VARSTVOSLOVJE
Journal of Criminal Justice and Security
year 2026
volume 28
pp. 1–16

Two Paradigms of Open-Source Use: Investigation and Situational Awareness

Jaroš Britovšek

Purpose:

The article examines whether contemporary uses of open sources are best understood as a single activity or as two distinct paradigms. It is argued that the growing diversity of open-source practices has produced a functional differentiation between investigative and situational OSINT, which serve different decision-support needs.

Design/Methods/Approach:

Conceptual analysis based on literature from intelligence studies, OSINT research, journalism, digital investigations and situational awareness. A review is made of the historical evolution of OSINT, debates over its status as an intelligence discipline, and the impact of digital platforms and artificial intelligence.

Findings:

Two paradigms are identified. Investigative OSINT emphasises attribution, evidence and accountability, whereas situational OSINT stresses monitoring, warning, and decision support. The paradigms vary in their objectives, verification standards, outputs, and measures of success. This distinction may also be understood as one between open-source investigations and open-source intelligence.

Practical Implications:

The proposed framework suggests that investigative and situational OSINT should be organised, trained, governed and evaluated differently. Guidance is offered to intelligence organisations, law-enforcement agencies, journalists, researchers and policymakers.

Originality/Value:

A conceptual framework is proposed where investigative OSINT is distinguished from situational OSINT, which demonstrates how each supports different intelligence functions, including attribution, situational awareness, warning, and decision support.

Keywords: open-source intelligence (OSINT); open-source investigations; situational awareness; decision support; intelligence studies

UDC: 355.40

Pristopa uporabe odprtih virov: preiskovanje in situacijsko zavedanje

Namen:

Prispevek obravnava vprašanje, ali je sodobno uporabo javno dostopnih virov smiselno razumeti kot enotno dejavnost ali kot dva različna pristopa. Trdi, da je vse večja raznolikost njihove uporabe povzročila funkcionalno razlikovanje med preiskovalnim in situacijskim OSINT, ki podpirata različne potrebe odločanja.

Metode:

Prispevek temelji na konceptualni analizi in pregledu literature s področij obveščevalne dejavnosti, OSINT, novinarstva, digitalnih preiskav in situacijskega zavedanja. Obravnava zgodovinski razvoj OSINT, razpravo o njegovem statusu kot obveščevalni disciplini ter vpliv digitalnih platform in umetne inteligence.

Ugotovitve:

Analiza opredeli dva pristopa. Preiskovalni OSINT je usmerjen v atribucijo, dokazovanje in odgovornost, situacijski OSINT pa v spremljanje, opozarjanje in podporo odločanju. Pristopa se razlikujeta glede ciljev, zahtev preverjanja, rezultatov in meril uspešnosti. Prispevek pokaže tudi, da je razlikovanje mogoče razumeti kot razlikovanje med preiskavami iz javno dostopnih virov in obveščevalno dejavnostjo iz javno dostopnih virov.

Praktična uporabnost:

Predlagani okvir kaže, da bi bilo treba preiskovalni in situacijski OSINT različno organizirati, usposabljati, upravljati in vrednotiti. Razlikovanje lahko pomaga obveščevalnim organizacijam, organom pregona, novinarjem, raziskovalcem in oblikovalcem politik pri izbiri ustreznih metod in tehnologij.

Izvirnost/pomembnost:

Prispevek predlaga konceptualni okvir, ki razlikuje med preiskovalnim in situacijskim OSINT ter pokaže, kako vsak od njiju podpira različne obveščevalne funkcije, vključno z atribucijo, situacijskim zavedanjem, opozarjanjem in podporo odločanju.

Ključne besede: obveščevalna dejavnost na podlagi javno dostopnih virov (OSINT); preiskave na podlagi javno dostopnih virov; situacijsko zavedanje; podpora odločanju; obveščevalne študije.

UDK: 355.40

1 INTRODUCTION

Intelligence is best understood as a decision-support activity whose primary purpose is to generate decision advantage over competitors, adversaries or other actors operating in the same environment. The core function of intelligence is therefore not secrecy, information collection or surveillance per se, but to lower

uncertainty in support of superior decision-making in a competitive environment. Since the early development of intelligence theory, scholars have consistently argued that intelligence exists to provide knowledge that reduces uncertainty and supports decision-makers confronted with complex strategic problems (Herman, 1996; Kent, 1966; Omand, 2010). More recent scholarship similarly notes that intelligence provides decision-makers with an informational and analytical advantage that enables more effective action than would otherwise be possible (Lowenthal, 2017). Contemporary intelligence theory increasingly conceptualises intelligence as a means of creating and sustaining **decision advantage**, whether in national security, military operations, law enforcement or business competition (Britovšek, 2024; Riehle, 2025; Sims, 2022). In this sense, intelligence is valuable not because information is secret, but since it allows decision-makers to understand situations more accurately, anticipate developments more effectively and act more appropriately than competitors or adversaries.

The described understanding is especially important for Open-Source Intelligence (OSINT). Publicly available information does not become intelligence simply due to the fact it is collected. A map, social media post, satellite image, dashboard or database only acquires intelligence value when it is systematically collected, evaluated, analysed, and transformed into knowledge that supports a specific decision. Beyond the gathering of open information, OSINT should thus be viewed as the production of decision advantage from open sources. RAND's concept of "second-generation OSINT" highlights this distinction by arguing that the real challenge is not gaining access to information, but converting vast quantities of publicly available data into actionable intelligence that reduces uncertainty and improves decision quality (Williams & Blum, 2018). The Office of the Director of National Intelligence (2024) similarly defines OSINT as intelligence derived from publicly or commercially available information that addresses particular intelligence priorities, requirements and gaps. In this perspective, OSINT is best understood as a decision-support capability whose ultimate purpose is to help decision-makers gain and maintain an advantage in a competitive environment.

The central argument in this article is that contemporary OSINT is better described through two related, yet distinct paradigms. **Investigative OSINT** is evidentiary, retrospective and attribution-oriented. **Situational OSINT** is continuous, monitoring-centred and warning-oriented. The distinction is not merely semantic. It helps explain why Bellingcat-style investigations, human-rights documentation, military watch-floor monitoring, live conflict maps, AI-generated alerts and public 'situation dashboards' all appear under the same OSINT label despite operating with different tempos, standards, risks and outputs. The article therefore presents a conceptual comparison grounded in the literature, before an assessment is made of the ways the distinction clarifies current debates on intelligence disciplines, journalism, misinformation, artificial intelligence (AI) and ethics.

The distinction in focus also raises a broader conceptual question. If intelligence is understood chiefly as a decision-support activity, does this mean every form of open-source analysis should be regarded as intelligence? It is argued that the distinction between investigative and situational OSINT can alternatively be

seen as between open-source investigations and open-source intelligence. While the two frameworks describe the same empirical practices, they stress different conceptual perspectives. The first framework explains how open sources are operationally used, whereas the second explains why they are used and how as a decision-support activity they contribute to intelligence.

The proposed distinction is not merely operational; it reflects two fundamentally different ways in which open sources create value. Investigative OSINT seeks to establish justified conclusions about events, actors, and responsibility, whereas situational OSINT aims to support understanding and decision-making under conditions of uncertainty. Consequently, the distinction extends beyond methods and outputs to the very standards by which success is evaluated.

2 EVOLUTION AND CONCEPTUAL DEBATES

Although OSINT is often presented as a product of the digital age, historical scholarship shows that its origins long predate the Internet. Stephen Mercado (2004) showed that the systematic exploitation of publicly available information (foreign broadcasts, newspapers, journals, government publications, other documentary sources) was institutionalised long before the advent of social media. Building on this historical perspective, Block (2024) states the origins of OSINT are older than generally assumed. After considering historical case studies, he argues the collection and analysis of openly available information has been a feature of intelligence practice for centuries, challenging narratives that mostly associate the emergence of OSINT with the Second World War or the digital revolution. Instead of being a novel form of intelligence, OSINT can thus be seen as one of the oldest intelligence practices, continuously adapting to changing information environments (Block, 2024; Mercado, 2004).

Although the post-Cold War period did not create OSINT, it fundamentally transformed its scale, speed and visibility. Schaurer and Störger (2010) identified the growing importance of open sources within modern intelligence systems, claiming that technological change was adding to both the availability and operational value of publicly accessible information. As digital platforms, social media, satellite imagery, commercial data providers and online databases proliferated, OSINT evolved from a supplementary collection function to become a major component of contemporary intelligence activity. Williams and Blum (2018) characterised this transformation as "second-generation OSINT", emphasising Internet-scale data collection, new analytical workflows, and stronger reliance on commercial technologies. More recently, Hoffman and Fuller (2025) questioned whether the concept of second-generation OSINT adequately captures contemporary developments, arguing that the rapid integration of artificial intelligence, automation, and increasingly complex data environments requires a reconceptualisation of OSINT as an intelligence discipline.

Recent scholarship has also challenged the widely held view that OSINT is a revolutionary break from traditional intelligence. Van Puyvelde and Tabárez Rienzi (2025) believe the rise of OSINT should mainly be understood as an

evolution of longstanding intelligence functions rather than a fundamentally new paradigm. While the volume of publicly available information has grown dramatically, the essential intelligence tasks of collection, processing, analysis and dissemination remain unchanged. They add that OSINT neither democratises nor revolutionises intelligence. Instead, it expands participation in intelligence-related activities while confronting practitioners with familiar challenges like information overload, source reliability, verification, and legal or ethical constraints. Their argument reinforces the historical continuity identified by Block (2024) and Schaurer and Störger (2010), suggesting that contemporary OSINT reflects the adaptation of intelligence practice more than its transformation.

The digital turn has nevertheless altered not simply the quantity of available information but also the range of actors involved in intelligence production. OSINT is no longer confined to government agencies and specialist monitoring organisations. Investigative journalists, researchers, human-rights organisations, private-sector analysts, non-governmental organisations and online communities increasingly operate in the same information environment. Charlton, Mayer and Ohme (2024) describe this development as a new division of labour between journalism and OSINT communities. Their research shows how journalists and OSINT practitioners are collaborating ever more on digital platforms, combining investigative reporting, technical verification, geolocation, and open-source analysis to produce publicly accessible findings. The emergence of organisations such as Bellingcat[1] and the widespread use of open-source methods during the conflicts in Ukraine and Gaza illustrate how intelligence-related analytical practices have expanded beyond traditional intelligence institutions.

The mentioned diversification of actors adds weight to a longstanding theoretical question: is OSINT a distinct intelligence discipline or a methodological environment that permeates all intelligence activities? The discipline perspective holds considerable institutional appeal. Intelligence organisations increasingly maintain dedicated OSINT units, specialised training programmes, professional standards and collection strategies. Williams and Blum (2018), as well as the Office of the Director of National Intelligence (2024), largely adopt this position by describing OSINT as a distinct intelligence discipline capable of generating unique intelligence value while supporting other collection disciplines. Seen in this way, OSINT resembles other intelligence disciplines, such as HUMINT, SIGINT, GEOINT and MASINT, each of which is characterised by a distinct source domain, specialised collection methods, tradecraft, and professional expertise.[2]

However, an alternative perspective views OSINT less as a separate discipline and more as a cross-cutting methodology. Open-source information now permeates virtually every stage of the intelligence process and supports all

1 *Bellingcat is an independent investigative organisation founded in 2014 by Eliot Higgins that pioneered the systematic use of publicly available digital information, geolocation, chronolocation, and other verification techniques for open-source investigations (Higgins, 2021; Dubberley et al., 2020).*

2 *HUMINT (Human Intelligence), SIGINT (Signals Intelligence), GEOINT (Geospatial Intelligence) and MASINT (Measurement and Signature Intelligence) are established intelligence disciplines differentiated by their primary sources of information and associated collection and analytical methods (Lowenthal, 2017).*

intelligence disciplines. Lowenthal (2017) notes that contemporary intelligence increasingly relies on open information regardless of the collection discipline involved, while Van Puyvelde and Tabárez Rienzi (2025) regard OSINT as an emerging community of practice that extends beyond traditional intelligence organisations. From this perspective, OSINT may function simultaneously as both an intelligence discipline and a methodological environment. As the boundaries of intelligence activity itself remain contested (Britovšek, 2024), debates concerning the status of OSINT should be understood as part of broader unresolved questions within intelligence theory.

The conceptual argument advanced in this article hence departs from the usual question of whether OSINT constitutes a separate discipline. While that debate is important, it offers limited analytical leverage for understanding contemporary practice. A more useful enquiry concerns the purpose for which open sources are used and the decision needs they are intended to support. An investigation aiming to identify a covert operative through geolocation, facial recognition, travel records and cross-source corroboration is fundamentally different from a real-time monitoring system that continuously integrates social media, satellite imagery, aircraft tracking, financial indicators and conflict reporting. Even though both activities rely on open sources, they pursue different objectives, employ different analytical processes, and support different forms of decision-making. The article uses this observation as a foundation for the distinction developed between **investigative and situational** OSINT in the section below.

3 INVESTIGATIVE AND SITUATIONAL OSINT

Investigative OSINT is best understood as a verification-intensive form of inquiry whose goal is to reconstruct events, identify actors, evaluate competing claims and establish robust evidentiary conclusions. Bellingcat is perhaps the most prominent modern example of this approach. Higgins (2021) refers to Bellingcat's methodology as being grounded in transparency, reproducibility and publicly inspectable reasoning. The identification of the Salisbury poisoning suspect travelling under the alias "Ruslan Boshirov" as Russia's foreign military intelligence agency (GRU) Colonel Anatoliy Chepiga illustrates this model well. The investigation combined leaked passport data, military records, photographs, open-source databases and extensive cross-source corroboration to attribute the alias to a particular individual while making much of the evidentiary reasoning available for external scrutiny (Bellingcat Investigation Team, 2018a, 2018b). Investigative OSINT is thus defined not merely by the use of open sources, but by methodological rigour, traceability, and the possibility of challenge and verification. Notably, some contemporary investigations also incorporate legally obtainable commercial data and leaked datasets, revealing that modern OSINT increasingly extends beyond information that is simply published openly.

This same logic explains why investigative OSINT has become important to journalism, human rights documentation, sanctions enforcement, and legal accountability. The human rights and digital-evidence literature represented by Dubberley et al. (2020) and the Berkeley Protocol (Office of the United Nations

High Commissioner for Human Rights [OHCHR], 2022), treats open digital material not as disposable online content but as potential evidence requiring preservation, authentication, verification, and careful handling. From this perspective, the value of OSINT lies not only in discovery but also in its capacity to support accountability processes. Mukhopadhyay et al. (2024) reinforce this argument by showing that large-scale open-source investigations require structured workflows, task decomposition, coordination mechanisms, and ethical oversight. Serious investigations do not scale automatically through volunteer participation alone; rather, they depend on organized investigative processes capable of maintaining analytical rigor and evidentiary standards.

Situational OSINT operates according to a different purpose and tempo. Rather than asking primarily who did what and with what evidence, it asks what is happening now, what has changed, and what might matter next. Akhgar and Wells (2018) state that situational awareness depends upon timely, reliable and actionable intelligence, while stressing that OSINT contributes most effectively when integrated into broader intelligence and decision-support processes. Wells and Gibson (2017) similarly highlight that organisational context shapes OSINT requirements and outputs, leading to various operational uses across military, law-enforcement and security environments. Within this paradigm, the typical output is not an attribution report or evidentiary package but a current operating picture: a dashboard, watch report, alert, map or briefing designed to maintain organisational awareness in real- or near-real-time.

Public-facing dashboards exemplify this situational turn. Liveuamap presents itself as an editorially independent service providing geospatial monitoring of conflicts and security events. SitDeck advertises live monitoring using hundreds of data sources, AI-assisted analysis, alerts, and intelligence briefings. Iran Monitor combines news reporting, social media activity, connectivity indicators, commodity monitoring, mapping, and AI-generated summaries. World Monitor describes itself as a real-time intelligence platform aggregating conflict reporting, military movements, economic indicators and country-level assessments. Intel Sky focuses on military, government and strategic aircraft tracking, while Monitor the Situation combines crisis mapping, infrastructure monitoring, transportation tracking, and OSINT news aggregation. These descriptions come mainly from the platforms themselves and thus should be interpreted as claims about capability rather than independently validated assessments of analytical performance.

The distinction between the two paradigms may be summarised as follows:

Dimension	Investigative OSINT	Situational OSINT
Core question	Who did what, how, and with what evidence?	What is happening now, what has changed, and what might matter next?
Temporal logic	Retrospective or longitudinal	Real-time or near-real-time
Primary output	Attribution report, exposé, evidentiary package, timeline	Dashboard, alert, live map, watch report, briefing
Verification threshold	Very high and publication-oriented	High, yet time-constrained and iterative

Dominant value	Accountability and explanation	Warning, prioritisation, and current awareness
Key risks	False attribution, evidentiary contamination, analytical overreach	Noise, false signals, overreaction, pseudo-insight

The conceptual distinction developed above can be illustrated through two practical examples. Despite the two paradigms frequently relying on many of the same publicly available sources, their objectives, analytical logic, verification requirements, and outputs vary substantially.

Illustrative examples contrasting investigative and situational OSINT

Military operational monitoring

Following reports of an explosion at an ammunition depot, investigative OSINT analysts would combine satellite imagery, archived photographs, geolocated social-media posts, procurement records and historical imagery to determine what exploded, identify the responsible military unit, estimate the extent of the damage, and produce an attribution report suitable for policymakers or investigators. By contrast, during the same conflict, situational OSINT analysts at a military watch centre would continuously monitor social media, satellite imagery, flight tracking, maritime tracking and conflict maps in order to maintain a current operational picture, detect unusual military movements, and provide commanders with timely warning and decision support.

Foreign influence operations

A similar distinction appears in the context of foreign influence operations. Following allegations of external interference in a national election, investigative OSINT analysts would combine social-media data, domain-registration records, archived web pages, financial disclosures, leaked documents, and network analysis to attribute a coordinated influence campaign to a specific organisation or state actor. The objective would be to establish responsibility via transparent and reproducible evidence capable of supporting public reporting, sanctions or legal action. In contrast, during an ongoing election campaign, situational OSINT analysts would continuously monitor social-media trends, coordinated online behaviour, emerging narratives, cyber incidents, foreign media activity and public sentiment in order to identify potential influence operations, detect emerging risks and provide decision-makers with timely situational awareness. Immediate attribution would be secondary to early warning and informed decision support.

These illustrative examples demonstrate the distinction between investigative and situational OSINT does not chiefly concern the sources being used given that both paradigms often draw upon largely identical information environments. Instead, the distinction is found in the purpose for which open sources are employed and the decision-support function they are intended to fulfil. Investigative OSINT seeks to produce defensible attribution, explanation, and accountability, whereas situational OSINT aims to maintain awareness, reduce uncertainty and support timely decision-making amid dynamic conditions.

The mentioned framework should be viewed as a conceptual synthesis of literature on open-source investigations, digital evidence, intelligence support and situational awareness more than a typology derived from original fieldwork (Akhgar & Wells, 2018; Dubberley et al., 2020; Higgins, 2021; Mukhopadhyay et al., 2024; Wells & Gibson, 2017). The distinction proposed here is analytical rather

than ontological. Investigative and situational OSINT should be understood as ideal types representing varying dominant purposes, standards and outputs more than mutually exclusive categories.

By identifying two different epistemic logics within contemporary open-source activity, the distinction proves analytically useful. Investigative OSINT seeks justified conclusions about past or ongoing events and is therefore evaluated according to standards of verification, attribution and evidentiary defensibility. Situational OSINT aims for timely understanding sufficient to support action under uncertainty, which means it is evaluated by relevance, timeliness, and decision utility. While organisations often move between these two modes, the standards governing them remain different.

A watch centre may employ situational OSINT to detect anomalies, emerging crises or indicators of change before transferring a case to an investigative team for deeper analysis. Conversely, investigative organisations often maintain situational monitoring capabilities to be able to identify potential leads and emerging lines of inquiry. For that reason, the two paradigms are complementary rather than mutually exclusive. However, they should not be collapsed into a single analytical category. Much of the debate today on OSINT concerns evaluating one model according to the standards, expectations and key risks of the other.

The distinction in focus has been presented as two paradigms within OSINT. Yet, it can also be interpreted from a broader intelligence-theoretical perspective. Instead of distinguishing between two forms of OSINT, in certain contexts it may be more useful to distinguish **open-source investigations** from **open-source intelligence**. The discussion below develops this alternative interpretation and explains how both frameworks describe the same functional differentiation from different analytical perspectives.

When intelligence is viewed as a means of generating decision advantage, it becomes possible to differentiate between open-source investigations and open-source intelligence. Sims (2022) argues the core purpose of intelligence is to generate decision advantage by enabling actors to learn and adapt more effectively than their competitors. Britovšek (2024) and Riehle (2025) similarly point to relative advantage in decision-making as a central objective of intelligence activity. Seen via this lens, open-source investigations mainly focus on explaining events, establishing attribution and answering questions about what happened and who was responsible. Open-source intelligence, in comparison, concentrates on understanding what is happening now, what might happen next, and how emerging developments may affect future decisions. The distinction namely reflects two different contributions of open sources: evidentiary understanding of events, and decision support in conditions of uncertainty.

4 CHALLENGES FOR CONTEMPORARY OSINT

The rapid expansion of open-source has created considerable opportunities for intelligence organisations, journalists, researchers and civil society. At the same time, the greater availability of digital data, analytical tools and public monitoring

platforms has led to new challenges that affect both investigative and situational forms of OSINT.

The most obvious challenge is **information overload**. Second-generation OSINT literature points out the difficulties created by large-scale digital environments featuring growing data volumes, source diversity and increasing complexity in information processing. The emergence of dashboard-based OSINT platforms may be seen as a market and technological response to these challenges, with the goal to aggregate, prioritise and visualise vast volumes of heterogeneous information. Platforms such as SitDeck, World Monitor, Iran Monitor, and Monitor the Situation aim to aggregate, filter and prioritise large quantities of information from numerous sources into a single analytical environment. Still, aggregation does not necessarily produce understanding. McBrien (2026) argues the consumption of continuously updated information streams can easily become "hypercharged doomscrolling" rather than intelligence if users lack clear analytical questions, contextual knowledge and methodological discipline. Moreover, access to monitoring tools may create the illusion of expertise, encouraging users to mistake information access for genuine analytical understanding (McBrien, 2026; Poisson, 2026). From a practical perspective, organisations should mitigate information overload by defining clear intelligence requirements, prioritising information needs and employing AI-assisted filtering and visualisation tools while making sure that analytical judgement remains under human control.

A second challenge is **misinformation and disinformation**. Open-source ecosystems are vulnerable because the same platforms that provide valuable evidence also distribute rumours, manipulated media, strategic deception, partisan narratives and speculative interpretations. Niu et al. (2025) investigate the distinction between genuine OSINT and what they term "BULLSHINT" in discussions on X (former Twitter) of the Russo-Ukrainian War. Their findings suggest that OSINT-related online communities may contain mixtures of military analysis, partisan narratives and misinformation, creating significant challenges for evaluating credibility and reliability. Similarly, some forms of "OSINT-cowboy" culture[3] can generate misinformation disguised as informed synthesis (McBrien, 2026; Poisson, 2026). The consequences vary between paradigms. Investigative OSINT risks false attribution when conclusions are based on insufficiently verified evidence, whereas situational OSINT risks the rapid dissemination of false positives given that assessments are often produced under considerable time pressure. This means both paradigms require systematic source evaluation, multi-source corroboration and transparent confidence assessments, albeit the acceptable verification threshold differs by operational purpose.

A third challenge concerns **gamification and speculative forecasting**. McBrien (2026) claims that today parts of the OSINT community increasingly resemble spectator cultures, with participants searching for predictive meaning in publicly observable signals such as aircraft movements, transportation patterns, satellite imagery or commercial activity. This trend is further reinforced by the stronger

3 *Colloquially known as "OSINT cowboys" or "BROSINT", these practitioners are typically characterised by overconfidence, insufficient methodological rigour, inadequate source verification, and a tendency to prioritise rapid online speculation over systematic analysis and professional tradecraft (McBrien, 2026; Wright & Ysart, 2025).*

convergence of OSINT monitoring and prediction-market culture. PizzINT provides a particularly revealing example. The platform presents itself through the "Pentagon Pizza Index", displays "DOUGHCON" alert levels, incorporates prediction-market data, and encourages users to interpret unusual commercial activity as a potential indicator of geopolitical developments. Yet the platform explicitly warns that observed correlations should not be interpreted as evidence of causation. These developments suggest a broader risk that users might conflate attention, probability and evidence when open-source signals are combined with social-media engagement metrics and prediction-market incentives (McBrien, 2026; Poisson, 2026). Situational OSINT should therefore clearly distinguish observed indicators from analytical assessments and speculative forecasting so as to avoid possibility being confused with probability.

A fourth challenge concerns **legal and ethical restraint**. The fact that information is publicly accessible does not automatically make its collection, retention, aggregation, republication or analytical reuse proportionate or legitimate. This principle is especially important in the European Union's General Data Protection Regulation (GDPR), where publicly available personal information remains protected personal data. Investigative OSINT also creates specific risks of misidentification, reputational harm, doxxing and harassment. McBrien (2026) highlights concerns about online investigations that contribute to public speculation and false accusations. Human-rights and digital-evidence frameworks such as the Berkeley Protocol (OHCHR, 2022) and the work of Dubberley et al. (2020) are valuable precisely because they stress verification, preservation, harm mitigation and legal accountability. Open-source evidence thus requires the same attention to consequence and responsibility as other forms of evidentiary material. Organisations should establish governance frameworks that address proportionality, privacy, evidentiary standards and accountability for the collection and use of publicly available information.

A fifth challenge concerns **artificial intelligence**. Williams and Blum (2018) noted that machine learning and natural-language-processing techniques could greatly improve the efficiency of collecting, sorting, translating and analysing open-source information. Contemporary OSINT platforms increasingly embody this promise via automated summarising, AI-generated briefings, anomaly detection and AI-assisted analytical interfaces. These applications are particularly compatible with situational OSINT since they support triage, clustering, translation and alerting across large data streams. Nonetheless, the same technologies raise more substantial concerns within investigative OSINT. Conclusions about identity, chronology, causation, and responsibility require levels of explainability and evidential robustness that current generative AI systems cannot yet consistently provide. While AI may function as an analytical accelerator, it does not constitute evidence and cannot substitute for human judgment. AI is hence likely to provide greater value within situational OSINT by supporting monitoring, prioritisation and anomaly detection than within investigative OSINT, where attribution and evidentiary reasoning remain fundamentally human responsibilities.

A sixth challenge concerns **journalism and democratic accountability**. OSINT has expanded the ability of journalists, researchers, civil society organisations,

and citizens to discover, verify and publish information. Investigative OSINT can expose covert activity, challenge official narratives, and preserve evidence of human-rights abuses that might otherwise remain hidden. Simultaneously, situational OSINT risks encouraging audiences, analysts and even news organisations to experience conflict mainly through dashboards, maps, aircraft trackers and social-media feeds rather than through contextualised reporting and direct human testimony. McBrien (2026) argues that real-time OSINT monitoring platforms can generate valuable leads for journalists, yet do not replace the professional tasks of contextualisation, corroboration, and editorial judgment. Instead, continuous monitoring may create a sense of participation in geopolitical events without necessarily fostering a deeper understanding of them (McBrien, 2026; Poisson, 2026). The democratic value of OSINT therefore depends not only on openness and accessibility, but in addition on the standards governing its collection, analysis, interpretation and dissemination. While openness may broaden participation in intelligence-related activities, it does not remove the need for professional judgment, contextualisation, and accountability. These differences add to the need to distinguish investigative and situational OSINT while developing training programmes, organisational structures, technological support and evaluation criteria.

4.1 Practical implications

Taken together, these challenges demonstrate that the distinction proposed in this article holds important practical implications for organisations using OSINT. First, investigative and situational OSINT should be organised as complementary, albeit distinct functions, each requiring different workflows, staffing models and performance metrics. Second, investigative practitioners should receive advanced training in verification, attribution, digital evidence and legal standards, whereas situational analysts should emphasise monitoring, alert management, trend analysis and rapid assessment. Third, technological support – including artificial intelligence – should be tailored to the requirements of each paradigm. AI is likely to provide greater value for situational OSINT by supporting monitoring, prioritisation, and anomaly detection, while investigative OSINT should continue to rely primarily on human judgement for attribution and evidentiary reasoning. Finally, organisations should evaluate the two paradigms differently: investigative OSINT according to evidentiary robustness and analytical accuracy, and situational OSINT according to timeliness, relevance, and contribution to decision advantage.

5 CONCLUSION

It is argued in this article that contemporary OSINT is no longer adequately understood as a single, homogeneous activity. The expansion of digital information environments, emergence of platform-based monitoring systems, growing role of non-state actors, and increasing use of artificial intelligence have produced distinct forms of open-source practice that vary by purpose, tempo, evidentiary

standards, and relationship to decision-making. As a result, a useful analytical distinction can be made between investigative OSINT and situational OSINT.

Investigative OSINT is chiefly concerned with attribution, explanation and evidence. Its purpose is to reconstruct events, identify actors, evaluate competing claims and establish defensible conclusions. **Situational OSINT**, by contrast, is principally concerned with awareness, warning, and decision support. Its purpose is to monitor evolving developments, identify relevant changes, and reduce uncertainty for decision-makers operating in dynamic environments. Although both forms rely on open sources, they differ in their temporal orientation, verification requirements, outputs, vulnerabilities, and measures of success

The distinction helps explain several apparent contradictions in contemporary debates about OSINT. The same technological developments that enable unprecedented transparency and accountability also facilitate misinformation, speculation, information overload, and the illusion of understanding. Artificial intelligence can significantly enhance the monitoring and processing of large information streams, yet remains less suited to tasks requiring attribution, causation, and evidentiary judgment. Likewise, the growth of real-time monitoring platforms shows both the potential and limits of open-source intelligence: greater visibility does not necessarily produce greater understanding.

Viewed through the broader lens of intelligence as a decision-support activity aimed at generating decision advantage, the distinction also suggests an alternative conceptualisation. Rather than viewing contemporary OSINT solely through the distinction between investigative and situational OSINT, it may be equally useful to distinguish **open-source investigations** from **open-source intelligence**. The former seeks to explain events, establish attribution and support accountability through evidence. The latter seeks to reduce uncertainty, improve understanding of evolving situations, anticipate developments, provide warning, and support decision-making. With this interpretation, investigative OSINT represents a form of open-source investigation, while situational OSINT is a form of open-source intelligence. These two conceptualisations capture the same functional differentiation, although from different analytical vantage points: the distinction between investigative and situational OSINT stresses differences in operational practice, methods, outputs, and temporal orientation, while the distinction between open-source investigations and open-source intelligence emphasises the broader purpose served; namely, evidentiary explanation and accountability on one hand, and uncertainty reduction, situational understanding, warning, anticipation, and decision support on the other.

The main contribution of this article is therefore not to propose a new intelligence discipline; instead, it is to provide a conceptual framework for understanding the functional differentiation that has emerged within contemporary open-source practice. Rather than competing perspectives, the two conceptualisations are complementary. The distinction between investigative and situational OSINT is most useful for analysing operational practice, organisational design, technologies, analytical workflows and professional competencies, whereas the distinction between open-source investigations and open-source intelligence is better suited to examining the fundamental purpose of open-source

activities within intelligence theory. As the volume, velocity and accessibility of digital information continue to rise, the critical challenge will not be collecting more information but determining which form of open-source activity is most appropriate to generate meaningful understanding and decision advantage.

REFERENCES

Akhgar, B., & Wells, D. (2018). Critical success factors for OSINT driven situational awareness. *European Law Enforcement Research Bulletin, 18*. https://shura.shu.ac.uk/22734/

Bellingcat Investigation Team. (2018a, September 26). *Skripal suspect Boshirov identified as GRU Colonel Anatoliy Chepiga*. Bellingcat. https://www.bellingcat.com/news/europe/2018/09/26/skripal-suspect-boshirov-identified-gru-colonel-anatoliy-chepiga/

Bellingcat Investigation Team. (2018b, October 2). *Anatoliy Chepiga is a Hero of Russia: The writing is on the wall*. Bellingcat. https://www.bellingcat.com/news/europe/2018/10/02/anatoliy-chepiga-hero-russia-writing-wall/

Block, L. (2024). The long history of OSINT. *Journal of Intelligence History, 23*(2), 95–109. https://doi.org/10.1080/16161262.2023.2224091

Britovšek, J. (2024). *Definicija obveščevalne dejavnosti*. *Sodobni vojaški izzivi, 26*(4), 185–197. https://doi.org/10.2478/cmc-2024-0032

Charlton, T., Mayer, A.-T., & Ohme, J. (2024). A common effort: New divisions of labor between journalism and OSINT communities on digital platforms. *The International Journal of Press/Politics, 32*(1), 118–139. https://doi.org/10.1177/19401612241271230

Dubberley, S., Koenig, A., & Murray, D. (Eds.). (2020). *Digital witness: Using open source information for human rights investigation, documentation, and accountability*. Oxford University Press.

Herman, M. (1996). *Intelligence power in peace and war.* Cambridge University Press.

Higgins, E. (2021). *We are Bellingcat: Global crime, online sleuths, and the bold future of news*. Bloomsbury Publishing.

Hoffman, F. P., & Fuller, B. (2025). Rebranding second-generation open-source intelligence: "It's not your father's OSINT". *Issues in Information Systems, 26*(3), 61–74.

Intel Sky. (n.d.). *Live radar*. Retrieved June 12, 2026, from https://intelsky.org/stats/map.php

Iran Monitor. (n.d.). *Iran Monitor: Real-time OSINT dashboard for Iran*. Retrieved June 12, 2026, from https://www.iranmonitor.org/

Kent, S. (1966). *Strategic intelligence for American world policy* (Rev. ed.). Princeton University Press. (Original work published 1949)

Liveuamap. (n.d.). *Liveuamap news*. Retrieved June 12, 2026, from https://liveuamap.com/

Lowenthal, M. M. (2017). *Intelligence: From secrets to policy* (7th ed.). CQ Press.

McBrien, T. (2026, March 12). *Situational unawareness*. *The Baffler*. https://thebaffler.com/latest/situational-unawareness-mcbrien

Mercado, S. C. (2004). Sailing the sea of OSINT in the information age. *Studies in Intelligence, 48*(3), 45–55. https://www.cia.gov/resources/csi/static/Sailing-the-Sea-OSINT.pdf

Monitor the Situation. (n.d.). *Monitor the Situation: Live conflict map and global crisis tracker*. Retrieved June 12, 2026, from https://monitor-the-situation.com/

Mukhopadhyay, A., Venkatagiri, S., & Luther, K. (2024). OSINT research studios: A flexible crowdsourcing framework to scale up open source intelligence investigations. *Proceedings of the ACM on Human-Computer Interaction, 8*(CSCW1), Article 105. https://doi.org/10.1145/3637382

Niu, J., Stillman, M., & Kruspe, A. (2025). *OSINT or BULLSHINT? Exploring Open-Source Intelligence tweets about the Russo-Ukrainian War* [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2508.03599

Office of the Director of National Intelligence. (2024, March 8). *The IC OSINT strategy 2024–2026*. https://archive.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf

Office of the United Nations High Commissioner for Human Rights (OHCHR). (2022). *Berkeley protocol on digital open source investigations: A practical guide on the effective use of digital open source information in investigating violations of international criminal, human rights and humanitarian law*. United Nations. https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source

Omand, D. (2010). *Securing the state.* Columbia University Press.

PizzINT. (n.d.). *Pentagon Pizza Index*. Retrieved June 12, 2026, from https://www.pizzint.watch/

Poisson, J. (Host). (2026, March 23). *Open source intelligence cowboys "monitoring" Iran* [Audio podcast episode]. In *Front Burner*. Canadian Broadcasting Corporation. https://www.cbc.ca/listen/cbc-podcasts/209-front-burner/episode/16204614-open-source-intelligence-cowboys-monitoring-iran

Riehle, K. P. (2025). *Counterintelligence at its core: Assessing and preventing foreign espionage*. Lynne Rienner Publishers.

Schaurer, F., & Störger, J. (2010). *The evolution of open source intelligence*. Center for Security Studies, ETH Zurich. https://bib.opensourceintelligence.biz/STORAGE/2013.%20the%20evolution%20of%20open%20source%20intelligence.pdf

Sims, J. E. (2022). *Decision advantage: Intelligence in international politics from the Spanish Armada to cyberwar*. Oxford University Press.

SitDeck. (n.d.). *SitDeck: Open-source intelligence dashboard*. Retrieved June 12, 2026, from https://sitdeck.com/

Van Puyvelde, D., & Tabárez Rienzi, F. (2025). The rise of open-source intelligence. *European Journal of International Security, 10*(4), 530–544. https://doi.org/10.1017/eis.2024.61

Wells, D., & Gibson, H. (2017). OSINT from a UK perspective: Considerations from the law enforcement and military domains. In *Proceedings Estonian Academy of Security Sciences, 16: From research to security union* (pp. 84–113). Estonian Academy of Security Sciences. https://shura.shu.ac.uk/17412/

Williams, H. J., & Blum, I. (2018). *Defining second generation open source intelligence for the defense enterprise* (RR-1964-OSD). RAND Corporation. https://doi.org/10.7249/RR1964

World Monitor. (n.d.). *World Monitor: Real-time global intelligence dashboard*. Retrieved June 12, 2026, from https://www.worldmonitor.app/

Wright, P., & Ysart, N. (2025, July 29). *OSINT cowboys: A beginner's guide (to doing it wrong!).* Coalition of Cyber Investigators. https://coalitioncyber.com/osint-cowboys-a-beginners-guide-to-doing-it-wrong

About the Author:

Jaroš Britovšek, PhD, employed at the Ministry of Defence of the Republic of Slovenia. E-mail: jaros.britovsek@mors.si