned social media platforms following the onset of the Ukraine conflict. User numbers in Russia grew from 25 million in Jan to 41.5 million by Jul, with 13 million joining between Feb and Mar, 2022. Telegram became an effective tool for both communication and information dissemination. Telegram's rise created a valuable OSINT resource, with numerous channels providing insights into Russian sentiment and attitudes toward the war.

OSINT has been pivotal in countering Russian narratives and aiding Ukraine's defence. It debunked Putin's invasion claims and empowered Ukraine to track Russian military movements through data from civilians and soldiers' posts. The

intelligence's value led to the creation of Diia, an app that manages contributions from external OSINT volunteers and analysts, underscoring its critical role in modern conflict.

Endnotes

---

[1] Riccardo Ghioni, Mariarosaria Taddeo, and Luciano Floridi, "Open Source Intelligence and AI: A Systematic Review of the GELSI Literature", *AI & Society* 39, no. 4 (2024): 1827–1842, accessed 20 May 2026, https://doi.org/10.1007/s00146-023-01628-x

[2] William Usher et al., *The Future of Intelligence Analysis: U.S.-Australia Project on AI and Human-Machine Teaming* (Arlington, VA: Special Competitive Studies Project, and Canberra: Australian Strategic Policy Institute, Sep 2024), accessed 20 May 2026, https://www.scsp.ai/wp-content/uploads/2024/09/AI-The-Future-of-Intelligence-Analysis-SCSP-ASPI-Report.pdf

[3] "LLMs and GenAI in Digital Scholarship: Retrieval Augmented Generation (RAG)", accessed 20 May 2026, https://researchguides.case.edu/GenAI/RAG

[4] Patrice Béchard and Orlando Marquez Ayala, "Reducing Hallucination in Structured Outputs via Retrieval-Augmented Generation", in *Proceedings of the 2024 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies (Volume 6: Industry Track)* (Mexico City: Association for Computational Linguistics, 2024), 228–238, accessed 21 May 2026, https://aclanthology.org/2024.naacl-industry.19/

[5] "Human-Machine Teaming: Enhancing Decision-Making & Operational Agility in Defence (Thales, Aug 2025)", accessed 20 May 2026, https://www.thalesgroup.com/sites/default/files/2025-08/2025.06.08%20Thales%20HMT%20whitepaper%20designed%20FINAL.pdf

[6] Anna Knack, Richard J Carter, and Alexander Babuta, "Human-Machine Teaming in Intelligence Analysis: Requirements for Developing Trust in Machine Learning Systems", *CETaS Research Report* (London: Centre for Emerging Technology and Security, The Alan Turing Institute, Dec 2022), accessed 20 May 2026, https://cetas.turing.ac.uk/sites/default/files/2022-12/cetas_research_report_-_hmt_and_intelligence_analysis_vfinal.pdf

[7] Maj Gen P K Mallick, VSM (Retd.), "Defining China's Intelligentized Warfare and Role of Artificial Intelligence", (New Delhi: Vivekananda International Foundation, Mar 2021), accessed 20 May 2026, https://indianstrategicknowledgeonline.com/read_book.php?fnam=defining_china_intelligentized_warfare_and_role_of_artificial_intelligence.pdf&tnam=PKPaper

[8] Tate Nurkin and Julia Siegel, "Battlefield Applications for Human-Machine Teaming: Demonstrating Value, Experimenting with New Capabilities, and Accelerating Adoption", Atlantic Council, Aug 2023, accessed 20 May 2026, https://www.atlanticcouncil.org/wp-content/uploads/2023/08/Battlefield-Applications-for-HMT.pdf

[9] Riccardo Ghioni, Mariarosaria Taddeo, and Luciano Floridi, "Open Source Intelligence and AI: A Systematic Review of the GELSI Literature", *AI & Society* 39, no. 4 (2024): 1827–1842, published online 28 Jan 2023, accessed 21 May 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC9883130/pdf/146_2023_Article_1628.pdf

[10] Tomislav Dokman and Tomislav Ivanjko, "Open Source Intelligence (OSINT): Issues and Trends", in *INFuture 2019: Knowledge in the Digital Age* (Zagreb: Faculty of Humanities and Social Sciences, University of Zagreb, 2020), accessed 21 May 2026, https://openbooks.ffzg.unizg.hr/index.php/FFpress/catalog/download/39/51/2033-1

[11] Adam Simmons, "The New Battlespace: How Geospatial AI Is Reshaping Military Intelligence", *Project Geospatial*, 12 Mar 2026, accessed 21 May 2026, https://projectgeospatial.org/geospatial-frontiers/the-new-battlespace-how-geospatial-ai-is-reshaping-military-intelligence

[12] Mark Finlayson and Azwad Anjum Islam, "Weaponized Storytelling: How AI Is Helping Researchers Sniff Out Disinformation Campaigns", FIU News, 29 May 2025, accessed 21 May 2026, https://news.fiu.edu/2025/weaponized-storytelling-how-ai-is-helping-researchers-sniff-out-disinformation-campaigns

[13] "The Synthetic Disinformation Boom: AI and the Collapse of Trust", *Institute for Strategic Risk and Security*, 06 Nov 2025, accessed 21 May 2026, https://www.isrs.ngo/fpb/the-synthetic-disinformation-boom-ai-and-the-collapse-of-trust

[14] Matthew Miller, Deepfakes: Real Threat, KPMG, 2025, accessed 21 May 2026, https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2025/deepfakes-real-threat.pdf

[15] Ibid

[16] "The Role of AI in Social Engineering," zvelo, 08 Nov 2023, accessed 22 May 2026, https://zvelo.com/the-role-of-ai-in-social-engineering/

[17] Emelia Probasco, Helen Toner, Matthew Burtell, and Tim G J Rudner, "AI for Military Decision-Making: Harnessing the Advantages and Avoiding the Risks", *Center for Security and Emerging Technology*, Apr 2025, accessed 22 May 2026, https://cset.georgetown.edu/publication/ai-for-military-decision-making/

[18] Charlotte Brown, "Signals in Sync: OSINT, HUMINT, SIGINT, GEOINT in the Modern Intelligence Environment", *Mattermost*, 28 Oct 2025, accessed 22 May 2026, https://mattermost.com/blog/signals-in-sync-modern-intelligence-environment/

[19] Christopher Wissuchek and Patrick Zschech, "Exploring Agentic Artificial Intelligence Systems: Towards a Typological Framework", *arXiv*, 07 July 2025, accessed 21 May 2026, https://arxiv.org/pdf/2508.00844

[20] "Agentic AI: Does the Future of Warfare Look Autonomous?", *The Soufan Center*, 06 Aug 2025, accessed 22 May 2026,

https://thesoufancenter.org/intelbrief-2025-august-6/

[21] Adam Simmons, "The New Battlespace: How Geospatial AI Is Reshaping Military Intelligence", *Project Geospatial*, 12 Mar 2026, accessed 22 May 2026, https://projectgeospatial.org/geospatial-frontiers/the-new-battlespace-how-geospatial-ai-is-reshaping-military-intelligence

[22] Long Yuan, Fengran Mo, Kaiyu Huang, Wenjie Wang, Wangyuxuan Zhai, Xiaoyu Zhu, You Li, Jinan Xu, and Jian-Yun Nie, "OmniGeo: Towards a Multimodal Large Language Models for Geospatial Artificial Intelligence", *arXiv*, 20 Mar 2025, accessed 22 May 2026, https://arxiv.org/abs/2503.16326

[23] Rina Diane Caballar and Cole Stryker, "What Is Computer Vision?", *IBM Think*, accessed 22 May 2026, https://www.ibm.com/think/topics/computer-vision

[24] "Geospatial Intelligence and AI: Defense and Government Applications", *Digital Divide Data*, accessed 23 May 2026, https://www.digitaldividedata.com/blog/geospatial-intelligence-and-ai-defense-and-government-applications

[25] The Applications of AI in Natural Language Processing, Computer Vision, and Speech Recognition, *NASSCOM FutureSkills Prime*, accessed 23 May 2026, https://www.futureskillsprime.in/blogs/applications-ai-natural-language-processing-computer-vision-and-speech-recognition/

[26] Aaron Conti, "Built, Not Stolen: How Commercial Data Is Changing Intelligence", RealClearDefense, 04 Jun 2026, accessed 23 May 2026, https://www.realcleardefense.com/articles/2026/06/04/built_not_stolen_how_commercial_data_is_changing_intelligence_1186667.html?utm_source=substack&utm_medium=email

[27] Ibid

[28] Julia Fioretti, "US Sanctions Chinese Satellite Imagery Companies over Iran War", *Bloomberg*, 09 May 2026, accessed 23 May 2026, http://bloomberg.com/news/articles/2026-05-09/us-sanctions-chinese-satellite-imagery-companies-over-iran-war

[29] *UK Ministry of Defence, Defence Artificial Intelligence Strategy*, Jun 2022, accessed 23 May 2026, https://assets.publishing.service.gov.uk/media/62a7543ee90e070396c9f7d2/Defence_Artificial_Intelligence_Strategy.pdf

[30] "Open-Source Intelligence Challenges State Monopolies on Information", *The Economist*, 07 Aug 2021, accessed 21 May 2026, https://www.economist.com/briefing/2021/08/07/open-source-intelligence-challenges-state-monopolies-on-information

[31] *Office of the Director of National Intelligence*, *Intelligence Community OSINT Strategy*, Mar 2024, accessed 23 May 2026, https://static.carahsoft.com/concrete/files/3917/3887/7500/Strategy_Intelligence_Community_OSINT_Strategy.pdf

[32] *US Department of Defense*, *OSINT Strategy 2024–2028*, 23 Oct 2023, accessed 23 May 2026, https://www.dia.mil/Portals/110/Documents/OSINT-Strategy.pdf

[33] Zoe Haver, "Private Eyes: China's Embrace of Open-Source Military Intelligence", *Recorded Future*, 01 Jun 2023, accessed 24 May 2026, https://assets.recordedfuture.com/insikt-report-pdfs/2023/ta-2023-0601.pdf

[34] Philip Ingram, "Inside China's Hidden OSINT Networks Shaping the Future of Intelligence Warfare", *Karve International*, 29 Apr, 2025, accessed 24 May, 2026, https://www.karveinternational.com/insights/inside-chinas-hidden-osint-networks

[35] Zoe Haver, *Private Eyes: China's Embrace of Open-Source Military Intelligence* (Recorded Future, 01 Jun, 2023), accessed 24 May 2026, https://www.recordedfuture.com/research/private-eyes-chinas-embrace-open-source-military-intelligence

[36] "Agentic AI: Does the Future of Warfare Look Autonomous?", *The Soufan Center*, 06 Aug 2025, accessed 24 May 2026, https://thesoufancenter.org/intelbrief-2025-august-6/

[37] SIMKRA, "Understanding Russian Cognitive Warfare COA", *Medium*, 02 Apr 2025, accessed 24 May 2026, https://medium.com/h7w/understanding-russian-cognitive-warfare-7ef978afa087

[38] Noor Hammad, "The Proliferation of AI-Enabled Military Technology in the Middle East", *International Institute for Strategic Studies (IISS)*, 02 Apr 2026, accessed 24 May 2026, https://www.iiss.org/online-analysis/charting-middle-east/2026/04/the-proliferation-of-ai-enabled-military-technology-in-the-middle-east/

[39] Harry Davies and Yuval Abraham, "Revealed: Israeli Military Creating ChatGPT-Like Tool Using Vast Collection of Palestinian Surveillance Data", *The Guardian*, 06 Mar 2025, accessed 24 May 2026, https://www.theguardian.com/world/2025/mar/06/israel-military-ai-surveillance

[40] Zoe Haver, *Artificial Eyes: Generative AI in China's Military Intelligence* (Recorded Future, 17 Jun 2025), accessed 24 May 2026, https://assets.recordedfuture.com/insikt-report-pdfs/2025/ta-cn-2025-0617.pdf

[41] Sarah Logan, "Tell Me What You Don't Know: Large Language Models and the Pathologies of Intelligence Analysis", *Australian Journal of International Affairs* 78, no. 2 (2024): 220–228, published 31 May 2024, accessed 24 May, 2026, https://www.tandfonline.com/doi/full/10.1080/10357718.2024.2331733

[42] US Government Accountability Office, "Spectrum IT Modernization: NTIA Should Fully Incorporate Cybersecurity and Interoperability Practices", GAO-25-107509, 22 May 2025, accessed 25 May 2026, https://www.gao.gov/products/gao-25-107509

[43] Jay Meil, "LLMs Alone Aren't Fit for Military and Intelligence Operations", SAIC, accessed 25 May 2026, https://www.saic.com/blogs/four-reasons-llms-alone-arent-fit-for-military-and-intelligence-operations

[44] Ibid

[45] Zachery Tyson Brown, "The Incalculable Element": The Promise and Peril of Artificial Intelligence, *Studies in Intelligence* 68, no. 1 (Mar 2024), accessed 25 May 2026, https://www.cia.gov/resources/csi/static/643e18ba5bf779749a14059019db53b2/Article-The-Promise-and-Peril-of-Artificial-Intelligence-Studies-68-1-March-2024.pdf

[46] Ibid

[47] "What Percentage of Intelligence Comes From Open Sources?", *LegalClarity*, accessed 25 May 2026, https://legalclarity.org/what-percentage-of-intelligence-comes-from-open-sources/

[48] Jean-Marc Rickli and Federico Mantellassi, "The War in Ukraine: Reality Check for Emerging Technologies and the Future of Warfare", *Geneva Paper* 34/24, The Geneva Centre for Security Policy, Apr 2024, accessed 25 May 2026, https://www.gcsp.ch/publications/war-ukraine-reality-check-emerging-technologies-and-future-warfare

About the Author

Major General PK Mallick, VSM (Retd) is an Electronics and Telecommunication Engineering graduate from Bengal Engineering College (now the Indian Institute of Engineering Science and Technology), Shibpur, and holds an MTech from the Indian Institute of Technology, Kharagpur. Commissioned into the Corps of Signals of the Indian Army, he has held a wide range of command, staff and instructional appointments during a distinguished military career. He has operational experience in Operation RAKSHAK (Punjab), Operation RHINO (Assam) and Operation RAKSHAK in Jammu and Kashmir. A prolific defence author, he has published six books: The History of the Corps of Signals (Vol. IV), China in Cyber Domain, Information, Cyber and Space Domain: Its Application in Future Land Warfare, Offensive Cyber Operations (OCO): A 360 Degree View, Mind Wars: The New Battlefield of Information Warfare, and The Profession of Arms: A Guide for Young Army Officers.

About the United Service Institution of India (USI)

The USI was founded in 1870 by a soldier scholar, Colonel (later Major General) Sir Charles MacGregor 'For the furtherance of interest and knowledge in the Art, Science and Literature of National Security in general and Defence Services, in particular'. It commenced publishing its Journal in 1871. The USI also publishes reports of its members and research scholars as books, monographs, and occasional papers (pertaining to security matters). The present Director General is Vice Admiral Sanjay J Singh, SYSM, PVSM, AVSM, NM, PhD (Retd).

(Estd. 1870)

United Service Institution of India (USI)
Rao Tula Ram Marg, Opposite Signals Enclave,
New Delhi-110057
Tele: 2086 2316/ Fax: 2086 2315,
E-mail: dircpl@usiofindia.org

₹ 250