

ARTICLE

The role and potential applications of open-source intelligence in ensuring the security of the Republic of Poland¹

ANNA NASTUŁA

Independent author

 <https://orcid.org/0000-0002-2061-5067>

Abstract

The aim of this article is to determine the significance and potential applications of open-source intelligence (OSINT) in ensuring state security. The paper discusses theoretical issues related to the characteristics of OSINT, including its methods and means, as well as the legal and non-legal aspects of its use. It also presents the development of OSINT in the United States, the United Kingdom and Israel. Subsequently, the results of empirical research conducted in 2023–2024 are presented. The study employed the method of individual in-depth interviews carried out with 12 experts in the fields of security and OSINT. Based on the the analysis undertaken and findings of the empirical research,

¹ This article is based on a doctoral thesis entitled *The Importance of Open-Source Intelligence in National Security*, defended at the Military University of Technology. The thesis was awarded a prize in the 15th edition of the competition organised by the Head of the Internal Security Agency (ABW) for the best doctoral, master's or bachelor's thesis on national security in the context of intelligence, terrorist and economic threats.

conclusions and recommendations were formulated regarding the possibilities of using open-source intelligence in ensuring the security of the Republic of Poland.

Keywords open-source intelligence, OSINT, security, open-source information, open sources, cybersecurity

Introduction

The role and scale of the use of open-source information are steadily increasing. This is due to the ongoing revolution in information technology, the growing transparency of political processes characteristic of democratic states, and the processes of globalisation. These phenomena are accompanied by a significant increase in the volume of information from open sources, its diversity, and the challenges associated with its analysis. In the face of these challenges, it is reasonable to ask about the role and significance of open-source intelligence (OSINT), the prospects for its development, and – most importantly – the possibilities for utilising it to ensure national security.

National security depends to a large extent on access to reliable and up-to-date information, which constitutes one of the state's strategic assets. Societal and communication changes have contributed to the growing importance of social media as a space for the exchange of information, the shaping of public opinion and the conduct of political discourse. Consequently, decisions relating to national security are increasingly based on information obtained from open sources, which form the basis of open-source intelligence (OSINT). Open-source intelligence is the planned and organised collection and processing of information, followed by the distribution of an analytical product to a specific audience (decision-makers) in a predetermined format, in accordance with a specified information requirement. OSINT sources are legal and publicly available, but access to some may require a certain amount of effort.

The aim of this article is to determine the significance and potential applications of open-source intelligence in ensuring the security of the Republic of Poland. The arguments presented are based on the findings of research carried out by the author as part of her doctoral thesis entitled *The Importance of Open-Source Intelligence in National Security*.

Characteristics of open-source intelligence

In the traditional framework, which has evolved from American military and intelligence terminology based on the types of sources used to gather information, five basic intelligence disciplines are distinguished:

- 1) HUMINT – human intelligence (human sources),
- 2) SIGINT – signals intelligence (electromagnetic sources),
- 3) IMINT – imagery intelligence (imagery sources),
- 4) MASINT – measurement and signature intelligence (measurement and signature sources),
- 5) OSINT – open-source intelligence (open sources of information).

Starting the intelligence-gathering process by exploring open-source information is almost always justified and usually leads to a reduction in the costs associated with other categories of intelligence activities². Security experts believe that it is open-source information gathered from all possible publicly available sources that currently forms the basis of a final intelligence report³. For this reason, it is reasonable to view the aforementioned intelligence disciplines as overlapping, and open-source intelligence as an integral part of all intelligence activities⁴.

Open-source intelligence provides context for ongoing reconnaissance by supplying general knowledge that serves as a starting point for determining its further directions. The usefulness of OSINT stems from its ability to rapidly gather information on a wide range of topics. Another significant advantage is the ability to verify and supplement information with that obtained from closed sources. Widespread access to open sources enables a rapid response to incidents and shortens the time taken to make security-related decisions. Open-source intelligence can provide concise and precise information that allows for the verification of existing assumptions and serves as a sufficient basis for formulating new analytical

² J. Konieczny, *Kryminalistyczny leksykon śledztwa* (Eng. A forensic investigation glossary), Opole 2020, p. 336.

³ A NATO study indicated that over 80% of the information contained in final intelligence products may come from open sources. One of the estimates cited related to intelligence support in the field of counter-proliferation. See: NATO, *Open Source Intelligence Reader*, February 2002, <https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL%20Oct2002.pdf>, p. 17, 73 [accessed: 27 III 2025]. In 2005, W.M. Nolte, a retired senior CIA officer, stated that 95–98% of all information processed by the US intelligence community came from open sources. See: S.D. Gibson, *Open-Source Intelligence: A Contemporary Intelligence Lifeline*, Cranfield University, PhD thesis, 2007, <https://dspace.lib.cranfield.ac.uk/server/api/core/bitstreams/13574c5b-9ba2-4eea-8ef8-fd0d035cb6e8/content>, p. 93 [accessed: 25 VI 2026].

⁴ M.M. Lowenthal, *OSINT the State of Art, The Artless State*, "Studies in Intelligence" 2001, vol. 45, no. 3, p. 63.

hypotheses. An additional advantage of such intelligence is the ease with which the knowledge obtained can be exchanged and disseminated among the bodies responsible for security. Furthermore, it enables analyses to be carried out on an ongoing basis, which is of particular importance in a rapidly changing security environment⁵.

The development of the global network has influenced the evolution of open-source intelligence. The emergence of successive generations of OSINT is linked to the stages of development of the World Wide Web – Web 1.0, Web 2.0 and Web 3.0⁶. Each of them reflects both technological progress and changing needs in the field of open-source intelligence. Figure 1 illustrates the key features of successive generations of OSINT.

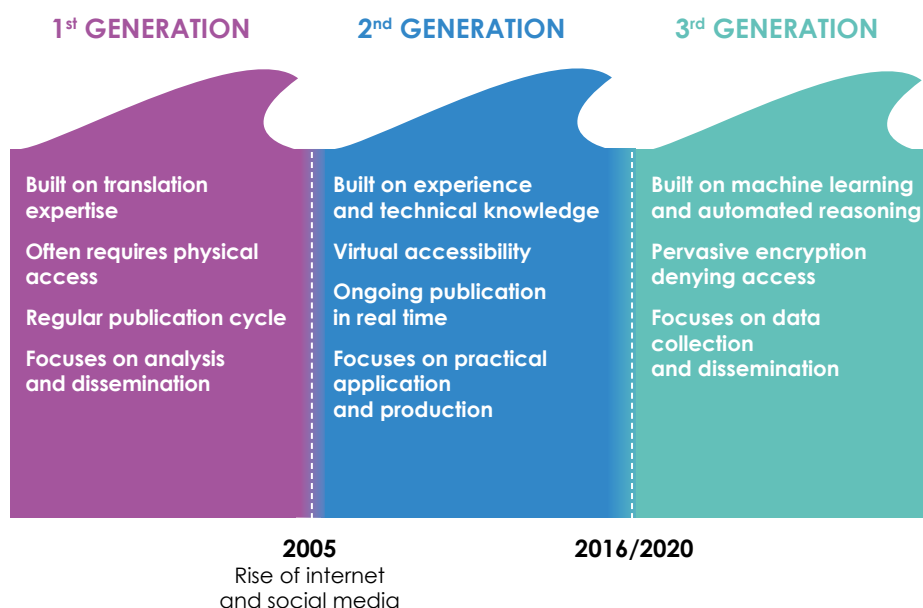


Figure 1. Generations of open-source intelligence.

Source: own elaboration based on: H.J. Williams, I. Blum, *Defining Second Generation Open-Source Intelligence (OSINT) for the Defense Enterprise*, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf, p. 40 [accessed: 27 III 2025].

⁵ S.D. Gibson, *Open Source Intelligence*, in: *The Routledge Companion to Intelligence Studies*, R. Dover, M.S. Goodman, C. Hillebrand (eds.), London 2014, p. 127.

⁶ H.J. Williams, I. Blum, *Defining Second Generation Open-Source Intelligence (OSINT) for the Defense Enterprise*, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf, p. 39 [accessed: 27 III 2025].

The first generation of OSINT was linked to the development of Web 1.0 in the 1990s. It was characterised by a lack of interactivity and simple, one-way communication, the model of which can be compared to the triad of traditional media, namely: the press, radio and television. During this period, intelligence activities were based on the collection, monitoring, analysis and dissemination of information, as well as the translation of foreign materials.

The transition to the second generation of OSINT coincided with the development of Web 2.0 and a shift in the model of communication between website owners and their users. The increase in the interactivity of communication and in user participation in content creation fostered the dynamic growth of social media and the almost continuous publication of information. As a result, the proportion of open-source information used in intelligence operations has increased.

The third generation of open-source intelligence is linked to the development of Web 3.0. This web, referred to as the 'semantic web', enables machine learning and automated reasoning. At this stage in the development of OSINT, augmented reality and psychometrics are also becoming particularly significant, while one of the main challenges is the widespread use of encryption, which restricts access to information⁷.

Key concepts such as open-source data, open-source information, open-source intelligence and verified open-source intelligence, as well as the principles underpinning OSINT, were developed by US intelligence agencies and experts specialising in reconnaissance activities who collaborate within NATO. The process of transforming open-source data into an intelligence product is illustrated in Figure 2.

Open-source data (OSD) is raw data derived from primary sources. It takes the form of printed material, radio and television broadcasts, public oral statements, or other formats, including photographs, audio and audiovisual recordings, commercial imagery, and private correspondence. This data can be classified by format into: structured, semi-structured and unstructured data.

Open-source information refers to data obtained in the first stage and subjected to appropriate processing, which, depending on the nature of the open-source data, may include translation, transcription, format conversion, as well as filtering, correlation, grouping and interpretation. An intelligence product is produced as a result of the integration, assessment and analysis of information carried out to answer specific enquiries. An additional stage involves the multi-source verification of the intelligence product by officers with access to classified information, which

⁷ Ibid., p. 40.

enables the product's reliability to be assessed. A high level of reliability can also be achieved in the case of information derived from an open source whose veracity is beyond doubt. In this way, a verified open-source intelligence product is produced.

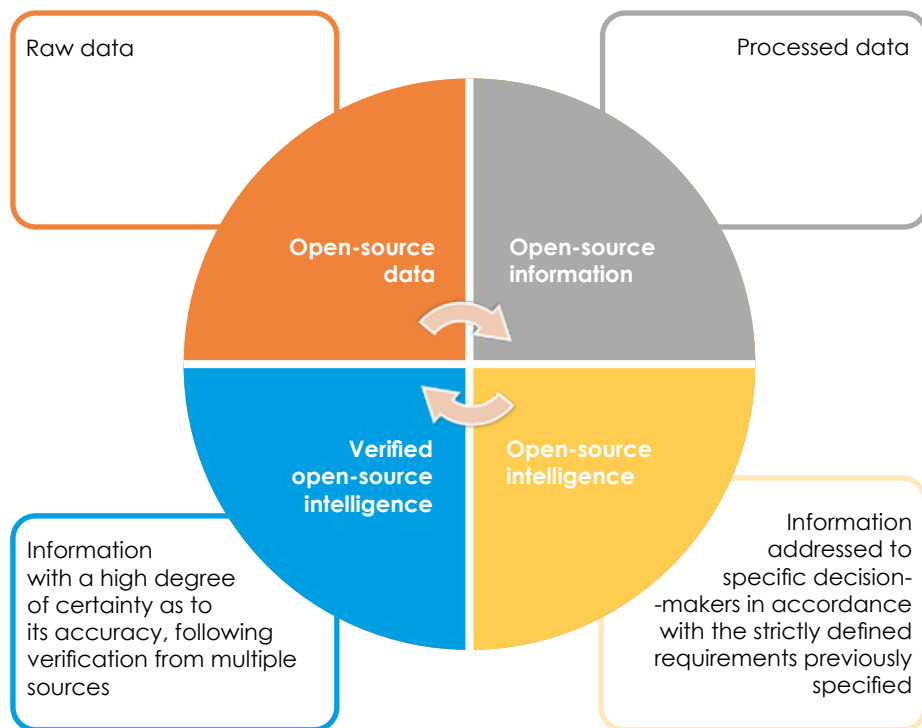


Figure 2. The process of transforming open-source data into an intelligence product.

Source: own elaboration.

Open sources can be classified, according to the channel through which publicly available information is transmitted, as follows: content obtained through observation; documents and printed materials; content broadcast by the media and digital content⁸.

Gathering information through observation involves obtaining it directly from individuals, groups of people or during public events, official contacts and by observing the surroundings. This makes it possible to obtain up-to-date information that is not yet available from formal sources.

⁸ OSINT Foundation, *Mediums of Publicly Available Information*, Document Number: 20230304-01a, 4 III 2023, p. 2. Document is available at the website: <https://www.osintfoundation.com/osint/Standards.asp>, p. 2 [accessed: 25 VI 2026].

Documents and printed materials, including, among others, newspapers, books, reports, official documents and grey literature, constitute the primary source of factual and specialist knowledge, enabling the verification and in-depth analysis of information.

Broadcast media, such as radio, television and other non-internet-based publicly accessible broadcasts, provide information on socio-political, economic and security matters, enabling the public to keep abreast of current events.

Publicly available digital content includes any data that can be downloaded and processed using digital devices, regardless of its format. This category of content includes websites, blogs, social media and other online resources available across all layers of the internet, including the dark web.

The effectiveness of OSINT depends on the correct identification of sources, the selection of appropriate analytical methods, and a critical assessment of the reliability of the information obtained. The rapid development of open sources is leading to a gradual blurring of the boundaries between public and classified information⁹. This requires a change in approach to the classification of information sources and the methods used to analyse them, as well as taking into account new legal and organisational challenges.

OSINT methods and tools in cyberspace

The development of modern technologies has significantly increased the efficiency and precision of gathering information from open sources. When adopting a classification of information gathering based on the four types of open sources used (observation, printed documents, broadcast media, digital content), it should be noted that open-source intelligence now encompasses both traditional methods of information gathering and advanced solutions utilising automation, big data analysis and artificial intelligence. Online sources play a dominant role in contemporary open-source intelligence.

Information can be gathered from the internet either manually or automatically, using specialised tools and scripts. Typical methods of digital OSINT include: monitoring, searching, technical footprinting, social media analysis and web scraping.

Monitoring involves the structured and systematic tracking, over a specified period, of changing content generated by a fixed source.

Searching involves using specialised software or websites to explore the internet in order to find information that meets specific information needs.

⁹ H.J. Williams, I. Blum, *Defining Second Generation...*, p. 37.

Technical footprinting, also known as digital footprint reconstruction, is the process of gathering available information about computer systems, network infrastructure, technologies, services and the entities to which they belong. Thanks to technical footprinting, it is possible to reconstruct a technical and organisational picture of the subject under investigation, identify its digital assets and recognise potential information vulnerabilities based on open-source information.

Social media analysis enables the identification of content, relationships, sentiments, behavioural patterns and communication dynamics in the digital environment. This type of analysis plays a significant role in crisis management, as it enables the monitoring of radicalisation processes, the identification of threats and the forecasting of trends affecting security. Information obtained from social media is used in the fight against crime and terrorism – it supports criminal profiling, including indirect personality assessment, the development of interrogation tactics and the selection of candidates for recruitment as agents¹⁰.

Web scraping involves automatically extracting data from online sources and saving it to a file system or database for subsequent retrieval, processing and analysis.

Methods of gathering information can be categorised, according to the level of interaction with the target, as passive, semi-passive and active¹¹. The choice of the appropriate method depends on the entity conducting the reconnaissance, the purpose and nature of the activities, the type of information being gathered, and operations security (OPSEC) requirements, and should be determined at the planning stage. Semi-passive and active methods require interaction with the target or its infrastructure; they therefore go beyond the classical definition of open-source intelligence, which is based on gathering information without interfering with the target¹². Passive reconnaissance is the primary method of open-source intelligence gathering, given that its aim is to collect information exclusively from open sources and the need to maintain high ethical and security standards in the conduct of such operations.

Open-source information may also be purchased from commercial entities or obtained through outsourcing. Agent programmes and bots are often used for this purpose. However, these solutions require adherence to appropriate ethical standards and compliance with applicable regulations.

¹⁰ See in more detail: J. Konieczny, *Kryminalistyczny leksykon...*, p. 145, 202–203.

¹¹ N.A. Hassan, R. Hijazi, *Open Source Intelligence Methods and Tools. A Practical Guide to Online Intelligence*, New York 2018, p. 14.

¹² In Israel, due to differences in legal standards and socio-historical circumstances, some semi-passive and active methods are regarded as part of open-source intelligence.

Based on the methods used to gather and process open-source information, four main categories of tools can be identified:

- 1) linguistic and textual,
- 2) geospatial,
- 3) based on network theory (network-based),
- 4) utilising visual forensics¹³.

Linguistic tools enable the analysis of large text datasets drawn from multiple sources and languages. They are used to identify keywords, analyse their frequency of occurrence, and draw conclusions about the demographic characteristics, views and behaviours of authors. Sentiment analysis and stance analysis help to determine the emotional tone of statements, as well as the attitudes and intentions of the subjects under study. Natural language processing (NLP) and machine learning are playing an increasingly important role, enabling the automatic analysis of multilingual and unstructured datasets and the identification of linguistic patterns.

Geospatial tools enable the collection and analysis of information that pinpoints the location of people, objects and events in geographical space, thereby supporting the assessment of political, military and crisis situations. The basic methods of geospatial analysis include geotagging, geolocation, geoinferencing and georeferencing¹⁴. They enable the location of objects to be determined, their movements to be tracked and spatial relationships to be identified. Geographical Information Systems, GPS data, satellite and aerial imagery, LIDAR and information published on social media are utilised in these analyses. The integration of geospatial data with other OSINT sources enables the monitoring of armed conflicts, population movements, crisis situations and critical infrastructure, thereby enhancing situational awareness and supporting decision-making processes in the field of national security.

Network analysis tools utilise methods for analysing relationships between people, organisations, places and other entities. This enables the identification of social structures and interdependencies within the networks under study. In open-source intelligence, they are primarily used to analyse social media by searching for, mapping and evaluating relationships between users, utilising computational network analysis and artificial intelligence. Network tools are used, among other things, to identify terrorist and criminal networks, analyse disinformation campaigns and recognise mechanisms for influencing social groups.

¹³ H. Akın Ünver, *Digital Open Source Intelligence and International Security: A Primer*, "Cyber Governance and Digital Democracy", 2018, no. 8, p. 8. DOI:10.13140/RG.2.2.16242.56000.

¹⁴ H.J. Williams, I. Blum, *Defining Second Generation...*, p. 33.

Tools utilising visual forensics are used to extract data from image and video files, enabling the detection of manipulated images and the performance of photogrammetric analysis. Their importance has grown alongside the development of social media and the shift from text-based to media-based communication. The analysis of visual material utilises, among other things, artefact analysis, photogrammetry, metadata analysis, photographic comparison and digital analysis, supported by geospatial data, satellite imagery and drone footage. These methods enable the verification of the authenticity of images and recordings, the detection of manipulation, the geolocation of events and the reconstruction of their sequence, thereby providing evidence-based material. Visual forensics solutions are widely used in intelligence and investigative operations, as well as in documenting human rights violations and armed conflicts.

Development of information technology, automation and artificial intelligence has significantly increased the efficiency and accuracy of open-source intelligence. It has enabled the collection and automatic analysis of vast amounts of data, reduced the time taken to produce intelligence products and enhanced their analytical value. The integrated use of various OSINT tools allows the information obtained to be cross-referenced and verified, providing a more comprehensive and reliable picture of the phenomenon under analysis. However, the effectiveness of their use depends not only on technological capabilities, but also on the analyst's knowledge and practical skills, as well as the appropriate selection of methods and tools.

Legal and non-legal aspects of open-source intelligence

Open-source intelligence operates within a legal framework that has not yet been comprehensively regulated at either national or international level. The lack of clear regulations leads to differences in interpretation and varying practices in the application of OSINT. This may limit its effectiveness while simultaneously increasing the risk to national security. Although the essence of OSINT lies in the use of information from publicly available sources, aggregating this information using modern tools can lead to the identification of individuals – the so-called ‘mosaic effect’. This raises challenges regarding the protection of privacy and personal data. Legal aspects also concern the protection of copyright and databases, which may contain open-source materials. Further considerations arise from the growing role of private entities engaged in OSINT activities, whose operations are influencing the existing model of intelligence information management. Another issue is the collection of information that goes beyond the scope of the query, which

may lead to breaches of the law and ethical standards concerning the protection of privacy and individual dignity.

The fragmentation of legal regulations means that ethical standards serve to complement the law, setting limits on the collection and analysis of information. The automation of processes for collecting and analysing large datasets (Big Data) increases the importance of these standards; however, their voluntary nature does not ensure that emerging risks are effectively mitigated. Both in practice and in the relevant literature, the urgent need to develop a coherent ethical framework for open-source intelligence gathering by state and private entities is emphasised¹⁵.

Other non-legal factors that influence OSINT include methodological and technical considerations. These include, among others, disruptions to the intelligence cycle, cognitive biases on the part of analysts, language issues, and limitations in technical infrastructure and operational security.

Open-source information, due to its accessibility and ease of dissemination, is particularly susceptible to manipulation. The most serious threats to open-source intelligence are disinformation and propaganda, which aim to deliberately distort reality, shape the attitudes of audiences and influence decision-making processes. The development of digital media and information technology has significantly increased the effectiveness of these activities, enabling the rapid dissemination of false narratives and their tailoring to specific audiences. Propaganda now serves not only a persuasive function, but also a mobilising one, and is used to shape socio-political narratives. Disinformation has become one of the key elements of hostile information operations conducted by both states and non-state actors. Its aim is to destabilise the political, social and economic situation and to undermine trust in state institutions. Modern technologies, including artificial intelligence, enable the creation of sophisticated forms of manipulation, such as fake news and deepfakes, the detection of which is becoming an increasingly significant analytical challenge.

At the same time, open-source intelligence plays a significant role in detecting and analysing disinformation and propaganda campaigns. However, effectively countering information manipulation requires the use of modern technologies to support OSINT analysis, as well as the development of analysts' skills and the public's resilience to disinformation.

¹⁵ International research projects have been carried out on the ethical aspects of open-source intelligence, e.g.: The Versatile InfoRmation Toolkit for end-Users oriented Open Sources explOitation (VIRTUOSO, 2010–2013), The Collaborative information, Acquisition, Processing, Exploitation and Reporting for the prevention of organized crime (CAPER, 2011–2014), The Maritime Integrated Surveillance Awareness (MARISA, 2017–2020).

The development of open-source intelligence in the United States, the United Kingdom and Israel

An analysis of the experiences of the United States, the United Kingdom and Israel in the use of open-source intelligence for national security purposes makes it possible to identify the trends to date in the development of OSINT in democratic states with highly developed security institutions and a long-standing tradition of utilising open-source information.

The origins of institutionalised open-source intelligence in the US date back to World War II, when the Foreign Broadcast Monitoring Service (FBMS) was established, which was subsequently transformed on 26 July 1942 into the Federal Broadcast Information Service (FBIS). This organisation was responsible for monitoring, translating and analysing foreign information derived from open sources. In the years that followed, the development of OSINT was supported by, among others, the Foreign Documents Division (FDD) and the Federal Research Division (FRD) of the Library of Congress. The reforms carried out following the end of the Cold War¹⁶ and after the attacks of 11 September 2001¹⁷ were of landmark significance and led to the creation of the Open Source Centre (OSC), and subsequently the Open Source Enterprise (OSE), operating within the structure of the Central Intelligence Agency (CIA).

In March 2024, *the United States Intelligence Community's OSINT Strategy for 2024–2026* was published¹⁸, setting out a comprehensive vision, priorities and directions for the further development of open-source intelligence, as well as measures aimed at strengthening its role within the intelligence system. The strategy's objectives are set out in four key areas:

¹⁶ The 1996 report by the Commission on the Roles and Capabilities of the United States Intelligence Community (commonly known as the Aspin-Brown Commission) contained recommendations regarding the reform of the US Intelligence Community. The authors of the report emphasised the importance of open-source intelligence and the need to adapt intelligence activities to complex and multifaceted threats. See in more detail: *Preparing for the 21st Century: An Appraisal of U.S. Intelligence: Report of the Commission on the Roles and Capabilities of the United States Intelligence Community*, “American Intelligence Journal” 1995, vol. 16, no. 2/3, pp. 11–17.

¹⁷ The need to reform the US intelligence structure, including the establishment of a body responsible for open-source intelligence, was highlighted by the National Commission on Terrorist Attacks Upon the United States (commonly known as the 9/11 Commission) in its report published in 2004. See: *The 9/11 Commission Report*, <https://www.9-11commission.gov/report/911Report.pdf> [accessed: 15 VI 2026].

¹⁸ United States Intelligence Community, *IC OSINT Strategy 2024–2026. The INT of First Resort: Unlocking the Value of OSINT*, https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf [accessed: 15 VI 2026].

1. Coordinating the collection of data from open sources and expanding access to it.
2. Establishing integrated management of open-source information assets.
3. Developing innovation in the field of OSINT to create new analytical and operational capabilities.
4. Training specialists and refining open-source intelligence methodologies¹⁹.

The strategy represents a significant step towards the institutionalisation of OSINT, strengthening its integration with the activities of the US Intelligence Community and reaffirming its importance for analytical and decision-making processes.

The evolution of open-source intelligence in the US has led to its formalisation and professionalisation, and to the consolidation of its role in intelligence activities.

The development of open-source intelligence in the United Kingdom has the longest documented history of all the countries analysed. A significant role in its development was played by BBC Monitoring, established in 1939, which was responsible for monitoring, translating and analysing foreign sources of information. Following the end of the World War II, international cooperation within the framework of the Five Eyes alliance became an integral part of the British security system²⁰, facilitating the exchange of open-source information and the coordination of intelligence operations. Open-source intelligence is also utilised by the British police and security services, such as the Security Service (MI5) and the Secret Intelligence Service (MI6). It supports the prevention of terrorism, the fight against crime and countering hybrid threats.

The rules governing the use of open-source information by law enforcement agencies in the United Kingdom have been set out by the National Police Chiefs' Council (NPCC). In its guidelines, the NPCC emphasises, among other things, the need to comply with the law, to ensure that actions are proportionate, and to respect the right to privacy and the protection of personal data²¹. For its part, the British Ministry of Defence (MOD) has incorporated OSINT into its intelligence

¹⁹ Ibid., p. 1.

²⁰ Five Eyes – an intelligence partnership between the United States, the United Kingdom, Canada, Australia and New Zealand, founded on a British-American agreement concluded on 5 March 1946. The cooperation involves the exchange of information gathered through various intelligence disciplines, including open-source intelligence.

²¹ J. Housego, *NPCC Guidance on Open Source Investigation/Research*, April 2015, <https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/disclosure-logs/workforce-coordination-committee/2023/061-2023-07-published-npcc-guidance-osint---reserach.pdf>, pp. 4–5 [accessed: 14 VIII 2026].

doctrine, defining it as intelligence derived from publicly available information and other unclassified information with restricted access or distribution²².

Cooperation with the private sector and the academic community, carried out, among other things, through the OSINT Hub operating within CENTRIC²³, fosters the development of modern tools, skills and innovative methods for gathering and analysing open-source intelligence. This model is complemented by the activities of specialised non-governmental organisations and private entities, such as the Association of British Investigators and the UK OSINT Community, which promote the development of skills, standards and best practice in the field of OSINT. Meanwhile, the achievements of Bellingcat and the BBC have confirmed the importance of open-source intelligence in documenting armed conflicts, human rights violations and countering disinformation, including in relation to Russia's aggression against Ukraine²⁴.

The British model of open-source intelligence is characterised by an approach that combines the development of organisational and legislative aspects, international cooperation, and the utilisation of the potential of the private sector and the academic community.

Israel's intelligence activities are regarded as the most effective in the world. At the same time, analysing the Israeli model of OSINT utilisation poses a research challenge due to the limited availability of official information. This limitation stems from the country's geopolitical and historical circumstances, as well as the ability to deliberately shape the narrative and distort information available in open sources as part of disinformation campaigns.

An analysis of the training programme for European intelligence services launched by the Mossad in 2021 indicates that open-source intelligence is used extensively in the operational activities of Israeli intelligence²⁵. The programme emphasises the importance of integrating open-source information with data from other

²² Ministry of Defence, *Joint Doctrine Publication 2-00. Understanding and Intelligence Support to Joint Operations*, 3rd Edition, August 2011, <https://www.yumpu.com/en/document/read/5888415/jdp-2-00-3rd-edition-understanding-and-intelligence-support-to-/3>, pp. 2-12, point 227 [accessed: 14 VIII 2026].

²³ OSINT Hub. *CENTRIC open source intelligence hub*, CENTRIC, <https://centric-research.co.uk/projects/osint-hub> [accessed: 15 VI 2026].

²⁴ A. Janjeva, A. Harris, J. Byrne, *The Future of Open-Source Intelligence for UK National Security*, 2022, https://static.rusi.org/330_OP_FutureOfOpenSourceIntelligence_FinalWeb0.pdf, p. 11 [accessed: 25 VI 2026].

²⁵ *Mossad trains European intel agents in open source spy tools analysis*, Intelligence Online, 20 VII 2022, <https://www.intelligenceonline.com/government-intelligence/2022/07/20/mossad-trains-european-intel-agents-in-open-source-spy-tools-analysis,109800613-gra> [accessed: 18 VI 2026].

intelligence sources, the development of modern methods of information gathering and analysis, and cooperation between Israeli intelligence and the private sector.

Both Shin Bet, which is responsible for internal security, and Aman, the military intelligence service, use OSINT to supplement information obtained from other intelligence sources. An example of the effective use of analysis of communications conducted via social media and instant messaging services was the foiling of attacks planned by Al-Qaeda on the US Embassy in Tel Aviv and the International Convention Center in Jerusalem²⁶.

Within Aman, Unit 8200 specialises in signals intelligence (SIGINT). A cell called Hatzav, responsible for open-source intelligence, has been established within its structure. The evolution of social media has led to an expansion of Hatzav's activities from monitoring traditional Arabic media to analysing information published in real time on websites. This has been significant both tactically, enabling the monitoring of information relating to specific operations, and strategically, allowing for the analysis of public sentiment. Hatzav developed specialised analytical tools and a training model based on language proficiency, knowledge of social media and IT skills. In 2021, Hatzav was disbanded and its responsibilities dispersed. Opponents of this decision pointed to an over-reliance on technical methods of information gathering at the expense of analyses carried out by specialist OSINT analysts.

The experiences of the war following 7 October 2023 led to the re-establishment of Hatzav and the rebuilding of the services' open-source intelligence capabilities. The decision to reactivate the unit confirmed that OSINT constitutes a distinct form of intelligence gathering that complements other intelligence disciplines. It cannot be replaced solely by advanced technological solutions and artificial intelligence, which fail to capture, for example, linguistic and cultural nuances such as political context, social conditions or institutional memory²⁷.

A comparative analysis of the development and use of open-source intelligence in the United States, the United Kingdom and Israel shows that all the countries analysed recognise the growing importance of information derived from open sources and its significant impact on security. Differences are evident both in terms of definition and in the way open-source intelligence is perceived. The United States and the United Kingdom focus on the parallel development of its organisational

²⁶ M. Ginsburg, T. Staff, *Al-Qaeda planned to blow up US Embassy in Tel Aviv, Jerusalem convention center*, The Times of Israel, 22 I 2014, <https://www.timesofisrael.com/al-qaeda-targeting-us-embassy-jerusalem-convention-center/> [accessed: 25 IV 2024].

²⁷ A. Bohbot, *IDF revives disbanded Hatzav intelligence unit amid regional threats*, The Jerusalem Post, 22 VI 2025, <https://www.jpost.com/israel-news/defense-news/article-858491> [accessed: 25 VI 2026].

and legislative aspects, while in Israel, OSINT plays only a supporting role, serving as a guide for undertaking complex operational activities.

At the same time, all the countries analysed are witnessing rapid development and widespread use of modern technologies, including artificial intelligence and Big Data, which necessitates further investment in technological infrastructure and the development of analytical methods. These technologies are being applied, respectively, to the development of OSINT tools in the US, police operations and the monitoring of internal threats in the UK, and the integration of open-source intelligence with cybersecurity operations in Israel.

Another common feature is the fragmentation of open-source intelligence activities and responsibilities among public bodies. This leads to limited cooperation between institutions, insufficient funding for operational needs, and variations in the level of access and methods of data collection.

Open-source intelligence capabilities remain a key area requiring further development, with shortcomings still being identified in the United States and the United Kingdom in the analysis, selection, integration and distribution of open-source information throughout the intelligence cycle. Israel, on the other hand, is developing these capabilities in cooperation with the private sector, including the transfer of knowledge and technology, as well as training activities.

A common trend in all the countries analysed is also the strengthening of international cooperation, both within alliances such as the Five Eyes and through partnerships with the private sector, which serve to facilitate the exchange of information, coordinate actions, develop modern technologies and enhance intelligence and cybersecurity capabilities.

The analysis carried out indicates that the United States, the United Kingdom and Israel are systematically increasing their use of open-source intelligence, thereby strengthening their capabilities in both defensive and offensive operations.

The use of OSINT and the state's capabilities in countering threats. Research findings

The aim of the research carried out by the author as part of the preparation of her doctoral thesis was to gather qualitative information enabling the identification of the relationship between the use of open-source intelligence and the state's capabilities in countering internal and external threats. The aim was also to obtain forecasts regarding the future development of methods and technical means used to gather and analyse open-source information for the purpose of ensuring national security.

The study was carried out from December 2023 to April 2024, which made it possible to maintain relatively stable research conditions with regard to both the legal and non-legal aspects of the use of open-source intelligence, the geopolitical context, and the methods and technical means employed in open-source intelligence gathering. The method of individual in-depth interviews (IDI) was employed. Twelve experts, selected according to specific criteria, were invited to participate in the research. These were individuals possessing specialist knowledge and extensive professional experience in the field of security and OSINT. Some of them had been involved, after 1990, in the establishment of organisational units dealing with open-source intelligence in Poland. The respondents included former and serving officers of the Internal Security Agency, the Police, the Border Guard, the GROM Military Unit, the Territorial Defence Forces and the Cyber Defence Forces; a representative of the government administration employed in the Department of Cybersecurity at the Ministry of Digital Affairs; a researcher specialising in intelligence and national security issues; a detective; and an investigative journalist who had previously served as director of an analysis and information office. The research tool was *an interview script designed for experts who utilise open-source intelligence in their professional work*, comprising 11 questions concerning the respondents' experiences with the use of OSINT and their assessment of its significance for national security.

Experts consistently emphasised that open-source intelligence plays a vital role in ensuring national security, supporting decision-making processes at all levels of governance, from local to international. Integrating open-source information with operational intelligence at an early stage of analysis enhances understanding of the issue and improves the effectiveness of operational planning. Respondents also emphasised that advances in information technology and the evolving security environment are steadily increasing the importance of OSINT, although its potential is not being fully utilised, particularly in supporting the country's economic and strategic development.

The survey participants predict that the use of modern technologies, including artificial intelligence and advanced Big Data tools, will lead to further development and increased efficiency in the use of open-source intelligence within the security sector. The automation of processes for gathering and analysing open-source information, supported by machine learning algorithms, enables broader and, above all, continuous monitoring of open sources. This makes it possible to reduce the time required to process information, which in turn enhances the ability to identify and assess threats and contributes to a faster response to them. Artificial intelligence-based tools streamline the analysis of text, images, audio and other multimedia content, as well as the identification of patterns, correlations and trends, and the analysis of social media. Experts emphasised that, among the methods used

in OSINT, predictive analysis, semantic analysis and social network analysis are of particular importance. At the same time, the integration of OSINT methods and tools enables a multi-faceted analysis of information from various sources, enhancing the ability to identify relationships, detect threats and support decision-making processes in the field of national security.

An analysis of these statements indicates that the legal and non-legal conditions governing open-source intelligence gathering have a significant impact on its effectiveness, with the greatest challenge remaining the manipulation of information, including disinformation campaigns, propaganda, fake news and information overload. The aggregation and processing of open-source information, despite having been obtained legally, may lead to the identification of individuals, which raises significant legal and ethical challenges in the area of privacy and personal data protection. The effectiveness of OSINT use is also influenced by technological, economic and organisational factors, in particular limited access to specialist tools, the high costs of implementing them, and insufficient cooperation between institutions. Another significant barrier is the inadequate level of analytical skills, lack of experience, psychological aptitude and specialist training among officers.

Based on the interviews conducted, it can be concluded that one of the main areas of development for open-source intelligence in democratic states is the strengthening of international cooperation and the exchange of information with allied states. International cooperation helps to enhance states' ability to identify and assess global threats, such as terrorism, cyber-attacks and disinformation, thereby supporting decision-making processes in the field of security. The effectiveness of this cooperation requires the application of uniform security standards, adherence to ethical principles and compliance with applicable legal regulations. At the same time, experts emphasised that international cooperation requires particular caution and careful selection of the materials shared, so as not to disclose to allies information that might reveal a country's vulnerabilities, especially in the context of changing geopolitical conditions and the differing priorities of individual allies.

Conclusions and recommendations for Poland

The ever-increasing volume of open-source information, coupled with the rapid development of information technology, is leading to a steady rise in the importance of open-source intelligence as an integral part of intelligence processes. The use of modern technologies enhances the efficiency of gathering, processing and analysing open-source information, while reducing response times to threats.

Legal and non-legal factors influence the effectiveness of OSINT. One of the greatest challenges in this area remains disinformation, the effective countering of which requires the integration of technological, organisational, legal and educational measures. The lack of uniform regulations and the ambiguity of key concepts can lead to legal uncertainty and divergent interpretations, limiting the effectiveness of open-source intelligence. Its effective use therefore depends on the implementation of legal, organisational and technical measures that ensure consistency in the actions of the bodies responsible for national security.

Open-source intelligence plays a vital role in supporting decision-making processes in the field of national security by identifying and assessing threats and building situational awareness. At the same time, cooperation and the exchange of information with allied states, the private sector and the academic community can lead to more effective monitoring of global threats, the standardisation of analytical methods and an improvement in the quality of intelligence products.

Based on the conclusions drawn from theoretical analysis and empirical research, the author has formulated recommendations aimed at improving the use of open-source intelligence for the benefit of Poland's security. Implementing these recommendations could enhance cooperation between the bodies responsible for national security, increase the efficiency of open-source information management, and reduce the risk of errors arising from the interpretation of such information. Consequently, it would be possible to enhance the state's capacity for the early detection and assessment of threats, to plan security measures more effectively, and to utilise open-source information better in decision-making processes. The recommendations, which could also form part of the further modernisation of security structures, cover four areas.

1. Clarification of terms relating to open-source intelligence within the Polish legal system

Defining the basic concepts relating to open-source intelligence will help to minimise differences in interpretation and precisely define the scope of the collection and analysis of open-source information. Consequently, this will reduce the risk of breaching regulations concerning the protection of personal data, the right to privacy, copyright and other sector-specific regulations. The introduction of appropriate legal regulations will ensure transparency in the operation of open-source intelligence and lay the foundations for the development of uniform procedures, standards and best practices in the conduct of OSINT activities, thereby contributing to its standardisation and professionalisation. A coherent legal framework will increase confidence in the results of OSINT analyses and their potential use in decision-making processes. It will also create the conditions for

the secure implementation of tools utilising modern technologies, including artificial intelligence, in the analysis of open-source information. Aligning regulations with international standards will also improve international cooperation in this area.

This recommendation is in line with trends in the development of open-source intelligence in the United States and the United Kingdom, where organisational and legislative aspects are being improved in parallel.

2. Establishment of the Open-Source Intelligence Coordination Team

A team reporting directly to the Prime Minister and comprising representatives of the security services and government agencies would ensure the coordination of the state's activities in the field of open-source intelligence. Its operation would help to speed up the processes of gathering and analysing open-source information, eliminate duplication of effort, improve the cost-effectiveness of operations and optimise the use of resources. The development of coherent analytical products, based on open-source information gathered by various entities, would enhance the comprehensiveness of analyses and the state's ability to identify and counteract disinformation campaigns.

The team's remit would include initiating, coordinating and monitoring activities undertaken by government administrative bodies in the field of open-source intelligence. The team would carry out tasks relating to the preparation and provision of source data and open-source analyses to the secret services, bodies responsible for national security – including the President of the Republic of Poland, the Prime Minister, the Marshals of the Sejm and the Senate, the Council of Ministers in accordance with the distribution list, the Minister coordinating the special services, the heads of the individual services, and the public. The team would also prepare open-source analyses in the form of bulletins, reports or periodic analytical studies intended for the public, made available in accordance with national security requirements. In this way, it would support efforts to counter disinformation.

A key area of its work would be organising international cooperation in the field of open-source intelligence and preparing comprehensive analyses of threats to Poland and its allies. This group's remit would also include drafting ethical standards, procedures for conducting OSINT, and guidelines on the tools used to gather and analyse information. Furthermore, the team would draw up proposals to improve the methods and tools used by public bodies and monitor trends in disinformation campaigns, as well as the open sources used to generate and disseminate them.

This recommendation is in line with the measures set out in the *US Intelligence Community's OSINT Strategy for 2024–2026*²⁸, which emphasises the importance

²⁸ United States Intelligence Community, *IC OSINT Strategy 2024–2026...*

of central coordination, common standards and the integration of activities in the field of open-source intelligence.

3. Creation of a government platform for the exchange of open-source information as a shared space for searching for, linking and promoting open-source materials

The establishment of a centralised government OSINT platform will provide all bodies responsible for national security with access to a shared space for gathering, integrating and sharing open-source information. This will enhance the efficiency of the exchange of open-source information between bodies responsible for national security, streamlining their cooperation and the exchange of best practice. Shorter timescales for identifying threats and producing analytical materials will, in turn, enhance the effectiveness of decision-making processes and optimise the use of human, technical and financial resources. Furthermore, the integrated OSINT platform will enable comprehensive analyses to be carried out, taking into account the broader context of threats and the interrelationships between them, going beyond the scope of the tasks carried out by individual services.

This recommendation is supported by the measures being implemented in the US and the UK. Both the American concept of shared OSINT platforms linked to a centralised, multi-domain catalogue of publicly and commercially available information²⁹, and the British INDEX platform³⁰, are based on the centralisation of resources, ensuring the interoperability of systems, and the creation of a shared space for the collection and exchange of open-source information, reports and OSINT tools. These solutions aim to eliminate duplication of effort between individual institutions, harmonise analytical standards and increase the use of modern technologies, such as machine learning and advanced analytical methods, in information analysis processes. Their implementation serves as an important point of reference when designing Polish systemic solutions in the field of open-source intelligence.

4. Establishment of the Open-Source Intelligence Innovation Incubator

The aim of the initiative is to develop cooperation between the public administration, the private sector, the academic community and civil society in the field of open-source intelligence. This would result in the exchange of knowledge and experience,

²⁹ Ibid., p. 3.

³⁰ J. Hugill, *Introducing INDEX – A cross-government digital information and data exchange*, PUBLIC, 18 X 2021, <https://www.public.io/blog-post/introducing-index-a-cross-government-digital-information-and-data-exchange> [accessed: 25 VI 2026].

the development of innovative OSINT methods and tools, and the building of lasting relationships that support the security of the Republic of Poland.

This model would enable the organisation to draw on the knowledge and experience of former intelligence officers with operational experience, as well as experts in modern technologies, who would form the incubator's staff. The synergy of their expertise would foster the development of innovative solutions in the field of open-source intelligence.

Cooperation with the private sector would enable the acquisition of modern technologies and the secure outsourcing of selected processes relating to the collection and analysis of information, while optimising costs through the co-funding of research, technological development and innovative projects.

The core tasks of the Open-Source Intelligence Innovation Incubator would include the creation of new technologies and tools, and the development of methods used in open-source intelligence, including the development of algorithms to support the analysis of open-source information. Another key area of its activity should be the recruitment of staff with a diverse range of professional skills and experience, reflecting the interdisciplinary nature of OSINT. The Incubator would also be responsible for organising training and educational activities aimed at both intelligence officers and staff of public finance sector bodies, as well as the general public. Furthermore, its remit would include organising conferences and symposia at government and local authority level, and developing cooperation with the private sector, academic centres and research institutions with a view to jointly developing innovative solutions in the field of OSINT.

The case for establishing such an incubator is supported by Israel's experience – the launch of the CyberSpark Innovation Arena, a joint venture between the Israeli public administration, the academic community and the industrial sector, aimed at fostering innovation and cooperation in the field of cybersecurity³¹. This initiative demonstrates that integrating the potential of government, academia and industry fosters the development of human capital, the transfer of knowledge and technology, and the strengthening of the state's capabilities in gathering and analysing open-source information.

³¹ *Prime Minister Announces National Cyber Hub*, Americans for Ben-Gurion University, 28 I 2014, <https://americansforbgu.org/prime-minister-announces-national-cyber-hub/> [accessed: 27 VI 2026]; *Cyberspark*, World Economic Forum, <https://www.weforum.org/organizations/cyberspark/> [accessed: 27 VI 2026].

Summary

Intelligence processes are closely linked to information, technology and the evolving security environment. The growing number of open sources, often available in real time, enables a faster response and provides answers to decision-makers' current information needs. Nowadays, the time taken to make decisions is one of the key factors determining the level of security and the maintenance of operational continuity. Information obtained through open-source intelligence not only complements information gathered through operational means, but also helps to reduce the time required to make a decision. This enhances the effectiveness of the state's actions in both defensive and offensive terms.

The specified circumstances highlight the need to change the way in which the role of OSINT is perceived by those responsible for national security, as well as the model of cooperation regarding the exchange of open-source information between intelligence services and public administration bodies. The implementation of comprehensive systemic solutions enabling the effective integration, analysis and use of information from open sources may contribute to increasing the effectiveness of operations and improving their cost-effectiveness by reducing the costs of information gathering.

The importance of open-source intelligence will steadily increase as our lives become increasingly digital and the volume of data in open sources grows.

In the face of increasingly complex threats to Poland's security, the need for reliable and verified information has never been greater. It is therefore a challenge to make effective use of the potential of open-source intelligence for the defence of the Republic of Poland and its strategic interests.

Bibliography

Akın Ünver H., *Digital Open-Source Intelligence and International Security: A Primer*, "Cyber Governance and Digital Democracy" 2018, no. 8. DOI:10.13140/RG.2.2.16242.56000.

Gibson S.D., *Open Source Intelligence*, in: *The Routledge Companion to Intelligence Studies*, R. Dover, M.S. Goodman, C. Hillebrand (eds.), London 2014.

Hassan N.A., Hijazi R., *Open Source Intelligence Methods and Tools. A Practical Guide to Online Intelligence*, New York 2018.

Konieczny J., *Kryminalistyczny leksykon śledztwa* (Eng. A forensic investigation glossary), Opole 2020.

Lowenthal M.M., *OSINT the State of Art, The Artless State*, “Studies in Intelligence” 2001, vol. 45, no. 3, pp. 61–66.

Preparing for the 21st Century. An Appraisal of U.S. Intelligence. Report of the Commission on the Roles and Capabilities of the United States Intelligence Community, “American Intelligence Journal” 1995, vol. 16, no. 2/3, p. 11–17.

Internet sources

Bohbot A., *IDF revives disbanded Hatzav intelligence unit amid regional threats*, The Jerusalem Post, 22 VI 2025, <https://www.jpost.com/israel-news/defense-news/article-858491> [accessed: 25 VI 2026].

Cyberspark, World Economic Forum, <https://www.weforum.org/organizations/cyberspark/> [accessed: 27 VI 2026].

Gibson S.D., *Open-Source Intelligence: A Contemporary Intelligence Lifeline*, Cranfield University, PhD thesis, 2007, <https://dspace.lib.cranfield.ac.uk/server/api/core/bitstreams/13574c5b-9ba2-4eea-8ef8-fd0d035cb6e8/content> [accessed: 25 VI 2026].

Ginsburg M., Staff T., *Al-Qaeda planned to blow up US Embassy in Tel Aviv, Jerusalem convention center*, The Times of Israel, 22 I 2014, <https://www.timesofisrael.com/al-qaeda-targeting-us-embassy-jerusalem-convention-center/> [accessed: 25 IV 2024].

Hugill J., *Introducing INDEX – A cross-government digital information and data exchange*, PUBLIC, 18 X 2021, <https://www.public.io/introducing-index-a-cross-government-digital-information-and-data-exchange/> [accessed: 25 VI 2026].

Janjeva A., Harris A., Byrne J., *The Future of Open-Source Intelligence for UK National Security*, 2022, https://static.rusi.org/330_OP_FutureOfOpenSourceIntelligence_FinalWeb0.pdf, [accessed: 25 VI 2026].

Mossad trains European intel agents in open-source spy tools analysis, Intelligence Online, 20 VII 2022, <https://www.intelligenceonline.com/government-intelligence/2022/07/20/mossad-trains-european-intel-agents-in-open-source-spy-tools-analysis,109800613-gra> [accessed: 18 VI 2026].

OSINT Hub CENTRIC open source intelligence hub, CENTRIC, <https://centric-research.co.uk/projects/osint-hub> [accessed: 15 VI 2026].

Prime Minister Announces National Cyber Hub, Americans for Ben-Gurion University, 28 I 2014, <https://americansforbgu.org/prime-minister-announces-national-cyber-hub/> [accessed: 27 VI 2026].

The 9/11 Commission Report, <https://www.9-11commission.gov/report/911Report.pdf> [accessed: 15 VI 2026].

Williams H.J., Blum I., *Defining Second Generation Open-Source Intelligence (OSINT) for the Defense Enterprise*, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf [accessed: 27 III 2025].

Other documents

Housego J., *NPCC Guidance on Open Source Investigation/Research*, April 2015, <https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/disclosure-logs/workforce-coordination-committee/2023/061-2023-07-published-npcc-guidance-osint---reserach.pdf> [accessed: 14 VIII 2026].

Ministry of Defence, *Joint Doctrine Publication 2-00. Understanding and Intelligence Support to Joint Operations*, 3rd Edition, August 2011, <https://www.yumpu.com/en/document/read/5888415/jdp-2-00-3rd-edition-understanding-and-intelligence-support-to-/3> [accessed: 14 VIII 2026].

NATO, *Open Source Intelligence Reader*, February 2002, <https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL%20Oct2002.pdf> [accessed: 27 III 2025].

OSINT Foundation, *Mediums of Publicly Available Information*, Document Number: 20230304-01a, 4 III 2023. Document is available at the website: <https://www.osintfoundation.com/osint/Standards.asp> [accessed: 25 VI 2026].

United States Intelligence Community, *IC OSINT Strategy 2024–2026. The INT of First Resort: Unlocking the Value of OSINT* https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf [accessed: 15 VI 2026].

Anna Nastuła, PhD

PhD in security sciences (Jarosław Dąbrowski Military University of Technology in Warsaw), lawyer, certified lead auditor for ISO/IEC 27001, AQAP 2110:2016 and ISO 9001:2015. Data protection officer, providing services to public and private sector organisations. She delivers training courses and workshops on personal data protection and cybersecurity. Speaker at national and international conferences. Author of academic publications in the fields of law and cybersecurity.

Contact: anna.nastula@arkadiapolska.com

