

Evolution in Open-Source Intelligence and Coercive Limitations in Contemporary Conflicts

Lessons for India

Rajnish Maahi*

This article argues that open-source intelligence (OSINT) has become a central, structural element of contemporary intelligence practice and strategic competition, particularly in environments characterised by persistent rivalry and rapid information flows, including that of India. The central research question explored here is: how has the transformation of OSINT driven by technological innovation and evolving conflict dynamics reshaped its role from a peripheral support function to an indispensable instrument in informational warfare and crisis management, and what are the implications for countries like India operating in contested and transparent security environments? OSINT has undergone extensive transformation in the last 20 years, mainly due to the advent of new technologies. Today, tools like AI-powered text analysis, large social network studies, commercial satellite images, ongoing location tracking and automated data combining have changed how public information is gathered, checked and used. These tools have taken OSINT beyond just watching the media to become a key part of what is called informational warfare, where competition and conflict happen constantly in both mental and physical arenas, often without official war being declared. In today's world, with many powerful

* Col Rajnish Maahi, SM, is a serving officer with over 26 years of combat, staff and instructor experience and is pursuing PhD at the Special Centre for National Security Studies, Jawaharlal Nehru University, New Delhi, India.

countries, states live in a state of negative peace, marked by ongoing pressure, influence campaigns, battles over stories and occasional military actions. This pattern is seen in all modern conflicts, which undertake operations across many areas, both physical and non-physical, to reach their goals. Military success now depends not just on winning on land, sea, air, cyber or space, but also on shaping people's perceptions, gaining legitimacy and influencing decisions in the information and mental areas. Recent wars have shown that OSINT, when used with modern technology, often gives an insight into the earliest signs of enemy plans and rising tensions, and helps in gaining the upper hand. The Ukraine war shows how connected civilian, government and commercial OSINT groups can create real-time awareness and strategic messaging benefits when systems for checking and combining information are in place. This article looks at global OSINT methods considering these technology and strategy changes, focusing on how advanced tools and organisational set-ups have helped intelligence groups adjust to ongoing competition. The research adopts a comparative case study approach, combining global organisational analysis with focused examination of the Indian experience. The rationale for this design is two-fold: first, a comparative framing enables structured analysis of how different states and alliances institutionalise OSINT and respond to persistent competition; second, the selection of Indian cases (specifically, the operations of Uri and Balakot, the subsequent information-focussed campaign of Operation Sindoor, and the evolution of data integration with the National Intelligence Grid—NATGRID) allows for an in-depth look at how a regional power adapts OSINT practices in a transparent, contested security environment. Case selection is guided by the objective of tracing the operationalisation of OSINT across different types of crises (cross-border strike, air operation, information management and data fusion initiatives) and their relevance in shaping India's intelligence adaptation. The article concludes that, for the Indian Armed Forces, making OSINT a formal part of their work is no longer optional but is closely tied to future operations across multiple areas. The real value of OSINT is not just having access to open data, but in the organised ability to turn technology-driven information into reliable intelligence in a setting of ongoing, low-level conflict.

Keywords: Informationalised Warfare; OSINT; Multi-domain Operations; Negative Peace; Cognitive Domain; Intelligence Fusion; Radical Transparency

INTRODUCTION: MODERN ERA OF INFORMATION DOMINANCE, PERSISTENT COMPETITION AND OSINT

Intelligence has changed less because secrets have disappeared and more because there is now an overwhelming amount of information openly available.

Unlike during the world wars, when open-source intelligence (OSINT) was mostly about reading newspapers, listening to foreign broadcasts or studying academic work and served as an auxiliary input,¹ today it operates in a world full of digital traces. Social media, commercial satellites, global financial records, mobile devices and sensors produce constant streams of public data worldwide in real-time, which can be accessed quickly and cheaply. This is the Information Age, different from the past not just because of the huge amount of information available but also because of technologies that can quickly and widely find meaning in it, something that was impossible earlier. Tools such as AI-powered text analysis, machine translation, image recognition, location tracking and network analysis have made OSINT a highly technical intelligence practice, not just a side analytics tool. OSINT today does not replace traditional intelligence methods like human espionage or sensitive information gathering. Instead, it supports them by providing early warnings, background understanding and publicly verifiable insights that improve overall intelligence, proving that intelligence advantage continues to be achieved by combining many sources rather than relying on just one in the Information Age. Contemporary technological advancements have coincided with a significant shift in global conflict dynamics. Today, power competition is constant and multifaceted, extending beyond traditional warfare to political, economic, informational and technological arenas, often in the absence of outright hostilities. This reflects Johan Galtung's concept of negative peace, where overt war is absent but persistent pressure, instability and rivalry endure. Modern conflict is less about direct confrontation and more focussed on shaping perceptions, legitimacy and influence particularly through information operations that blur the lines between peace and war, civilian and military, domestic and international spheres.²

For example, rather than short, decisive wars, states now employ limited, targeted actions and sustained influence campaigns, as seen in India–Pakistan relations and the drawn-out nature of the conflicts between Ukraine and Russia, Israel and Hamas and the United States and Iran. In these ongoing conflicts, intelligence organisations must not only provide early warnings of war but also continuously interpret evolving narratives, intentions and threats across both traditional and information domains.³ OSINT has thus become essential in this environment. Because information and perceptions circulate rapidly in the public domain, OSINT provides early signals of escalation, limitations and opportunities often faster than secret sources or classified channels. The primary conceptual shift is that information, rather than secrecy, has become the primary arena of strategic competition. As a

result, intelligence advantage now depends on the ability to extract meaning from open information to influence, anticipate and manage ongoing contests, making OSINT structurally central to understanding and responding to contemporary conflicts.⁴ Contemporary multi-domain operations are now extending beyond land, sea, air, cyber and space into the information and cognitive domains, where perception, legitimacy and narrative coherence are shaping strategic outcomes.⁵ In such operations, open-source information frequently provides the earliest indicators of intent, escalation and constraint. The speed at which narratives form in the public domain often outpaces classified collection cycles, rendering OSINT not supplementary but foundational to situational awareness.

The conflict between Russia and Ukraine served as the first major illustration of how OSINT technologies have been effectively weaponised, especially by a less conventionally potent nation state to yield operational outcomes.⁶ For instance, commercially available satellite imagery has been employed to reveal force mobilisation, battlefield developments and even war crimes in near real-time. Recent conflicts, including the ongoing and longest conflict between these two nations, underscore the power of open-source intelligence when formal and informal ecosystems are in place to provide rapid validation, contextualisation and dissemination. Where such institutional mechanisms were absent, open information remained noise; where they existed, OSINT became intelligence. This continuity of competition also implies that crises are not isolated global events, but moments within ongoing geopolitical and geo-economic strategic interactions, which are analysed near real-time using techniques like crowdsourcing on commercially available information.

India's security environment also exhibits many of the same characteristics of persistent competition, albeit in a distinct geopolitical context. Enduring rivalry with Pakistan and China, along with episodic military confrontations and continuous information contestation, mark the sub-continental strategic space. Operations such as the surgical strikes following the Uri attack, the Balakot air strikes after Pulwama and Operation Sindoor in the aftermath of Pahalgam, along with the subsequent phases of escalation management, unfolded not only across extended physical theatres but within a densely mediated information environment. Publicly available imagery, social media discourse and open-source assessments rapidly framed narratives of success, proportionality and intent, influencing domestic legitimacy and international perception alike. In highly polarised societies, where national sentiment is easily mobilised, these open information flows became integral

to escalation dynamics rather than peripheral commentary. Once analytically analysed, these experiences underscore that present and future Indian military operations will be conducted under conditions of radical transparency, in which open information will simultaneously constrain operational discretion while presenting significant intelligence opportunities.⁷

Hence, pragmatic though delayed at the institutional level, India has begun to recognise the importance of data integration through recently operationalised initiatives such as the National Intelligence Grid (NATGRID), designed to enable cross-agency access to diverse datasets. Though NATGRID is not an OSINT platform per se, as it primarily ingests closed government databases rather than public web data, its underlying logic reflects a broader shift towards fusion-centric intelligence architectures. The analytical question, therefore, is not whether OSINT should be used, but how intelligence institutions adapt their methodologies, structures and cultures to exploit open information effectively within an environment of continuous multi-domain competition.⁸

This article situates OSINT within this transformed strategic and technological landscape with relevance to the Indian sub-continent. Instead of treating OSINT as a discrete discipline, it approaches it as an epistemic layer that reshapes how intelligence is generated, validated and acted upon in contemporary situations. By examining global OSINT methodologies and drawing analytical lessons through Indian experiences, the article seeks to illuminate how open information, when combined with appropriate technologies and institutional practices, has become central to intelligence in an age of negative peace and informationalised warfare. In analytical terms, OSINT should be understood not as a source of coercive power, but as a medium through which coercive signals are constructed, transmitted and interpreted.

Evolution of OSINT Methodologies: From Peripheral Inputs to Core Intelligence Function

Open-source intelligence did not emerge suddenly as a product of the digital age; its contemporary prominence is the outcome of a long, uneven and rapid evolution shaped by changes in media, technology and the organisation of state power. To clarify its development, recent scholarship and RAND Corporation analyses identify three distinct 'generations' of OSINT, each marked by characteristic sources, technologies and organisational roles. The first generation of OSINT, spanning roughly from the early 20th century through the end of the World War II, was characterised by the use of openly

available materials such as newspapers, journals, diplomatic reporting and radio broadcasts. Intelligence organisations primarily used these sources to supplement clandestine collection, especially where direct access to restricted areas was limited. Analytical standards were basic, with open sources often considered inferior to secrets, and validation relied on human judgement rather than systematic procedures.⁹

The second generation, emerging during the Cold War, overlapped with rapid technological growth in signals intelligence, imagery intelligence and covert collection. With the expansion of classified technical collection, OSINT was relegated to a secondary, contextual role. Intelligence agencies developed an institutional bias valuing secrets over open data, investing in classified sensors and secure processing, while open-source exploitation was mainly handled by manual monitoring units with limited analytical authority. Even formal structures such as foreign broadcast monitoring focussed on translation and summarisation without independent assessment. This era was underpinned by the belief that open information merely reflected surface phenomena, while strategic intent lay hidden in classified channels.¹⁰ A third generation of OSINT began to emerge from the late 20th century onwards, particularly after globalisation accelerated and digital information proliferated. The advent of the internet, real-time news and social media dramatically expanded both the quantity and diversity of publicly available data. Crucially, methodological innovation shifted OSINT from passive collection to active pattern analysis across vast datasets. Intelligence value began to move from isolated secrets to observable trends and networks in open information. This period is often called the democratisation of information, as states, militaries and non-state actors increasingly operated in public view, whether deliberately through signalling, or unintentionally via commercial activity, bureaucratic leakage or adaptive social behaviour.¹¹ In India, developments such as the media coverage of the Kargil conflict and the Mumbai terror attacks reflected this shift towards real-time, open-source analysis and highlighted the growing intelligence value of integrated public data.

The decisive methodological shift, however, occurred only when new technologies enabled the systematic exploitation of this informational abundance. Advances in computing power, data storage and algorithmic analysis transformed OSINT from a labour-intensive activity into a scalable intelligence function. Automated web scraping, natural language processing, machine translation and sentiment analysis enabled analysts to process millions of documents across languages and platforms. Social network analysis tools

revealed relational structures that were previously invisible, while computer vision techniques allowed imagery and video to be treated as analysable data rather than illustrative evidence.¹² These capabilities marked a fundamental break from earlier OSINT practices, which depended on selective reading and human intuition.

By the early 21st century, several intelligence communities formally acknowledged this transformation. The United States, for example, institutionalised OSINT through the establishment of the Open Source Centre and later codified it as a distinct intelligence enterprise. Official doctrine explicitly recognised that publicly available information could provide strategic warning, situational awareness and context unavailable through classified channels alone.¹³ The latest OSINT Strategy document 2024–2026 of the Office of Department of National Intelligence (ODNI) reflects a significant doctrinal shift by increasingly treating OSINT as the foundational layer supporting intelligence fusion, strategic warning and decision support rather than as a supplementary collection discipline. Similar developments have occurred within the North Atlantic Treaty Organization (NATO), where OSINT began to be integrated into alliance-wide intelligence and early warning mechanisms, particularly in relation to hybrid threats and information operations.¹⁴ At the same time, divergent models of OSINT exploitation emerged worldwide. Some states pursued centralised approaches, creating dedicated OSINT units with enterprise-wide mandates, while others adopted federated models in which multiple agencies retained OSINT capabilities coordinated through common governance structures. China's approach represented a distinct trajectory, treating open scientific, technical and economic information as a primary intelligence resource and embedding OSINT-like practices within broader state planning mechanisms.¹⁵ Despite these differences, a common methodological convergence became apparent, wherein OSINT was no longer defined by source openness alone, but by the processes of validation, cross-referencing and fusion that transformed raw data into intelligence. China's approach to OSINT diverges structurally from Western institutional models but converges methodologically in its emphasis on integration. Rather than isolating OSINT as a discrete intelligence function, Chinese practice embeds the exploitation of open scientific, technical, economic and geospatial data across state, military and industrial systems. The state-controlled mass surveillance and monitoring of all investments and activities worldwide, including the South China Sea, the Belt and Road Initiative, economic espionage and large-scale data aggregation, reflect a model in which open information directly contributes to strategic

planning. Advances in artificial intelligence and emerging developments in quantum computing further enhance China's capacity to process large volumes of open data, thereby reducing the epistemic divide between open and classified intelligence.

The Ukraine conflict represents the most visible inflexion point in this evolution. For the first time, OSINT methodologies were not only institutionalised within states but also distributed across transnational networks of analysts, journalists and volunteers for operational use in kinetic actions and cognitive targeting. Commercial satellite imagery, geolocated videos and social media posts were aggregated, verified and analysed at a pace that rivalled, and at times surpassed, traditional intelligence cycles.¹⁶ This development did not render state intelligence obsolete; it demonstrated that methodological rigour, transparency of sourcing and speed of analysis could co-exist outside state-controlled classified systems. The broader implication is that contemporary conflicts are progressively eroding the traditional state monopoly over strategic observation. As witnessed during the recent Iran–Israel–US confrontation and the associated disruptions across the Red Sea and Strait of Hormuz between 2024 and 2026, commercially available geospatial imagery, vessel-tracking systems, aviation-monitoring platforms and open-source analytical networks were and are being used extensively to assess military activity, monitor maritime security risks and evaluate escalation dynamics in near real-time. The significance of these developments lies not merely in the visibility of events, but in the emergence of intelligence assessments whose credibility increasingly derives from transparent methodologies, distributed verification and commercially available data rather than from secrecy and state control alone.

For India, this evolution assumes particular significance given the country's position as one of the world's largest generators and consumers of data. India's intelligence architecture, however, was largely shaped in an earlier era when security threats were spatially bounded, episodic and embedded within relatively constrained information environments. Contemporary challenges spanning contested borders, internal security imperatives and information warfare now unfold under conditions of continuous visibility and instantaneous dissemination. The Indian experience since the late 2010s demonstrates that open information has become integral to escalation management, strategic communication and the construction of public legitimacy, rendering OSINT a structural component of modern intelligence rather than a supplementary analytical input. The methodological lesson is not that OSINT can or should replace traditional intelligence, but that

intelligence itself has been reconstituted around information density and analytical integration.¹⁷ Thus, the evolution of OSINT methodologies reflects a broader transformation in intelligence practice, as what began as peripheral monitoring has now become a core function shaped by technology, organisational design and strategic context. Therefore, understanding this evolution is essential for analysing how contemporary intelligence systems operate under conditions of persistent competition and why OSINT now occupies a central place within them.

Global OSINT Methodologies and Organisational Scan: From Collection to Cognitive Advantage

The maturation of OSINT methodologies globally, especially in the present Information Age, has revealed a central paradox, where, on one hand, the availability of open-source data has expanded exponentially for all and sundry, and the intelligence advantage, on the other, can be accrued only by those institutions that are capable of transforming informational abundance into analytical clarity within the shortest possible time. As Manoj Joshi argues in his analysis for the Observer Research Foundation, OSINT's contemporary relevance does not stem from the novelty of sources but from its integration into intelligence workflows that influence decision-making under time pressure.¹⁸ In other words, OSINT succeeds not when it exists, but when it is trusted, fused and acted upon. This insight helps explain why intelligence organisations have increasingly shifted away from viewing OSINT as a discrete collection activity and towards embedding it within broader organisational models. Therefore, contemporary models emphasise organisational proximity to analysts and consumers, ensuring that open-source insights can and do shape assessments rather than merely supplement them.¹⁹

The establishment of the Open Source Centre after the 9/11 attacks and, later, the formalisation of the National Open Source Enterprise, reflected recognition that OSINT required governance, standards and professionalisation comparable to those of classified disciplines in the US. Importantly, the US doctrine does not frame OSINT as an alternative to classified collection, but rather as an enabling layer that enhances warning, context and analytical resilience.²⁰ The federated governance model coordinated through bodies such as the Defence Open Source Council seeks to balance decentralised exploitation with enterprise-wide coherence, ensuring that OSINT informs operational, strategic and policy-level intelligence simultaneously.²¹

NATO's evolving approach also reinforces Joshi's argument that OSINT must be organisationally embedded to generate cognitive advantage. Alliance-level assessments increasingly stress that hybrid threats, disinformation campaigns and grey-zone activities are best detected through open sources precisely because adversaries operate below thresholds that trigger classified intelligence collection.²² However, the NATO experience also highlights persistent barriers, including cultural scepticism towards non-secret sources, uneven analytical tradecraft and limited mechanisms to convert OSINT insights into shared situational awareness.²³ The case being where OSINT remains structurally marginal, it produces volume without influence.

However, Israel's oscillation in OSINT institutionalisation offers a different approach, as it has had a dedicated OSINT unit, Hatzav, since around independence. The temporary disbandment of its dedicated OSINT unit in 2021 reflected an enduring bias towards technology and AI, coupled with classified technical intelligence. Yet subsequent conflicts and intelligence surprises exposed the cost of under-utilising open information, particularly in identifying early indicators of intent and mobilisation visible in the public domain, which led to the unit's revival in 2023 and its expansion post-7 October 2022 Hamas attacks. The re-activation of OSINT capabilities in 2023 signalled an implicit acknowledgement that secrecy and technology alone no longer guarantee insight.²⁴ China's model diverges structurally from the US and NATO but converges methodologically. Rather than isolating OSINT, Chinese intelligence practice treats open scientific, technical and economic information as integral to national power accumulation. By embedding OSINT-like exploitation across state, military and industrial systems, China reduces the epistemic divide between open and classified knowledge.²⁵ On the other hand, India's political and legal context differs substantially, with the analytical lesson that OSINT effectiveness correlates with institutional centrality, not merely with tool availability. The Ukraine conflict demonstrates the outer limits of this transformation. There, OSINT was not confined to state institutions but diffused across transnational networks of analysts whose credibility rested on transparent methodologies, rapid validation and rapid weaponisation. The decisive factor was not access to data, which was universally available, but the ability to synthesise information into coherent narratives that shaped global perception and policy responses.²⁶ For India, these organisational models resonate strongly with recent experiences within its neighbourhood. Operations ranging from Uri through Balakot to Pahalgam, and the subsequent crisis phases, unfolded within an environment where public narratives, open imagery and social

media analysis, including misinformation and disinformation campaigns, shaped escalation dynamics and diplomatic signalling. Indian intelligence and military institutions have been operating under near-instantaneous global scrutiny, underscoring that OSINT is no longer external to operations but embedded within them. The emergence of integrative data architectures such as NATGRID reflects a partial shift towards fusion-centric models. Yet, the broader challenge remains institutional, requiring that open-source analysis be analytically authoritative, professionally trusted and structurally influential.²⁷

Thus, global OSINT methodologies converge on a shared conclusion irrespective of the approaches adopted. Intelligence advantage in the contemporary era does not derive from monopolising information, but from organising and empowering institutions capable of interpreting openly available data faster, more credibly and more coherently than adversaries. As contemporary scholars contend, OSINT is ultimately a test of institutional maturity: whether intelligence systems can adapt to an environment where visibility is constant, competition is persistent, and cognition is contested.²⁸

OSINT IN THE UKRAINE CONFLICT: A METHODOLOGICAL CASE OF INTELLIGENCE UNDER RADICAL TRANSPARENCY

The Ukraine conflict represents the most consequential methodological stress test of OSINT in contemporary warfare. Unlike earlier conflicts, where open-source analysis supplemented classified intelligence in retrospect, Ukraine demonstrated how OSINT could operate *in parallel with*, and sometimes even ahead of, state intelligence processes. The defining feature of this case was not the novelty of sources, many of which had existed for years, but the convergence of advanced technologies, distributed analytical communities and an information environment characterised by radical transparency.²⁹

From the outset of the crisis, publicly available information revealed indicators of forthcoming escalation that traditional intelligence assessments initially debated. Commercial satellite imagery, railway logistics data, social media posts by soldiers and civilians and even traffic congestion patterns provided early signals of Russian force mobilisation.³⁰ These indicators were visible not only to intelligence agencies but to journalists, researchers and independent analysts, illustrating that the informational asymmetry traditionally favouring states had narrowed substantially. The methodological implication was clear: intelligence advantage increasingly depended on analytical speed and synthesis rather than on privileged access. Technological

enablers played a decisive role in this shift. Advances in computer vision enabled analysts to geolocate imagery with precision, while machine translation and natural language processing enabled real-time exploitation of Russian- and Ukrainian-language content at scale. Network analysis tools helped identify coordinated information operations and trace amplification patterns across platforms.³¹ These technologies transformed disparate data points into structured intelligence products, often disseminated publicly with transparent sourcing. The credibility of OSINT analysis in this context rested not on secrecy but on methodological rigour, reproducibility and peer validation.

Equally significant was the organisational dimension, where OSINT during the Ukraine conflict did not reside within a single institutional framework; instead, it emerged from an ecosystem spanning state agencies, think tanks, investigative journalists and volunteer networks across the globe. Groups such as Bellingcat, Palantir and academic-affiliated research teams demonstrated that non-state actors could perform intelligence functions traditionally monopolised by governments.³² This diffusion of analytical capacity challenged conventional notions of authority in intelligence, stating that influence flows from trust in analysis rather than institutional pedigree. However, the Ukraine case also exposed the limits of OSINT when not integrated into decision-making structures. Open-source analysis, on the one hand, generated rapid situational awareness. On the other hand, its strategic impact varied depending on whether state institutions possessed mechanisms to absorb and act on it. In some instances, OSINT reinforced policy decisions by providing publicly defensible evidence, particularly in shaping international opinion and coalition cohesion.³³ In others, its influence was attenuated by bureaucratic inertia or competing classified assessments. This divergence underscores that OSINT effectiveness depends on institutional receptivity, not on analytical brilliance alone.

The conflict further highlighted OSINT's role in cognitive and informational warfare. Visual documentation of battlefield events, civilian suffering and infrastructure damage circulated globally within minutes, thereby shaping narratives and constraining diplomatic manoeuvres. Open-source imagery and video were effectively used not only to inform but to persuade, mobilise and legitimise.³⁴ In this sense, OSINT functioned simultaneously as intelligence and as a strategic communication instrument, blurring the boundary between analysis and influence. The methodological challenge lay in maintaining analytical objectivity amid intense narrative competition. For India, the Ukraine experience offers a powerful analogy

rather than a template. Indian military operations and crises increasingly unfold under comparable conditions of visibility, where open information shapes escalation dynamics and international perception. Episodes such as post-Uri and post-Balakot information cycles revealed how satellite imagery, social media discourse and open-source assessments constrained strategic ambiguity and influenced diplomatic engagement. The Ukraine case suggests that in such environments, the absence of institutionalised OSINT does not preserve secrecy; it merely cedes interpretive space to external actors.³⁵

The central methodological lesson from Ukraine, therefore, is not that OSINT replaces classified intelligence, but that intelligence itself has become inseparable from the open information environment. States that lack mechanisms to validate fuse and contextualise OSINT risk operating reactively within narratives constructed by others. Conversely, those who integrate OSINT into intelligence workflows gain cognitive resilience, the capacity to understand events more quickly, explain them credibly and act with greater strategic coherence. As Indian policymakers consider the implications of OSINT, they must ask themselves what institutional risk threshold justifies delaying OSINT adoption. The answer to this question could define the strategic trajectory of India's intelligence capabilities. In sum, the Ukraine conflict demonstrates that OSINT has matured into a decisive component of intelligence under conditions of radical transparency. Its utility lies not merely in exposing facts but in structuring meaning within contested information spaces. For intelligence systems confronting persistent competition and multi-domain operations, this represents a methodological inflexion point rather than a passing anomaly.³⁶ The Ukraine conflict is analytically distinctive because OSINT was employed symmetrically by both sides, though with markedly different objectives, organisational cultures and levels of effectiveness. Unlike earlier cases where OSINT primarily empowered external observers, in Ukraine, it became an integral component of military cognition, narrative control and escalation management. The conflict, therefore, allows a structured comparison of OSINT employment not merely as a tool, but as a system of intelligence practice operating under conditions of radical transparency.³⁷ The first analytical distinction emerges at the level of purpose. Ukrainian and Russian OSINT employment diverged fundamentally in intent as one prioritised validation, mobilisation and legitimacy, while the other focussed on denial, deception and narrative saturation. This divergence shaped how technologies, platforms and analytical workflows were employed and has valuable lessons in the Indian context.

Table 1 Comparative OSINT Employment in the Ukraine Conflict

Factors	Ukraine	Russia
Primary OSINT Objective	Situational awareness, validation, international legitimacy	Narrative control, obfuscation, information overload
Core OSINT Actors	State agencies, military, civil volunteers, NGOs, journalists	State-linked media, proxy influencers, information operations units
Dominant Platforms	Twitter/X, Telegram, commercial satellite imagery, open databases	Telegram, VK, state media amplification, bot networks
Analytical Orientation	Evidence-driven, transparent sourcing, peer validation	Volume-driven, ambiguity creation, selective disclosure
Integration with Operations	Tactical and strategic awareness, escalation management	Psychological operations, deterrence signalling
Credibility Outcome	High external trust and policy influence	Low credibility, diminishing persuasive power

Note: Author's deduction—OSINT effectiveness correlates more with analytical credibility and validation mechanisms than with control over platforms. Ukraine's OSINT succeeded because it reduced ambiguity; Russia's faltered because it amplified it.³⁸

TECHNOLOGICAL ENABLERS AND ANALYTICAL TOOLS

A second level of comparison concerns technological exploitation. Both sides had access to similar technologies, but their analytical employment differed sharply.

Table 2 OSINT Technologies and Modes of Exploitation

Factors	Ukraine	Russia
Commercial Satellite Imagery	Force tracking, damage assessment, public validation	Selective imagery release, denial of damage
Geo location & Chronolocation	Verification of strikes, troop movements	Occasional use, often undermined by contradictory narratives
Social Network Analysis	Detection of disinformation, tracking mobilisation	Amplification of confusion, bot-driven saturation

Computer Vision	Equipment loss databases, visual verification	Limited transparent use
NLP & Machine Translation	Real-time exploitation of Russian-language content	Primarily propaganda-oriented messaging

Note: Author’s deduction—Technological parity does not translate into analytical parity. OSINT tools amplify underlying institutional intent; they do not compensate for weak tradecraft.³⁹

OSINT ACROSS COGNITIVE AND NON-COGNITIVE DOMAINS

The Ukraine conflict illustrates that OSINT operates simultaneously across non-cognitive (physical, kinetic, spatial) and cognitive (perception, legitimacy, morale) domains, making it central to contemporary multi-domain operations.

Table 3 OSINT across Domains of Warfare

Factors	Ukraine	Russia
Land / Physical	Battle damage assessment, force movement	Open-source strike verification
Cyber	Attribution of cyber incidents	Public linkage of malware campaigns
Space	Satellite imagery analysis	Commercial ISR supplementation
Information	Narrative shaping, legitimacy	Transparent evidence dissemination
Cognitive	Trust-building, alliance cohesion	OSINT-backed diplomatic messaging

Note: Author’s deduction—OSINT functions as a cross-domain integrator, binding kinetic events to cognitive effects. Its strategic value lies precisely in this bridging function.⁴⁰ For India, the Ukraine case yields deduced lessons not templates, as all the Indian military and intelligence operations from Uri through Balakot and Pahalgam and subsequent crises unfolded within similar conditions of public visibility and narrative contestation. As open imagery, social media discourse and external OSINT assessments influenced escalation control and diplomatic signalling in the Indian context as well. In the contemporary security environment characterised by persistent competition and negative peace, OSINT becomes structurally inseparable from intelligence.

INDIAN ANALOGUES: OSINT, NATGRID AND CONFLICT EXPERIENCE UNDER PERSISTENT COMPETITION

India's recent security experience underscores a structural convergence with the conditions that elevated OSINT during the Ukraine conflict: persistent rivalry short of war, episodic kinetic escalation and continuous information contestation. Despite the differing geopolitical contexts, the informational conditions are comparable. Indian military operations since the mid-2010s have unfolded in an environment of near-instantaneous visibility, where open information shapes not only public perception but also diplomatic signalling and escalation control. In such conditions, OSINT ceases to be a peripheral analytical aid and becomes an intrinsic component of intelligence cognition. The analytical lesson is not that OSINT determined outcomes, but that it constrained the space for strategic ambiguity. Indian decision-makers operated within an information environment where open sources could not be ignored without ceding interpretive authority to external actors.⁴¹

This experience aligns with broader transformations, such as contemporary military operations, and with contemporary and future Indian security challenges, whether along contested borders, in maritime domains or within internal security contexts, which will continue to be characterised by prolonged competition rather than discrete wars. Intelligence requirements, therefore, would extend beyond warning of imminent attack to continuous assessment of posture, signalling and narrative. Therefore, OSINT is well-suited to this task because it captures patterns of behaviour that unfolds in public, infrastructure development, troop movements visible through commercial imagery, economic and logistical activity and information operations conducted through digital platforms.⁴²

At the institutional level, India's move towards data integration through the NATGRID reflects an implicit recognition of this reality. NATGRID was conceived to enable authorised agencies to access disparate datasets for counter-terrorism and national security purposes, addressing longstanding stovepipes in Indian intelligence architecture. Though NATGRID is not designed as an OSINT platform and is outside constitutional oversight, its logic fusion, accessibility and timeliness mirror global trends in intelligence modernisation.⁴³ The analytical significance of NATGRID lies less in its specific databases than in its architectural philosophy, which is that intelligence advantage is derived from integration rather than from isolated collection.

However, the Indian experience also reveals the limits of delayed and partial integration. OSINT remains stove-piped under separate users, institutionally

marginal; its exploitation tends to be ad hoc and reactive, often driven by crises rather than embedded within routine, integrated analysis under constitutional oversight. This pattern contrasts with mature OSINT ecosystems, where open-source exploitation is continuous, anticipatory and under constitutional oversight. The consequence is that Indian institutions may find themselves responding to externally generated OSINT narratives produced by foreign think tanks, media outlets or independent analysts rather than shaping them through homegrown, credible and authoritative analysis. The risk here is not misinformation alone, but strategic misinterpretation. Indian conflicts also highlight the cognitive dimension of OSINT. Information flows surrounding military operations influence domestic morale, international legitimacy and adversary perception. In an era of informationalised warfare, these effects are not ancillary as they are constitutive of strategic outcomes. OSINT thus operates across both cognitive and non-cognitive domains, linking physical actions to perceptual consequences. The absence of institutionalised OSINT does not insulate operations from these dynamics, but it merely reduces the state's ability to manage them.

To address these challenges and embed OSINT as a core element of national intelligence, several concrete policy steps can be considered. First, India should establish a dedicated inter-agency OSINT coordination cell at the national level, tasked with routine collection, validation and integration of open-source information across intelligence and security agencies. This unit should operate under clear protocols for data sharing, validation and dissemination to ensure that OSINT insights feed directly into decision-making processes rather than remaining siloed. Second, standardised professional training and certification for OSINT analysts should be developed in partnership with academic and technical institutions, ensuring a skilled workforce equipped to handle sophisticated analytical tools, verification techniques and ethical standards. Third, clear guidelines and oversight mechanisms for the ethical use of open-source data must be instituted to protect civil liberties while maximising operational utility. Fourth, India should foster public-private partnerships with technology firms, academic researchers and civil society organisations to leverage rapidly evolving commercial tools and crowdsourced analytical capacity, mirroring best practices from international OSINT ecosystems. Fifth, to reinforce credibility and support strategic communication, selective public disclosure of validated OSINT findings should become a formal element of crisis management and diplomatic signalling. Collectively, these reforms would move OSINT from its current marginal status to a routinely

institutionalised intelligence capability, strengthening India's resilience in cognitively contested environments.

From an analytical standpoint, the Indian case reinforces a central lesson from global experience: OSINT effectiveness depends on institutional absorption. Tools and data are necessary but insufficient to meet the requirements. What matters is whether open-source analysis is validated, trusted and integrated into intelligence assessments that inform decision-making. Wherever such mechanisms exist, OSINT enhances strategic coherence; where they do not, it exposes states to narrative vulnerability and interpretive dependency.⁴⁴

In sum, India's operational history since Uri demonstrates that OSINT is already shaping the strategic environment, regardless of formal institutionalisation. The challenge, therefore, is not adoption but alignment, where methodologies, structures and analytical cultures align with trained, optimised and professional workforce functions within an environment defined by persistent competition and radical transparency.⁴⁵ This alignment does not require replicating foreign models but it does require recognising that intelligence in the contemporary era is inseparable from the open information domain.

The cumulative evidence from global practice and recent conflicts suggests that the principal challenge confronting intelligence systems today is no longer scarcity of information, but the capacity to impose analytical order on informational abundance. OSINT has emerged as a central instrument in this transformation precisely because it operates at the intersection of visibility, speed and cognition.⁴⁶ For India, the lesson is not that OSINT introduces a novel intelligence function, but that it exposes structural characteristics of intelligence institutions operating under conditions of persistent competition and negative peace. The contemporary multi-domain operations increasingly unfold across cognitive and non-cognitive domains simultaneously. Physical operational and tactical actions, including troop movements, strikes and deployments, now generate immediate informational effects that shape strategic perception, legitimacy and escalation dynamics. OSINT functions as a cognitive integrator by linking observable activity across domains into coherent analytical narratives. Unlike classified intelligence, which is often compartmentalised by source and domain, OSINT inherently cuts across boundaries, connecting economic indicators, social behaviour, geospatial data and information operations in a transnational arena. This integrative quality explains why OSINT frequently provides early indicators of strategic change.⁴⁷ Public logistics movements, commercial satellite imagery, digital

communications and financial signals often reveal intent before it is formally articulated. Where intelligence institutions lack mechanisms to synthesise these signals, they risk strategic lag responding to events after narratives have already solidified.⁴⁸ OSINT thus serves as a test of an institution's capacity to think holistically rather than functionally. Another consistent pattern across OSINT-rich environments is that intelligence advantage accrues not to those with the most data, but to those with the highest institutional absorption capacity.⁴⁹ As absorption, in this context, refers to the ability to validate open information, integrate it with other intelligence streams and translate it into assessments that inform decision-making. This capacity is more organisational rather than technical, as it depends on analyst authority, validation protocols and leadership confidence in open-source products. However, where OSINT remains structurally marginal, intelligence systems exhibit a paradoxical vulnerability; they are exposed to open information but unable to act upon it authoritatively. This condition produces reactive intelligence, in which institutions respond to externally generated interpretations rather than shaping understanding proactively. The implication for India is that partial or informal adoption of OSINT may be more destabilising than its absence, as it creates analytical awareness without decision leverage.

As the Indian security environment continues to operate under conditions of radical transparency akin to those of any nation, it is imperative that the commercial sensors, global media ecosystems and digitally networked, democratically elected public entities monitor military activity and rapidly observe, interpret and contest it as applicable. In such an environment, traditional reliance on strategic ambiguity becomes progressively difficult to sustain. OSINT does not eliminate ambiguity but shifts its locus, requiring ambiguity to be managed through coherence and credibility rather than silence. This transformation has direct implications for escalation control. Open information shapes how actions are perceived by adversaries, partners and domestic audiences alike. Intelligence institutions that fail to account for OSINT dynamics risk misjudging adversary reactions or international responses. Conversely, those who integrate OSINT into assessment frameworks gain a more accurate sense of how actions resonate beyond immediate tactical effects. Negative peace implies competition without closure; therefore, unlike wartime intelligence, which is oriented towards discrete objectives, intelligence under persistent competition must operate continuously, often without clear thresholds for action. OSINT is particularly suited to this environment because it captures incremental change shifts in posture, narrative emphasis, economic signalling and social mobilisation.

These changes rarely trigger classified collection priorities but often precede strategic inflexion points. For India, whose security challenges span borders, domains and time horizons, OSINT offers a means of maintaining strategic continuity in analysis. However, this continuity demands institutional endurance as OSINT cannot be crisis-driven or episodic to sustain its domain relevance. It must be embedded within routine intelligence processes, with dedicated analytical capacity insulated from operational distraction.

Finally, in an environment where adversaries and external actors actively exploit open information, abstention does not confer protection. Instead, it creates a vacuum that others fill with their interpretations. Intelligence institutions that under-invest in OSINT effectively outsource cognitive authority to foreign analysts, media and platforms, thereby handing over the strategic leverage of credibility and narrative shaping in the cognitive domain.⁵⁰ This dynamic is particularly acute for democratic states, where public legitimacy and international perception are intrinsic to strategic outcomes. In the modern-day conflict, OSINT is not a discretionary enhancement but a structural requirement of intelligence in the contemporary era. Its value lies not in technological novelty but in its capacity to discipline perception, anchor analysis in observable reality and sustain strategic coherence under constant scrutiny. The analytical implication for India is not the replication of external models, but the development of institutional mechanisms that enable the validation, integration and authoritative use of open-source information within existing intelligence frameworks. In the absence of such mechanisms, OSINT risks remaining fragmented and reactive, limiting its contribution to strategic coherence and escalation management.

INSTITUTIONALISING OSINT FOR INDIA IN A COGNITIVELY CONTESTED ENVIRONMENT

India's recent military and strategic experience shows that open-source information is now closely tied to how crises unfold, especially in shaping public perception, diplomatic signalling and escalation management. Events such as the post-Uri and Balakot crises occurred in an environment of near-instant visibility, where satellite imagery, media coverage and independent analysis influenced how actions were understood both domestically and internationally. In such conditions, the gap between action and interpretation has narrowed considerably, reducing the scope for controlled ambiguity while increasing the importance of maintaining a coherent narrative. However, this greater visibility has not led to stronger compellence outcomes. Instead, it has

reinforced a pattern in which coercive actions remain limited and episodic, shaped by nuclear deterrence and differing motivations, even as their informational impact grows. The Indian experience, therefore, suggests that OSINT functions less as a tool of coercion and more as a factor that shapes how actions are perceived, debated and stabilised over time.

In this context, the key issue is not simply expanding OSINT capabilities, but understanding how open-source information can be effectively integrated into a contested cognitive environment. Comparative experience offers several broad insights. The United States demonstrates that OSINT becomes strategically useful when integrated into all-source intelligence systems, enabling timely analysis and decision-making. European Union efforts to counter disinformation highlight the importance of verification and transparency in maintaining credibility. China's approach illustrates how integrating open-source analysis across state, military and industrial systems can reduce the gap between open and classified knowledge, though within a different political framework. Israel's experience points to the risks of undervaluing open information, where reliance on classified sources may delay recognition of visible signals. The Ukraine conflict further demonstrates that distributed OSINT networks linking state, commercial and civilian actors can produce rapid situational awareness, but generate strategic impact only when supported by credible validation and interpretation mechanisms. Once integrated at the apex level, these experiences suggest that India's approach can be understood along three broad lines: integrating and institutionalising OSINT into regular inter-agency graded assessment processes; maintaining strong standards of cognitive verification to ensure credibility; and using selective disclosure to support strategic signalling while retaining necessary ambiguity. These elements are most effective when supported by a wider whole-of-nation alignment, involving coordination between state institutions; private platforms, including academia; and societal actors to manage the information environment. As such, this approach may not remove the structural limits of compellence, but it can effectively reduce cognitive vulnerabilities, improve interpretive stability and strengthen coherence in crisis communication in real-time under conditions of persistent rivalry.

CONCLUSION

This article has argued that the rise of open-source intelligence is neither a transient by-product of digital excess nor a substitute for traditional

intelligence disciplines, but rather a structural consequence of the changing character of contemporary conflict and strategic competition. Intelligence environments are no longer defined primarily by opacity, episodic crises and privileged access to information. Instead, they increasingly operate under conditions of persistent visibility, information abundance and continuous strategic interaction below the threshold of war. In such settings, intelligence authority derives less from exclusive possession of information and more from the capacity to identify, validate and interpret what is already observable within the public domain.

The global evolution of OSINT methodologies reveals a notable convergence across diverse political and institutional contexts. Whether through the institutionalised open-source enterprises of the United States, the validation-centred approaches of European organisations, the integrated state-centric systems of China or the distributed analytical ecosystems visible in Ukraine, intelligence communities are adapting to a world in which publicly and commercially available information increasingly shapes strategic warning, escalation management and political legitimacy. The Ukraine conflict demonstrated how OSINT, when supported by analytical discipline, commercial geospatial intelligence, AI-enabled fusion systems and institutional absorption mechanisms, can contribute not only to battlefield awareness but also to strategic communication and international policy coordination. Equally significant, recent conflicts in the Middle East have highlighted a parallel reality: intelligence failures increasingly stem not from an absence of information, but from challenges associated with interpretation, institutional assumptions and the integration of available indicators into decision-making processes.

The conflicts involving Israel, Hamas, Iran, the United States and maritime security challenges across the Red Sea and Strait of Hormuz between 2023 and 2026 further reinforce this transformation. Commercial satellite imagery, maritime tracking systems, flight-monitoring platforms and distributed open-source analytical networks were employed extensively by governments, international organisations, journalists and independent researchers to assess military deployments, missile activity, infrastructure damage, disruptions to shipping routes and broader escalation dynamics. These developments suggest that contemporary conflicts are progressively eroding the traditional state monopoly over strategic observation. Intelligence assessments increasingly derive credibility from transparent methodologies, distributed verification and commercially available data, rather than from secrecy and state control alone.

For India, these developments intersect directly with recent operational experience. Military crises and continuing strategic competition have unfolded within an environment of radical transparency, where satellite imagery, digital narratives and open-source assessments influence diplomatic engagement, public legitimacy and escalation management. Emerging intelligence architectures, greater inter-agency integration, and expanding access to geospatial and digital data reflect an implicit recognition that intelligence advantage increasingly depends upon fusion rather than isolation. The challenge, however, extends beyond technological adoption. It lies in developing analytical cultures, institutional trust, validation mechanisms and organisational processes capable of converting open information into credible intelligence and actionable strategic insight.

The central conclusion of this study is therefore conceptual rather than prescriptive. OSINT should not be viewed as another intelligence discipline competing for bureaucratic relevance, but as an epistemic layer that increasingly shapes how intelligence itself is produced, validated and communicated. In an era characterised by negative peace, informationalised warfare and persistent cognitive contestation, intelligence systems that fail to internalise this transformation risk strategic lag in responding to rapidly evolving narratives and perceptions. Conversely, institutions that integrate OSINT systematically, professionalise its tradecraft and combine it with emerging analytical technologies are likely to improve strategic coherence and decision-making under conditions of constant scrutiny.

At the same time, OSINT should not be understood as a panacea for intelligence failure, nor as a decisive instrument of coercion capable of overcoming the structural constraints of international politics. Open information may improve situational awareness, reduce uncertainty and support strategic signalling, but it cannot eliminate the enduring influence of power asymmetries, political objectives, deterrence dynamics or competing national interests. Its enduring significance lies instead in shaping the informational environment within which contemporary statecraft, coercive diplomacy and strategic competition increasingly unfold.

Looking ahead, several avenues for further research emerge from this study. First, there is scope to systematically evaluate different institutional models of OSINT integration across national intelligence systems and assess how organisational design influences strategic effectiveness. Second, further research is required into the relationship between OSINT, cognitive warfare and Foreign Information Manipulation and Interference (FIMI), particularly as democratic societies confront increasingly sophisticated

influence operations. Third, the expanding role of artificial intelligence in open-source exploitation warrants deeper examination, especially regarding the balance between analytical augmentation, human oversight and accountability. Fourth, comparative studies of OSINT's influence on crisis stability, escalation management and deterrence dynamics—particularly within nuclearised environments such as South Asia—would significantly enhance understanding of its strategic effects. Finally, the growing role of commercial geospatial intelligence, private technology firms and non-state analytical networks raises important questions regarding authority, legitimacy and the future distribution of intelligence capabilities in international politics. Collectively, these areas provide fertile ground for future scholarship and will remain central to understanding the evolving relationship between information, intelligence and power in the 21st century.

NOTES

1. M. M. Lowenthal, *Intelligence: From Secrets to Policy*, 8th ed., CQ Press, 2020, pp. 87–90.
2. J. Galtung, 'Violence, Peace, and Peace Research', *Journal of Peace Research*, Vol. 6, No. 3, 1969, pp. 167–191, available at <https://doi.org/10.1177/002234336900600301>
3. M. Herman, *Intelligence Power in Peace and War*, Cambridge University Press, 1996, pp. 182–186.
4. L. Freedman, *The Future of War: A History*, Allen Lane, 2017, pp. 261–268.
5. F.G. Hoffman, 'Will War's Nature Change in the Seventh Military Revolution?', *Parameters*, Vol. 51, No. 4, pp. 17–30.
6. M.G. Toma and O.V. Vasylova, 'OSINT Tools: Recording War Crimes in Ukraine', *Analytical and Comparative Jurisprudence*, Vol. 2, 2025, pp. 905–910.
7. 'Annual Report 2019–20', Ministry of Defence, Government of India, pp. 32–35.
8. S. Tanwar, 'Intelligence Setup in India: An Analysis', *Defence and Diplomacy Journal*, Vol. 11, No. 2, pp. 45–62.
9. Ibid.
10. Ibid., pp. 85–88.
11. P.H.J. Davies, K. Gustafson and P. Hennessy (eds), *Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere*, Georgetown University Press, 2013, pp. 211–214.
12. H. Akarslan, 'A Model Proposal for Analysing Open-source Information in End-user Computers', *International Journal of Intelligence and CounterIntelligence*, Vol. 35, No. 3, 2022, pp. 482–503, available at <https://doi.org/10.1080/08850607.2022.2030694>

13. 'Intelligence Community Directive 301: National Open Source Enterprise', 20ODNI, Office of the Director of National Intelligence.
14. 'Cognitive Warfare', NATO Allied Command Transformation (NATO ACT), 2020.
15. E.B. Kania, 'Open-source Intelligence and China's Military Modernisation', *China Brief*, Vol. 19, No. 16, 2019.
16. Ibid.
17. S. Tanwar, 'Intelligence Setup in India: An Analysis', n. 8, pp. 58–60.
18. M. Joshi, 'Why Open-source Intelligence Matters More Than Ever', Observer Research Foundation, 2022.
19. M. M. Lowenthal, *Intelligence: From Secrets to Policy*, n. 1, pp. 89–92.
20. 'DoD Open-source Intelligence (OSINT) Strategy 2024–2028', U.S. Department of Defence, pp. 6–9.
21. Ibid.
22. J. Watling and N. Reynolds, *Hybrid Threats and Open-source Intelligence*, Royal United Services Institute, 2022, pp. 14–18.
23. R. Bergman, 'Israel's Intelligence Blind Spot', *Yedioth Ahronoth*, 12 November 2021.
24. Kania, *Open-source intelligence*.
25. M.G. Toma and O.V. Vasylova, 'OSINT Tools: Recording War Crimes in Ukraine', n. 6.
26. S. Tanwar, 'Intelligence Setup in India: An Analysis', n. 8, pp. 55–62.
27. M. Joshi, 'Why Open-source Intelligence Matters More Than Ever', n. 18.
28. L. Freedman, *The Future of War: A History*, Allen Lane, n. 4, pp. 261–268.
29. M. Kofman, R. Lee, K. Migacheva and C. Fink, 'The Russian Invasion of Ukraine: Initial Military Assessment', *War on the Rocks*, 2022, available at <https://warontherocks.com>
30. Ibid.
31. E. Higgins, *We are Bellingcat: An Intelligence Agency for the People*, Bloomsbury, 2022, pp. 119–134.
32. 'Annual Threat Assessment of the U.S. Intelligence Community', Office of the Director of National Intelligence (ODNI), 2023.
33. Ibid.
34. M. Joshi, 'Why Open-source Intelligence Matters More Than Ever', n. 18.
35. F.G. Hoffman, 'Will War's Nature Change in the Seventh Military Revolution?', n. 5.
36. L. Freedman, *The Future of War: A History*, Allen Lane, n. 4.
37. Ibid.
38. H. Akarslan, 'A Model Proposal for Analysing Open-source Information in End-user Computers', n. 12.
39. 'Cognitive Warfare', n. 14.
40. M. Joshi, 'Why Open-source Intelligence Matters More Than Ever', n. 18.

41. S. Tanwar, 'Intelligence Setup in India: An Analysis', n. 8.
42. L. Freedman, *The Future of War: A History*, Allen Lane, n. 4.
43. M. Herman, *Intelligence Power in Peace and War*, n. 3.
44. L. Freedman, 'Strategy in the Age of Transparency', *Survival*, Vol. 61, No. 3, 2019, pp. 7–28, available at <https://doi.org/10.1080/00396338.2019.1600317>
45. 'The Future of Intelligence Analysis in an Open Information Environment', RAND Corporation, 2022.
46. International Institute for Strategic Studies, *Strategic Survey 2023: The Annual Assessment of Geopolitics*, Routledge, 2023, pp. 3–9.
47. 'Open-source Intelligence and Strategic Warning', Office of the Director of National Intelligence (ODNI), 2022.
48. 'Integrating Open-source Intelligence into All-source Analysis', RAND Corporation, 2022.
49. 'Multi-domain Operations and the Cognitive Dimension', NATO Allied Command Transformation (NATO ACT), 2021.
50. International Institute for Strategic Studies, *The Military Balance 2023*, Routledge, 2022, pp. 17–21.