IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/47AI/2026/4714626/
Vol. 2026 (12), Article ID 4714626

Current State and Possible Development Directions Of Open-Source Intelligence*

Grzegorz JASKULA

Faculty of Computing and Telecommunications, Poznan University of Technology, Poznan, Poland

Correspondence should be addressed to: Grzegorz JASKULA, grzegorz.jaskula@put.poznan.pl

*Presented at the 47th IBIMA International Conference, 29-30 June 2026, Madrid, Spain

Abstract

This paper examines the evolution, applications, and future trajectory of open-source intelligence (OSINT). It traces OSINT's origins from early uses of publicly accessible data in the 19th century, through its constrained role during the Cold War, to its resurgence in the digital era following the expansion of the internet and global information networks. The study highlights how digitization and the proliferation of online platforms, particularly social media, have transformed OSINT into a widely accessible and powerful tool used by governments, private organizations, and individuals. It discusses the emergence of collective intelligence and specialized tools that automate data gathering and analysis, while also addressing associated risks such as privacy violations, misinformation, and data overload. Through case studies, including the Sergei Skripal poisoning investigation and the Russia-Ukraine war, the paper demonstrates OSINT's operational significance in uncovering state-sponsored activities, supporting military intelligence, and shaping public perception. These examples underscore both the effectiveness of OSINT and its vulnerability to manipulation through disinformation. The paper further explores the growing role of artificial intelligence in enhancing OSINT capabilities, particularly in cyber threat intelligence, while noting limitations and ethical concerns related to profiling and synthetic content. It also emphasizes the lack of standardized methodologies, highlighting frameworks such as the Berkeley Protocol as steps toward improving reliability and legal accountability. OSINT is identified as an increasingly indispensable yet complex intelligence discipline, requiring improved standards, critical evaluation of information credibility, and careful balancing between security needs and individual privacy rights.

Keywords: open-source intelligence, information processing, public data, privacy

Introduction

Open-source intelligence (OSINT) is a concept that refers to process of collection and analysis of information gathered from overt and publicly available sources. By the definition analysts are utilizing only legal and ethical means for data gathering and processing. OSINT has proven its effectiveness numerous times in history, moreover its importance has been noted in recent years in particular. It has been identified as an essential tool not only for industrial espionage but also for IT security.

Cite this Article as: Grzegorz JASKULA Vol. 2026 (12) "Current State and Possible Development Directions Of Open-Source Intelligence " Communications of International Proceedings, Vol. 2026 (12), Article ID 4714626, https://doi.org/10.5171/2026.4714626

Its impact on geopolitics and even military intelligence is also considered significant. Increasing access to public sources, primarily via the internet, enables more and more people to apply open-source intelligence tools for different purposes.

In this paper various aspects of open-source intelligence will be discussed to determine the current state and possible developments in this area. Paper starts with historical approach showing shift from traditional intelligence towards public sources. Several cases in which OSINT played crucial role will be described. Next sections introduce novelty aspects of OSINT such as usage of artificial intelligence. Eventually, conclusions are drawn about current state of open-source intelligence and its possible future directions of development.

OSINT in history

The idea of open-source intelligence can be traced back to 19th century. As stated by Ludo Block (2024) signs of public data exploitation has been noted by General Alexander whose spies utilised daily newspapers as a crucial source of information. Similar movements have been later observed within other nations such as German Abteilung IIIB or Dutch GS III.

Further inventions such as radio and television became a subject of interest later on. Study by Michael Glassman (2012) tracks such incarnation of OSINT back to Second World War. Emergence of new means of communication enabled investigators to gather relevant information from such sources and mold it accountable intelligence. This was achieved by establishing various intelligence units such as BBC Monitoring Service in UK and Foreign Broadcast Information Service in the US. Not only has analysts started utilising technical means, they also began seeking for correlations between events and different data with prime example being the case of the fruit market in Les Halles, France. The correlating changes in the price of oranges in Paris with bombings of railway bridges has been proving if bombardments were either successful or not marking the rising prices with the disruptions of the enemy's logistics.

The concept of open-source intelligence experienced significant limitations during the Cold War era, primarily due to widespread censorship, information suppression, and the rigid control of communication channels by state actors. Governments, particularly those in authoritarian regimes, tightly regulated the dissemination and accessibility of information viewing unfiltered knowledge as a potential threat to national security. As a result, the potential of OSINT as a systematic intelligence discipline was largely stifled during this period. Nevertheless, the emergence and proliferation of mass media—including television, radio and print journalism—created new avenues for public access to information, albeit within constrained boundaries. These media sources, though often influenced or controlled by governmental policies, contributed to a growing awareness and demand for more transparent and diverse sources of information.

Despite the restrictions, the foundational idea of OSINT managed to endure, sustained by the continued evolution of information-sharing platforms and the work of journalists, analysts, and independent observers. With the end of the Cold War and the geopolitical shifts of the early 1990s the collapse of information monopolies coupled with the rapid expansion of the internet and digital communication gave OSINT a renewed relevance. In this new global context, open-source intelligence was not only revived but redefined as a critical pillar in modern intelligence practices characterized by unprecedented access to public data and global information networks.

The term OSINT has been introduced to the wider public in the early 2000s with NATO introducing Open-source intelligence handbook (2001) which became fundamental methodological document in the next years. Thus, OSINT has been accepted as a part of military intelligence.

Internet age

The embark of the internet impacted open-source intelligence in two distinct ways. Firstly, different sources have been to adapted for online use. This includes data ranging from news feeds, through scientific publications, up to government databases. On the other hand, it enabled access to the data for people who used to be unable to utilize such sources. Therefore, entry level for accessing the information, thus utilising OSINT, has been significantly lowered. Consequently, the threshold for obtaining and utilising open-source intelligence has been considerably reduced enabling individuals who previously lacked the means to consult such materials to now do so with relative ease. Open-source intelligence has become a critical resource for a wide range of actors, extending beyond governmental agencies to include private organisations and individual practitioners.

This has also led to the development of collective or crowd intelligence. It refers to the enhanced capacity of a group to solve problems and make decisions through collaboration and information sharing. This phenomenon emerges when individuals' contributions are combined, leveraging technology and social interactions to achieve outcomes that would be impossible for a single individual. This phenomenon has been recently amplified by the use of social media platforms, as noted by Michael Glassman (2012). The emergence of social media platforms has empowered ordinary users to engage actively in online activities through content creation and interaction with others. However, while originally intended to promote communal engagement, these platforms have also become a significant source of information regarding private individuals and entities. Data collected in this way can be utilised for intelligence purposes, whether by individuals or by organisations.

The rise of digital social platforms presents significant opportunities for enhancing governmental efficiency, responsiveness, and adaptability, while also generating broader social and economic benefits. Research by Demos (2012) proves the systematic use of social media intelligence (SOCMINT) has the potential to play a critical role in ensuring public safety by enabling the detection of criminal activities, providing early warnings of potential disturbances or threats, and facilitating situational awareness in rapidly evolving contexts. As society continues to embrace new forms of communication and organisation, it becomes essential for public institutions, including law enforcement agencies and the intelligence community, to adapt and align their practices with these developments.

This case had also risen numerous privacy and ethical concerns. In response, various countermeasures have been introduced by social media platforms to mitigate potential risks such as removing the metadata attached to uploaded media and the expansion of privacy settings that allow users to control the visibility of their material. Nevertheless, despite the effort substantial amount of information remains easily accessible for use. Research conducted by the University of Adelaide (2021) has demonstrated, that by exploiting certain features, social media platforms can function as a form of distributed surveillance system. While such data may be utilised to support law enforcement activities and facilitate the monitoring of criminal behaviour, it simultaneously poses serious risks to individual privacy.

Digitization of sources

The emergence of the internet has profoundly transformed the landscape of open-source intelligence, with an ever-increasing proportion of information sources becoming digitised. Whereas in the past data collection often required physically accessing specific locations or archives, the internet has enabled the retrieval of equivalent information through digital means, significantly accelerating the process. This shift has greatly enhanced the efficiency of intelligence gathering by reducing the time and resources needed to obtain relevant data. The digital adaptation has extended beyond governmental databases and public institutions to encompass a wide range of private entities, further broadening the scope and accessibility of open-source information.

The proliferation of online information has spurred the development of numerous tools and software specifically tailored for OSINT activities. As the volume of publicly accessible data expanded, processing workflows became increasingly automated. Works by Varin Khera, Anand R. Prasad and Suksit Kwanoran (2024) notes that early contributions originated from individual developers, exemplified by Shodan, which indexes devices exposed on the internet. Subsequently, additional infrastructure-reconnaissance tools such as Spider-Foot and recon-ng were introduced. Concurrently, a variety of SOCMINT-oriented applications emerged, including specialised web scrapers and crawlers. Even general-purpose search engines have been co-opted for OSINT through the skillful application of advanced search operators (e.g. Google dorking). These developments have collectively enabled more efficient, automated collection and analysis of open-source data. Research study by Krzysztof Wosinski (2023) indicates a growing number of information sources have begun to be aggregated through specialised platforms such as IntelX and Epieos, which enable analysts to access data from multiple origins in a single interface, thereby further accelerating OSINT workflows. In parallel, entire websites have been systematically collected and preserved in large-scale digital archives. The most prominent example - The Internet Archive, operated by a US-based non-profit organisation, stores approximately 916 billion webpages and nearly 80 billion other digital media items, including public domain books, music, videos, and software.

Since not all online content is readily accessible, increasing attention has been directed toward the dark web, including networks such as Tor. As the internet has become a fundamental medium of communication, used not only by legitimate actors but also by criminals, its monitoring has become essential for maintaining the security and integrity of corporate IT systems. According to Denis Stodelov and Natalia Miloslavskaya (2022) this approach has proven particularly valuable in the field of cyber threat intelligence (CTI), enabling the early detection of potential cyberattacks and the formulation of appropriate countermeasures. By adopting such proactive strategies, many organisations have enhanced their overall

security posture, with dark web monitoring through OSINT techniques contributing to a measurable reduction in the success rate and impact of cyberattacks.

Simultaneously, a range of companies specialising in OSINT software has emerged. One of the earliest, Paterva, developed Maltego Graphs, a platform integrating numerous APIs and data sources to automate aspects of the intelligence process. Since then, additional tools have been introduced within this ecosystem such as social media monitoring and digital evidence management software. This concept has evolved even further with the advent of comprehensive all-in-one platforms designed specifically for OSINT operations - examples include OSINT Industries and OSINT Quest. In the result, the intelligence process has become increasingly automated, with a growing number of analytical tasks being delegated to scripts and algorithmic workflows. This approach enhances the accessibility and efficiency of OSINT, significantly reducing operational costs and making it available to small organisations and even individual users. However, the increasing reliance on automation introduces important challenges and heightens the risk of uncorrected errors and misinterpretations.

Sergei Skripal Case

The Skripal poisoning case refers to the attempted assassination of Sergei Skripal, a former Russian military intelligence officer and British double agent, and his daughter Yulia Skripal in Salisbury, United Kingdom on 4 March 2018. Both victims were found unconscious on a public bench and were later determined to have been exposed to a military-grade nerve agent identified as Novichok, a substance developed by the Soviet Union during the Cold War. The incident prompted a major international response due to the use of a chemical weapon on NATO territory, raising significant concerns regarding state-sponsored attacks and breaches of international laws.

Investigations conducted by British authorities, supported by the Organisation for the Prohibition of Chemical Weapons (OPCW), identified two suspects alleged to be Russian military intelligence officers operating under aliases. Subsequently the case has been investigated and described in detail by Bellingcat. In a comprehensive investigation the true identity of the second suspect in the 2018 Salisbury attack has been conclusively established. Operating under the alias ”Alexander Petrov”, the individual was identified as Dr. Alexander Yevgeniyevich Mishkin, a trained military physician and operative of Russia’s Main Intelligence Directorate (GRU). This discovery follows earlier findings by the same investigative collective, which had previously unmasked the first suspect, ”Ruslan Boshirov” as Colonel Anatoliy Chepiga, a decorated officer in the GRU and a recipient of the Hero of the Russian Federation award.

Bellingcat’s identification of Mishkin (2018) was rooted in forensic analysis and open-source intelligence. The investigation began with a passport photo of ”Petrov”, corroborated by security footage from his 2018 RT interview. Initial digital searches yielded no matches indicating the possibility of a sanitized online footprint. Investigators subsequently shifted their approach employing a ”minimum change hypothesis” — a tactic based on previous GRU operations where cover identities retained significant personal data. The pivotal clue emerged from the covert passport’s reference to a prior document issued in St. Petersburg in 1999. By filtering through leaked databases using the retained biographical details investigators identified only one exact match - Alexander Yevgeniyevich Mishkin, residing across the street from the VMEDA campus in the early 2000s.

Bellingcat further substantiated this identity by tracing vehicle registration and insurance data, which linked Mishkin to a Volvo XC90 initially registered in St. Petersburg and later transferred to the Khoroshevsky District in Moscow, coinciding with the GRU’s headquarters. Subsequent car insurance records from 2014 confirmed the address as Khoroshevskoye Shosse 76B and fully aligned with the birthdate and name of the St. Petersburg resident. These details reinforced the high probability that Mishkin and ”Petrov” were the same individual. In pursuit of further corroboration, Bellingcat mass-contacted graduates of military universities between 2001 and 2007. While most responses were evasive or non-committal, one confidential source acknowledged that Mishkin had indeed graduated from the Kirov Academy and was recognised as ”Petrov”. The source also reported that Russian authorities had recently instructed alumni not to discuss Mishkin’s identity. Eventually, Bellingcat obtained a 2001 passport scan of Alexander Mishkin and with assistance from facial recognition expert Prof Hassan Ugail who conducted a forensic analysis comparing it to the alias passport of ”Petrov”. The conclusion was both images depicted the same individual.

In addition, Bellingcat dispatched an investigative journalist from The Insider to Loyga. Multiple villagers confirmed that the man known publicly as ”Petrov” was indeed Alexander Mishkin who become a military doctor in either Murmansk or Moscow. Several residents confirmed, with varying degrees of detail, that Mishkin had received the Hero of Russian Federation award for undisclosed reasons. One source even stated that Mishkin’s grandmother owned a photograph depicting President Putin awarding her grandson the Gold Star medal though this image was not publicly accessible.

Further validation came in the form of a property registry extract indicating that in 2014 Mishkin's wife and children acquired a high-value apartment in a Moscow skyscraper. Such legal phrasing suggests a state-sponsored gift rather than a market transaction. A comparable pattern was observed in the case of Chepiga, who received a similar apartment around the same time and under equivalent legal terms. The synchronicity of these transfers strongly implies that the apartments were bestowed as state remuneration linked to the conferral of the Hero of Russian Federation award. These findings carry broader operational implications. The inclusion of a trained military doctor such as Mishkin in a covert overseas operation, involving the use of a chemical weapon, points to a mission profile that likely extended beyond routine intelligence gathering. Experts consulted by Bellingcat offered differing views: some posited that multidisciplinary teams are standard GRU practice, while others asserted that the presence of a medical professional would be essential in an operation involving a toxic substance like Novichok, both for efficacy and team safety.

The investigation into Mishkin's identity not only solidifies the assertion that the GRU was directly involved in the Salisbury incident but also illustrates the depth of operational planning and logistical support underpinning Russian covert actions abroad. Furthermore, the methodical unmasking of both suspects underscores the utility of open-source intelligence in exposing state-sponsored clandestine activity. Through extensive data triangulation, Bellingcat's work has demonstrated that even operatives shielded by elaborate cover identities are not beyond the reach of publicly accessible information, when systematically and expertly analysed. His identification lends additional weight to the hypothesis that the Salisbury poisoning was an authorised Russian state action conducted by elite GRU personnel and facilitated by a sophisticated infrastructure of aliases and covert logistics. Moreover, it has led to widespread diplomatic consequences, including the expulsion of over 150 Russian diplomats from more than 20 countries and the imposition of sanctions by Western governments. The Russian Federation has consistently denied involvement characterizing the accusations as politically motivated.

Russian-Ukrainian war

As of 2022 interest in open-source intelligence has grown rapidly due to outbreak of war between Russian Federation and Ukraine. It can be considered the first large-scale military conflict which progress have been tracked via social media platforms by thousands of internet users, according to Aaron F. Brantly (2022). This phenomenon has been noticed by Ioannis Kotaridis and Georgios Benekos (2023) and described as ”social media warfare”. Since the onset of the Russian invasion of Ukraine, social media platforms have been inundated with video content shared by both sides of the conflict. Equipped with mobile phones, both soldiers and civilians have documented events in real time effectively transforming social networks into an extension of the battlefield. In this context, OSINT practitioners are confronted with vast quantities of publicly available information that must be systematically collected, analysed, and integrated in order to generate actionable intelligence. While it enables the collection of information directly from witnesses of the events, it must also be recognised as a potential vector for disinformation and, consequently, a domain of military operations in its own right.

While narrative control has traditionally been exercised by the state, the decentralisation of information dissemination has shifted this function to a wide array of actors who now possess intelligence-gathering capacities comparable to those of state institutions. This shift has profoundly influenced public perceptions of the conflict, enabling individuals to form conclusions independently of governmental agencies. One of the most prominent examples of OSINT utilisation in this context is the development of specialised tools by private entities, such as the “almost-live” interactive war map designed to monitor and track the conflict.

The Russian-Ukrainian war has demonstrated an unprecedented level of collaboration among various intelligence disciplines, including Imagery Intelligence (IMINT), Social Media Intelligence (SOCMINT), and Geospatial Intelligence (GEOINT). This integration has enabled the correlation and cross-verification of information from diverse sources, facilitating its effective application for military purposes. As noted by Ioannis Kotaridis and Georgios Benekos (2023), the combination of geolocated SOCMINT data with satellite imagery, further enhanced through machine learning techniques, has made it possible to track military units and assess damage inflicted on specific facilities.

On the other hand disinformation actors must be taken into account, however they are still applicable for military purposes. As described by William L. Mitchell (2025) various deception tactics have been utilised by Ukrainian forces to disguise the Kherson offensive in mid 2022. Such means included deceptive storylines being distributed via media outlets and social media platforms to create illusion of troops movement, eventually affecting Russian operational decision-making processes. However as stated by Mitchell confidence of establishing cause-and-effect relationships between influence and physical actions is limited.

The use of cyberspace as a means to influence and deceive adversaries has long been recognised and incorporated into military doctrines, including the Russian concept of ”operational camouflage”. This view encompasses a wide spectrum of techniques aimed at manipulating perception and shaping the adversary’s understanding of reality and remains crucial to the idea of non-contact warfare. Such methods range from the dissemination of strategic disinformation to the physical concealment of individual soldiers, all intended to obscure actual objectives, methods, and directions of military operations for as long as possible. As highlighted by Michal Wojnowski (2023), a diverse array of ”information and strike operations” seeks to influence the enemy’s cognitive processes through the deployment of ”information weaponry”, thereby amplifying the overall effectiveness of conventional warfare. Notably, the Russian–Ukrainian war represents the first instance in history where the use of OSINT has been directly associated with the potential to cause fatalities.

AI Boom

Recent advancements in artificial intelligence (AI) are rapidly transforming the way analysts approach open-source intelligence. Increasingly, automation plays a central role in the intelligence cycle, gradually rendering traditional methods of data collection and processing less effective and, in many cases, obsolete. When combined with specific frameworks or tools, such as retrieval-augmented generation, its impact can be increased even further.

Current research highlights the diverse applications of artificial intelligence (AI) within the domain of open-source intelligence (OSINT), with particular emphasis on its relevance to CTI. As noted by Fahim Sufi (2024), the integration of automated workflows such as those developed with Microsoft Power Automate in combination with ChatGPT can substantially enhance the management of security incidents. Such systems have been evaluated to achieve an overall accuracy rate of up to 98%, potentially surpassing the performance of human analysts.

AI is also redefining the scope of evidence aggregation in OSINT workflows. Study by Andrea Tundis, Samuel Ruppert Max Mühlhäuser acknowledges that by leveraging advanced natural language processing models, analysts can now ingest and synthesize vast corpora of unstructured data ranging from news feeds to forum posts in real time, identifying emerging narratives that would otherwise be buried beneath noise. These models can flag anomalous language patterns, detect misinformation campaigns, and even predict the evolution of threat actors’ tactics by learning from historical incident reports. Consequently, the traditional bottleneck of manual triage is being replaced with algorithmic prioritization, allowing human experts to focus on higher-level interpretation and decision making.

Other studies suggest that the usefulness of large language models (LLMs) in the context of CTI may be constrained. Researchers from the Universidade de Lisboa (2025) have identified several limitations, including difficulties in recognising specific vendors and challenges in comprehending specialised terminology. While the overall effectiveness of LLMs remains high, it has been found to be comparable to that of traditional binary classification methods, which require significantly fewer computational resources. On the other hand, AI can also be applied to fingerprinting and profiling. Szde Yu (2023) demonstrated that scraping and analysing content from social media platforms such as Minds or Twitter enables the mapping of an individual’s age, gender, educational background and political orientation based solely on their published content, with results aligning closely with self-reported survey data. AI technologies have the potential to extend this concept even further, for instance by predicting user behaviour or developing tailored models trained on such data. However, as an increasing number of companies automatically enroll users into AI training processes, these practices raise significant and well-founded concerns regarding privacy.

Simultaneously, AI-driven geospatial analysis is enhancing the precision of location-based intelligence. According to Fahim Sufi (2024) convolutional neural networks trained on satellite imagery can automatically detect changes in land use, infrastructure development, or suspicious activity patterns without requiring manual image annotation. When combined with open-source geotagged social media posts, these models create a multi-modal intelligence layer that offers granular situational awareness. As the volume and velocity of publicly available spatial data continue to surge, such AI capabilities are becoming indispensable for timely, actionable insights in both defensive cyber operations and broader security assessments.

Methodological aspects

It should to be noted that OSINT currently lacks unified methodologies and standardized procedures for conducting the intelligence process. The earliest frameworks, developed more than two decades ago, no longer correspond to the realities

of the contemporary technological environment. Although their fundamental principles remain relevant, they must be regarded as outdated. This underscores the necessity for a revised methodological approach.

The Berkeley Protocol on Digital Open Source Investigations is a landmark document developed jointly by the Office of the United Nations High Commissioner for Human Rights and the Human Rights Center at UC Berkeley School of Law (2022). It emerged from interdisciplinary collaboration that began in 2009, with legal experts, technologists, and human rights advocates seeking to professionalize the use of digital open-source information in documenting and investigating serious international crimes. The need for standardized methodologies arose from the growing reliance on publicly available digital data, such as satellite imagery, social media posts and user-generated content, to uncover violations of human rights and humanitarian law, especially in contexts where on-the-ground access is restricted or unsafe. The Berkeley Protocol provides a structured, principles-based framework for the identification, collection, verification, preservation, and analysis of digital information that is publicly accessible. Crucially, it stresses legal admissibility, ethical safeguards, and safety involved. Rather than focusing on specific tools, the Protocol establishes adaptable methodological and ethical standards applicable across technologies and investigative settings. These standards are critical for ensuring credibility and reliability in OSINT, supporting aligning rigor with legal accountability.

Nevertheless, the effective conduct of the intelligence process still requires the use of specialised tools. Although numerous toolkits and software ecosystems have been developed, both the tools themselves and the underlying information sources evolve at a rapid pace, necessitating continual adaptation and refinement. This dynamic environment makes the sustainability and consistency of OSINT investigations particularly challenging to uphold, as stated by Bert-Jaap Koops (2013).

Furthermore, the requirement for data credibility scoring and validation extends across all stages of the intelligence cycle. This issue has been explicitly addressed in the Berkeley Protocol as well as by scholars such as Paul Burke (2022) and Szde Yu (2023). The importance of credibility assessment has grown particularly in the context of widespread disinformation campaigns, which exert influence across multiple domains, including geopolitics. Ensuring the reliability of collected information is therefore fundamental to the integrity of any investigation. At the same time, this task has become increasingly complex due to the proliferation of AI-generated content, which further challenges traditional verification methods.

Conclusions

This paper has examined historical cases of open-source intelligence and explored its geopolitical dimensions, including the role of disinformation and its impact on military operations. It has also addressed growing concerns related to user privacy and the implications of artificial intelligence for OSINT practices. Furthermore, the discussion has highlighted the urgent need for the development of unified frameworks within the intelligence community in order to more effectively guide and structure future investigations.

The fundamental concept of open-source intelligence is not as recent as often assumed and can be traced back several centuries. Notably, the core idea has remained largely unchanged, with only the sources of information and tools for accessing them evolving over time. The emergence of the internet made this concept widely accessible, extending its use far beyond specialised domains. The subsequent rise of social media further simplified information exchange, allowing for rapid dissemination and interaction. As a result, OSINT has become particularly valuable, as individuals can independently collect and process information without relying exclusively on traditional media outlets or state-controlled channels.

Undoubtedly, OSINT became a crucial tool in the modern sociaty, accessible to both governmental institutions and private organisation. At the same time, it can be exploited by a wide range of threat actors operating at different levels. Such misuse may involve the violation of individual privacy for specific objectives or the execution of more sophisticated targeted attacks. On a broader scale, publicly available data may also be harnessed by states to profile citizens, thereby raising the prospect of mass surveillance. Addressing these challenges requires action on multiple fronts: technology companies that operate social media platforms must adopt stronger safeguards, while governments should establish legislative frameworks to protect users' fundamental rights to privacy.

It is evident that many entities remain vulnerable to OSINT investigations. A notable example is the Sergei Skripal case, which demonstrated that even global powers can be compromised by the failure to implement adequate operational security (OPSEC) measures. Safeguarding information is therefore of paramount importance, not only in military contexts but also in everyday life. The effects of OSINT extend far beyond the immediate actors involved. They can destabilize diplomatic

relations, erode public trust in institutions and even in fluence outcomes when personal data is leveraged for targeted persuasion campaigns. In the digital age, where every interaction leaves a traceable footprint, the line between private and public information becomes increasingly blurred. Organizations that neglect to routinely audit their data handling practices expose themselves to reputational damage. Moreover, individuals must recognize that even seemingly innocuous details shared online may be collated and analyzed by sophisticated tools, turning personal narratives into actionable intelligence for adversaries. Embedding a culture of security awareness through continuous training ensures understanding of the value of seemingly trivial safeguard. Only by treating information security as an evolving, collective responsibility can we hope to mitigate the pervasive vulnerabilities.

This leads to the conclusion that intelligence units must adhere to clearly defined guidelines in order to ensure the quality of their investigations and the reliability of disseminated findings. The publication of the Berkeley Protocol in 2022 represents a significant milestone in the establishment of industry standards for OSINT practices. However, its emphasis lies primarily on procedures and principles, while it does not prescribe specific tools to be employed within the workflow. It is plausible that the United Nations will continue to develop complementary documents dedicated to open-source investigations. Nevertheless, it remains unlikely that such standards will gain universal acceptance. More realistically, distinct frameworks may emerge within individual organisations or at the state level reflecting specific institutional or national requirements.

Standardisation of OSINT practices has become increasingly important in light of threats such as data poisoning, which make the grading of information credibility indispensable. The war in Ukraine has demonstrated that proficiently executed disinformation campaigns can distort decision-making at the state level and result in human casualties. This underscores the necessity of verifying information across multiple dimensions and within a broader context. Raising awareness of these risks must occur at all levels of society, with open discussion on issues such as the use of AI, state-sponsored campaigns, and other manipulative practices. At the same time, any measures taken must remain compliant with legal standards and safeguard fundamental right to privacy.

Furthermore, emergence of artificial intelligence tools and AI-generated content renders OSINT more complex than ever. The relative ease of producing fabricated texts, images, and videos underscores the critical importance of credibility assessment. This task is becoming increasingly challenging as AI technologies advance, rendering synthetic content nearly indistinguishable from that created by humans. As a result large-scale disinformation campaigns can be executed with minimal effort. Introducing systematic measures such as watermarking or labelling AI-generated content on social media platforms represents an essential first step toward mitigating these risks.

The right to privacy enshrined in constitutional provisions and international human-rights instruments guarantees individuals the ability to control how personal information is collected, processed, and disclosed. In contrast, open-source intelligence refers to the systematic gathering of publicly available data from diverse channels with the explicit purpose of generating actionable insights. While privacy law seeks to limit unauthorized intrusions into personal spheres, OSINT operates within the bounds of what is openly disclosed yet the sheer volume and granularity of publicly shared content can blur those boundaries, raising ethical questions about consent and the potential for re-identification. Thus, the tension between protecting individual autonomy and exploiting freely available information underscores a fundamental debate whether the collective utility derived from OSINT justifies intrusions that may erode the very privacy safeguards it ostensibly respects.

The fragile balance between privacy protection and information gathering has prompted social media platforms to introduce new privacy measures. Among recent proposals is the idea of linking social media accounts to government-issued IDs in order to better counter contemporary threats, including the spread of disinformation. While such measures may enhance security, they also risk significantly constraining OSINT practices and pose a substantial threat to individual privacy. At the same time, legislative initiatives such as the UK Online Safety Act and the EU's Chat Control proposal contribute to an uncertain future for the digital environment, with the potential for profound transformations in the coming years. Given that most OSINT relies on publicly available online data, these developments may drastically limit the accessibility of relevant information sources. Indeed, such restrictions are already becoming visible, as an increasing number of websites adopt subscription-based models that reduce open access. If these trends continue, the practice of OSINT could face severe obstacles, potentially reaching a point where rigorous controls make open-source investigations extremely difficult to conduct. In the long term, this trajectory could even resemble forms of censorship reminiscent of the Cold War era.

Despite, open-source intelligence is not a new idea, as it is believed to be, its role in modern world is increasing. Therefore, both pros and cons need to be assessed by both private actors and entire states. Numerous threats and concerns neede to be addressed in advance. Specific guidelines are required on both industrial and state level to leverage the quality of

investigations. Information credibility and validation is to be taken into account to improve overall grade of disseminated results and reduce the impact of disinformation or data poisoning. Impact of AI needs to be carefully considered. Both private and public sector must adhere to security guidelines and OPSEC rules. As the information society develops we may expect OSINT to become inseparable part of our life.

Acknowledgment

This research has been funded by the research component of the grant (0313/SBAD/1314) awarded by the Minister of Science and Higher Education to higher education institutions, intended for conducting scientific research or development-oriented degree projects and related tasks aimed at fostering the development of young researchers.

References

- Block, L., 2024. The long history of OSINT. Journal of Intelligence History, 23(2), pp. 95-109. DOI: 10.1080/16161262.2023.2224091.

- Brantly, A.F., 2022. Narrative Battles: The Impact Open-Source Intelligence on the Framing of Russia's War on Ukraine. SSRN Electronic Journal. DOI: 10.2139/ssrn.4256772.

- Burke, P., 2022. The Issues In The Collection, Verification And Actionability Of Citizen-derived And Crowdsourced Intelligence During The Russian Invasion Of Ukraine, 2022. Strategic Panorama. DOI: 10.53679/2616-9460.specialissue.2022.09.

- Demos, n.d. #Intelligence. [online] Available at: https://demos.co.uk/research/intelligence/ [Accessed 20 Aug. 2025].

- Glassman, M. and Kang, M.J., 2012. Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). Computers in Human Behavior, 28(2), pp. 673-682. DOI: 10.1016/j.chb.2011.11.014.

- Grozev, C., 2018. Full Report: Skripal Poisoning Suspect Dr. Alexander Mishkin, Hero of Russia. Bellingcat, 9 Oct. [online] Available at: https://www.bellingcat.com/news/uk-and-europe/2018/10/09/full-report-skripal-poisoning-suspect-dr-alexander-mishkin-hero-russia

- Khera, V., Prasad, A.R. and Kwanoran, S., 2024. 11 OSINT for Digital Forensics Investigations. In: Open Source Intelligence (OSINT) - A Practical Introduction: A Field Manual. River Publishers, pp. 95-106. [online] Available at: https://ieeexplore.ieee.org/document/10643799 [Accessed 27 Nov. 2024].

- Koops, B.-J., 2013. Police investigations in Internet open sources: Procedural-law issues. Computer Law Security Review, 29(6), pp. 654-665. DOI: 10.1016/j.clsr.2013.09.004.

- Kotaridis, I. and Benekos, G., 2023. Integrating Earth observation IMINT with OSINT data to create added-value multisource intelligence information: A case study of the Ukraine-Russia war. Security and Defence Quarterly. DOI: 10.35467/sdq/170901.

- Liveuamap LLC, 2014. Live Universal Awareness Map (Liveuamap). [online] Available at: https://liveuamap.com/ [Accessed 25 Jun. 2025].

- Matthews, R., Lovell, K. and Sorell, M., 2021. Ghost protocol - Snapchat as a method of surveillance. Forensic Science International: Digital Investigation, 36, p. 301112. DOI: 10.1016/j.fsidi.2021.301112.

- Mitchell, W.L., 2025. Assessing Deception Projection via OSINT: The Case of the Ukraine 2022 Counter-Offensive. Journal of Applied Operational Intelligence. DOI: 10.5750/jaoi.v1i1.2266.

- NATO, 2001. NATO OSINT Handbook V 1.2. [online] Available at: https://archive.org/details/NATOOSINTHandbookV1.2 [Accessed 28 Jul. 2025].

- OHCHR, n.d. 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. [online] Available at: https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source [Accessed Jan. 2025].

- Shafee, S., Bessani, A. and Ferreira, P.M., 2025. Evaluation of LLM-based chatbots for OSINT-based Cyber Threat Awareness. Expert Systems with Applications, 261, p. 125509. DOI: 10.1016/j.eswa.2024.125509.

- Stodelov, D. and Miloslavskaya, N., 2022. Open Source INTelligence Tools. Procedia Computer Science, 213, pp. 83-88. DOI: 10.1016/j.procs.2022.11.041.

- Sufi, F., 2024a. A systematic review on the dimensions of open-source disaster intelligence using GPT. Journal of Economy and Technology, 2, pp. 62-78. DOI: 10.1016/j.ject.2024.03.004.

- Sufi, F., 2024b. An innovative GPT-based open-source intelligence using historical cyber incident reports. Natural Language Processing Journal, 7, p. 100074. DOI: 10.1016/j.nlp.2024.100074.

- Tundis, A., Ruppert, S. and Muhlhauser, M., 2022. A Feature-driven Method for Automating the Assessment of OSINT Cyber Threat Sources. Computers Security, 113, p. 102576. DOI: 10.1016/j.cose.2021.102576.

- Wojnowski, M., 2024. Koncepcja wojny nowej generacji w ujeciu strategow Sztabu Generalnego Sil Zbrojnych Federacji Rosyjskiej. Przeglad Bezpieczenstwa Wewnetrznego, (13/15), pp. 13-39.

- Wosinski, K., 2023. Znaczenie wywiadu opartego na otwartych zrodlach (OSINT) w zapewnieniu bezpieczenstwa systemow teleinformatycznych i bezpieczenstwa osobowego. Uniwersytet Kaliski. [online] Available at: https://uniwersytetkaliski.edu.pl/uczelnia/procedura-postepowania-o-nadanie-stopnia-naukowego-doktora/krzysztof-wosinski/ [Accessed 3 Dec. 2024].

- Yu, S., 2023. Cyber profiling: Predicting political orientation with SOCMINT. Telematics and Informatics Reports, 10, p. 100058. DOI: 10.1016/j.teler.2023.100058.