

OSINT CHRONICLE



Quarterly paper series introducing
the world of open sources

OSINT CHRONICLE





Quarterly paper series introducing
the world of open sources



The four-part series of papers on Open Source Intelligence (OSINT) provides a quarterly insight into the profound world of this intelligence gathering discipline. The series starts on April 8, 2024 and continues on the first Monday of each subsequent quarter. The papers are designed to shed light on different facets of OSINT in order to provide readers with an in-depth understanding of the subject matter. Each paper will therefore focus on a different key area.

The first paper will be dedicated to the basic pillars of OSINT, starting with the history, definitions and funda-

mental concepts. The second paper will focus on the necessary skills and abilities as well as holistic training approaches to excel in the discipline. The third part will cover the legal framework and ethical issues surrounding the subject. It will provide a unique insight into the challenges and uncertainties of this discipline. The final fourth paper will conclude by exploring the current technological status quo of OSINT, presenting the latest trends and analyzing the discrepancies between theory and practice.

Date		Paper-topic
08.04.2024		Historical derivation and definition of OSINT
01.07.2024		Holistic training/training approaches
02.09.2024		Legal and ethical challenges/uncertainties
07.01.2025		Technological status quo

Follow the series for in-depth insights into the intelligence discipline OSINT.

A cooperation of the companies ESG Elektroniksystem- und Logistik-GmbH,
Munich Innovation Labs GmbH and PREVENY GmbH

On the Trail of OSINT

The Evolution and Foundations of Open Source Intelligence

1 Abstract

The topic of "Open Source Intelligence" (OSINT) is currently receiving unprecedented attention. Yet fundamental scientific publications that comprehensively penetrate the intelligence discipline are still missing. This paper aims to address this opacity of the topic and provides in-depth insights into the foundations of OSINT. To this end, the paper discusses the evolutionary stages of OSINT, examines the terms "Open Source Data" (OSD) and "Open Source Information" (OSINF), reveals the distinction between OSINT and the other "intelligence gathering disciplines" and outlines the phases of intelligence creation based on the "Intelligence Cycle".

2 Introduction

OSINT is currently a more frequently discussed topic than ever before. Gaining knowledge from data available to the public [1] has been irrefutably important since the Russian invasion of Ukraine in 2022 at the latest. Real-time analysis, especially of social media, has revealed highly relevant intelligence on smartphone videos and posts in this context [2,3]. Such information is, in turn, adopted by other countries to help shape public opinion around the world [2] or is utilized by research collectives such as Bellingcat [4] for investigative journalism. However, the term OSINT is also omnipresent beyond the Ukrainian-Russian war. It can, for instance, also be encountered in relation to the "Panama Papers" [5,6], which embody the biggest information leak in history [7,8]. Data journalists, who are consulted as OSINT experts for verification work, have established themselves as indispensable in this regard [5].

Nevertheless, OSINT is not a new concept, but dates back long before the emergence and use of the internet [9,10]. It is one of the oldest intelligence disciplines of all [11]. Despite numerous attempts to define OSINT or develop standardized frameworks [cf. e.g., 12-14], the concept of (intelligent) analysis remains controversial

in the relevant literature to this day [15-17]. This is not least due to the fact that every definition of OSINT is subject to advances in computer and data science, which continuously produce improvements in (intelligent) collection and analysis possibilities [16,17]. In addition, technological progress is accompanied by numerous new open means of communication, which have caused a veritable "information explosion" [14,1,12]. This, in turn, requires the continuous generation of new verification and assignment mechanisms [18,1]. Along with this, the developments of the 21st century have provoked numerous debates about whether and how OSINT should be distinguished from the related, classified intelligence gathering disciplines [17,3]. Technologies originally reserved for defense and intelligence agencies are now accessible to the general public, primarily via the internet [12,17]. As a result, the understanding of intelligence has changed completely [19]. Previous definitions of OSINT should therefore always be viewed in their historical context [17]. Moreover, the increasing speed of development makes it almost impossible to give predictions about the future shape of OSINT and its consequences [20]. Thereby, not only individuals and organizations are affected, but also society as a whole [16].

To date, however, there has been a lack of decisive fundamental scientific publications to penetrate the opacity of the subject area [21]. In order to address these problems and create a solid knowledge base as well as systematically explore the research field of OSINT more in depth, this paper first provides a comprehensive review of the relevant definitions over the course of history. In addition, the terms OSD, OSINF and "intelligence", which are directly linked to the definition of OSINT, are explained in more detail to gain a comprehensive understanding [22]. Furthermore, the distinction between OSINT and other intelligence gathering disciplines is discussed and the phases of intelligence creation are presented by means of the Intelligence Cycle.

3 Evolution of Open Source Intelligence (OSINT)

In light of the historical background, OSINT can be divided into three "generations". These run through history in a wave-like pattern (see Fig. 1), corresponding to the ascending and descending importance of the topic [17].

3.1 First Generation Open Source Intelligence (OSINT)

Although the terminology OSINT is modern, its techniques date back far before the internet [3,22,23,9]. The collection of information from public, unclassified, legally accessible sources is thus as traditional [3] as any other intelligence practice [11,10]. It originated in Great Britain in 1939 (some sources even point back to its origins as far as the 16th century, starting independently in various countries [24]). The British government commissioned the "British Broadcasting Corporation" (BBC) to investigate and summarize foreign print media and radio, which were becoming increasingly important at the time. A compilation was published in the form of the "Digest of Foreign

Broadcasts", known today as "BBC Monitoring" [25,10]. In 1941, with the founding of the "Foreign Broadcast Monitoring Service" (FBMS), the first official OSINT facility followed in the US. Its task was to monitor, filter, transcribe, translate and archive news and information from (foreign) media sources [9,26,10,17]. Just one year later, in 1942, when the US entered the Second World War, the "Office of Strategic Services" (OSS) was founded [27,10]. With this, the foundation was laid for modern intelligence research and analysis as well as the future Central Intelligence Agency (CIA) [27]. In this initial phase of OSINT, also referred to as the "first generation" or "first level" of OSINT, the focus was on the physical collection of publicly available information material. The subsequent evaluation and analysis of it was purely manual [19,16,28,17]. The focus of the activity was thus on the ability of an analyst to find and coordinate relevant information and to assemble it into a meaningful whole in a transparent manner [28,9]. This type of classic OSINT reached its peak during the Cold War and became an established intelligence gathering discipline during its course. [11,19,10]. In 1948, this led to an official cooperation between the BBC and the "Foreign Broadcast Intelligence Service" (FBIS), previously known as FBMS [26], with the aim

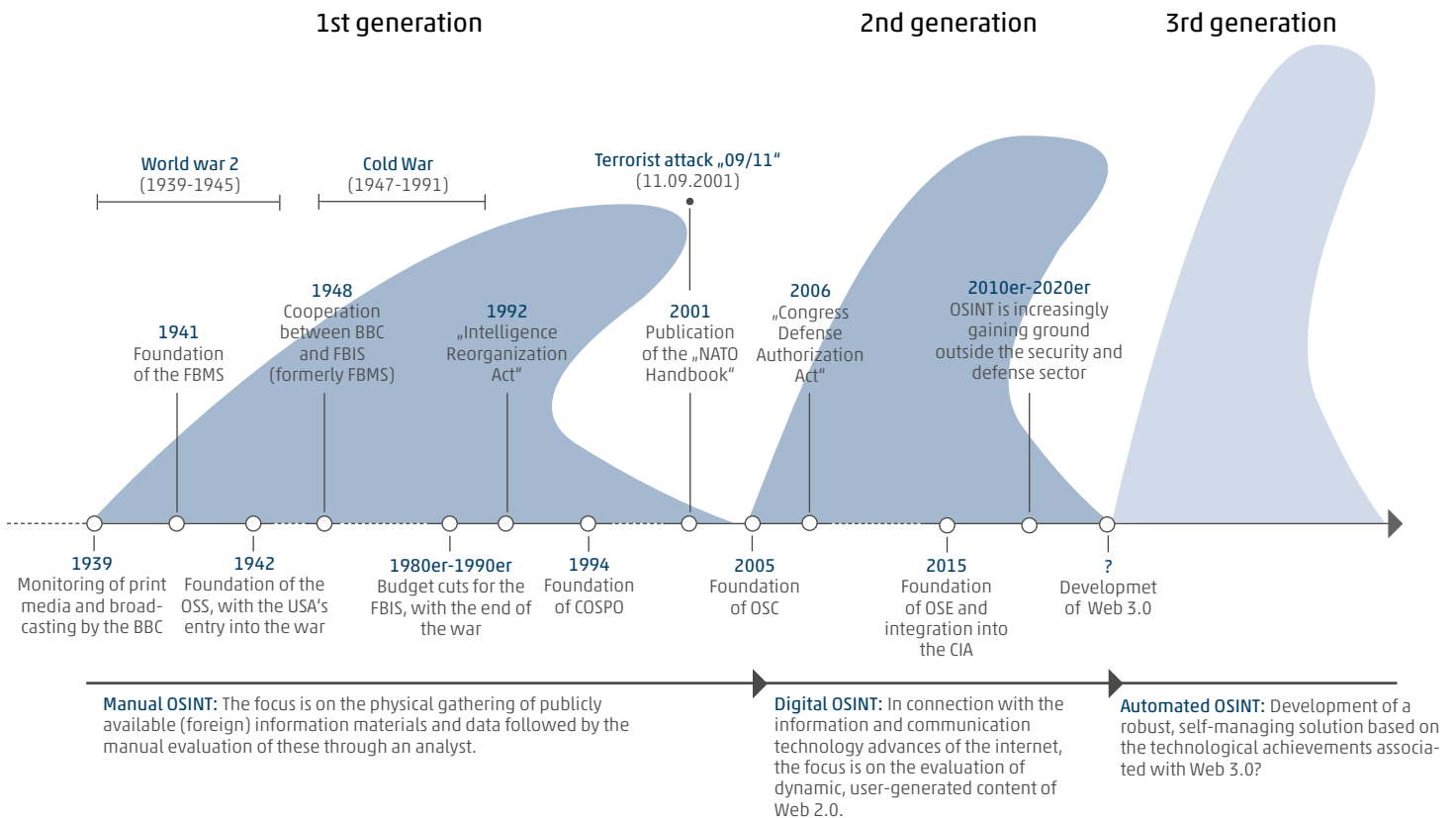


Fig.1: OSINT generations as well as influences and events over time/ Source: Own illustration, design based on Williams and Blum [17]

of avoiding duplication of work [10]. In the years that followed, OSINT spread to other countries on both sides of the Iron Curtain. The "East German Ministry for State Security" (MfS), for example, analyzed around 1,000 Western magazines and 100 books every month and summarized more than 100 newspapers and 12 hours of West German radio and television broadcasts every day [10].

Despite the successes achieved by the FBIS, such as the first indications of a withdrawal of Soviet missiles from Cuba [11,17], the end of the Cold War was followed by drastic budget cuts for the institution. The first-generation OSINT movement gradually came to a standstill [17]. The bias of the intelligence services towards the information content of public sources, combined with the mistake from earlier times of valuing only secrets as intelligence [29], prevailed [19,23,10,18,17].

Things started to change again with the increasing volume of information in the 1990s. The invention of the internet finally led to a fundamental information revolution [16,22,30,10], which resulted in a shift towards the modern information society. Information took on new technological, social and economic roles that had an enormous influence on every aspect of daily life [10]. This was accompanied by an increasing flood of information and ever more efficient technologies in the fields of computer science, data science and statistics. As a result, the collection and analysis of data and information became much simpler [19,16,22]. Traditional intelligence principles were thus fundamentally revised in a single stroke. With the introduction of modern information systems, a large part of the sources and techniques that were previously only available to secret services were now progressively accessible to the general public [23]. This finally led the "United States Intelligence Community" (IC) to the realization that a fundamental structural reform was necessary in order to continue to meet the increasingly dynamic information requirements and channels [19,30,17]. The term OSINT found its way into the literature [3]. The term was initially coined by US military intelligence, which officially listed public sources as the basis for information procurement for the first time in 1992 as part of the "Intelligence Reorganization Act" [31,30]. Following this, the "Community Open Source

Program Office" (COSPO) was established in 1994 with the aim of controlling the use of public information by the IC. However, keeping pace with the rapid increase in available information and the growing importance of OSINT was not possible, as the attacks of September 11, 2001 revealed [29]. "09/11" proved to be a turning point for the development of OSINT [11]. In the same year, the "North Atlantic Treaty Organization" (NATO) [22] published a handbook on OSINT in an attempt to introduce a uniform framework. In doing so, NATO released one of the first and still frequently referenced definitions [cf. 1]:

"Open Source Intelligence (OSINT) is information that has been deliberately discovered, discriminated, distilled, and disseminated to a select audience, generally the commander and their immediate staff, in order to address a specific question. OSINT, in other words, applies the proven process of intelligence to the broad diversity of open sources of information, and creates intelligence." [22]

In this process, NATO [22] also subdivided OSINT for the first time into the other consecutive components OSD and OSIF (see Fig. 2).

3.2 Second Generation Open Source Intelligence (OSINT)

On the advice of the 9/11 Commission, the "Open Source Center" (OSC) was established in 2005, incorporating the FBIS [31,10,30]. The establishment of the OSC as the leading OSINT institution of the US government marks the beginning of the "second generation" of OSINT. Driven by the further development of the internet into Web 2.0 and the associated advances in information and communication technology, the term "Digital OSINT" is also used in this context [16,18,17]. The associated dynamic websites and the emergence of decentralized user-generated content, e.g. through the development of social networks or the "Internet of Things" (IoT), have turned OSINT into an increasingly complex discipline [32,20,33,17]. In 2006, the "Defense Strategy for Open-Source Intelligence" was subsequently adopted to further expand OSINT under the US Department of Defense [11,29]. In addition, a new working definition

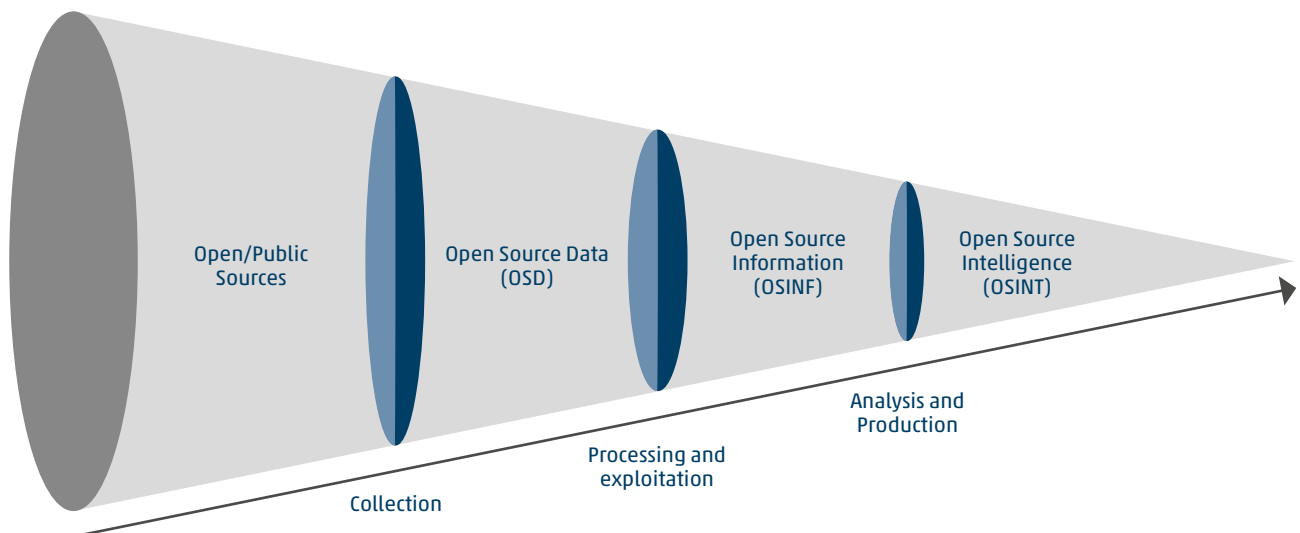


Fig.2: Open Source Intelligence Funnel
 Source: Own Illustration, design based on JCS [38]

for OSINT was passed as part of the “Congress Defense Authorization Act”:

“Open-source intelligence (OSINT) is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.” [30]

In 2011, this definition was adopted by the Office of the Director of National Intelligence (DNI) and expanded by the last sentence “OSINT draws from a wide variety of information and sources” [34]. With this, he underlined the growing flood of information, often referred to as “big data” [33,3,14]. The increasing flood of data also led to approaches to further subdivide the definition of OSINT based on the sources predominantly involved in a research process. In this manner, information derived from social media, for example, is also referred to by the acronym “Social Media Intelligence” (SOCMINT) [35–37]. A definition that is very similar to the previous one was also adopted by the Joint Chiefs of Staff of the U.S. Army (JCS):

Derived from the systematic collection, processing, and analysis of publicly available information in response to known or anticipated intelligence requirements. Also called OSINT.” [38]

Similar definitions can also be found in Germany. The online glossary of the „German Domestic Intelligence Services”, for example, states:

„Open Source Intelligence (OSINT) bezeichnet die Informationsgewinnung aus offenen Quellen. OSINT-Maßnahmen sind das Monitoring von Internetseiten, aber auch die gezielte Recherche nach sämtlichen öffentlich zugänglichen Informationen zu einer Zielperson. [...]”[39]

In translation, this can be understood as follows: “Open Source Intelligence (OSINT) refers to the gathering of information from open sources. OSINT methods include the monitoring of websites, but also targeted research for all publicly available information on a target person.”

3.3 Third Generation Open Source Intelligence (OSINT)

The definition of second-generation OSINT is thus slowly becoming established in the literature and appears to be asserting itself as a recognized intelligence gathering discipline. In 2015, for example, the OSC was renamed the “Open Source Enterprise” (OSE) and incorporated directly into the CIA under the new Directorate for Digital Innovation [40]. The internet, on the other hand, is already undergoing a new transformation

towards Web 3.0, which could herald a new generation of OSINT based on its history [17]. Web 3.0 is to be understood as a "semantic" web, which encompasses the direct and indirect machine processing of data through to artificial intelligence. Developing OSINT into a robust, self-managing solution and fully automating the process from data collection to analysis is thus moving to the foreground [9,13]. However, it is no longer seen as a purely governmental matter. Private research institutions and organizations outside the security and defense sector [41,29] are also massively driving the development of such systems, e.g. for competitive analysis or marketing activities [32,19,16]. In the current literature, it is therefore possible to find definitions that are not specifically tailored to security authorities. Dokman and Ivanjko [19] refer in their definition, for instance, as recipients to target groups and beneficiaries in general:

"Open Source Intelligence (OSINT) is an intelligence product which has been processed, analysed and obtained from the publicly available information. It should be actionable and disseminated in a timely manner to the appropriate audience. Open source intelligence transfers specific knowledge to beneficiaries for them to use it in their actions and the decision-making process."

4 Open Source Data (OSD)

The starting point for all OSINT activities is data. Data forms the basis of the analysis and the conclusions derived from it [36]. An inevitable rule applies in this regard, namely that a decision support system can only ever be as good as the data set used [42]. In this context, OSD refers to unprocessed [1], general raw data that is openly available [11] and can be accessed legally and in an ethical manner [10,22]. In practice, sources whose access requires additional effort [41] or must be acquired commercially [17,22,38] are not excluded. At the same time, however, the addition "legally and ethically acceptable" implies that not all publicly accessible data should automatically be treated as OSD [31,10].

A major difficulty in determining which data and sources are to be summarized under OSD in detail lies in the ongoing technological developments. Improved data

storage and transmission technologies, such as 5G data networks and cloud technologies, as well as search engines [28] make it possible to produce, research, store and exchange historically unprecedented amounts of data [18]. They also give rise to the rapidly changing nature of sources. As a result, the terminology used in existing attempts at classification and subdivision is often too narrow [17]. A clear classification has therefore not yet been conclusively clarified [17]. Just as unclear as the detailed classification of sources and data are the directly associated legal and ethical issues [43,16,18]. The borderline between public and classified sources is thus extremely blurred [23]. In addition, the accessibility and evaluation of the data as well as the use of the information obtained have not yet been clearly defined by law [43,13].

5 Open Source Information (OSINF)

OSD is of little use on its own and only becomes relevant to intelligence when combined [17]. The veritable explosion of data in recent years has made this task a real challenge in terms of "junk" content, misleading information and false information it may contain [18,19]. Before intelligence can be extracted, the data must therefore first undergo a preparation process that includes a certain amount of filtering, validation and summarization [1,22]. The result of this data organization [10] is referred to as OSINF [22], also known under the abbreviation OSIF [22]. It forms the basis for the subsequent knowledge generation [1,10]. In its handbook, NATO adopted the following definition [22]:

"OSIF is comprised of data that can be put together, generally by an editorial process that provides some filtering and validation as well as presentation management. OSIF is generic information that is usually widely disseminated. Newspapers, books, broadcast, and general daily reports are part of the OSIF world."

OSINF must therefore be clearly distinguished from OSD [1,19,38], although the use of the terms in the literature is not entirely clear-cut [22,34,38]. In addition, the definition of OSINF raises the legal question of whether publicly obtained information should also be considered as classified information from a certain point onwards [23,38,18].

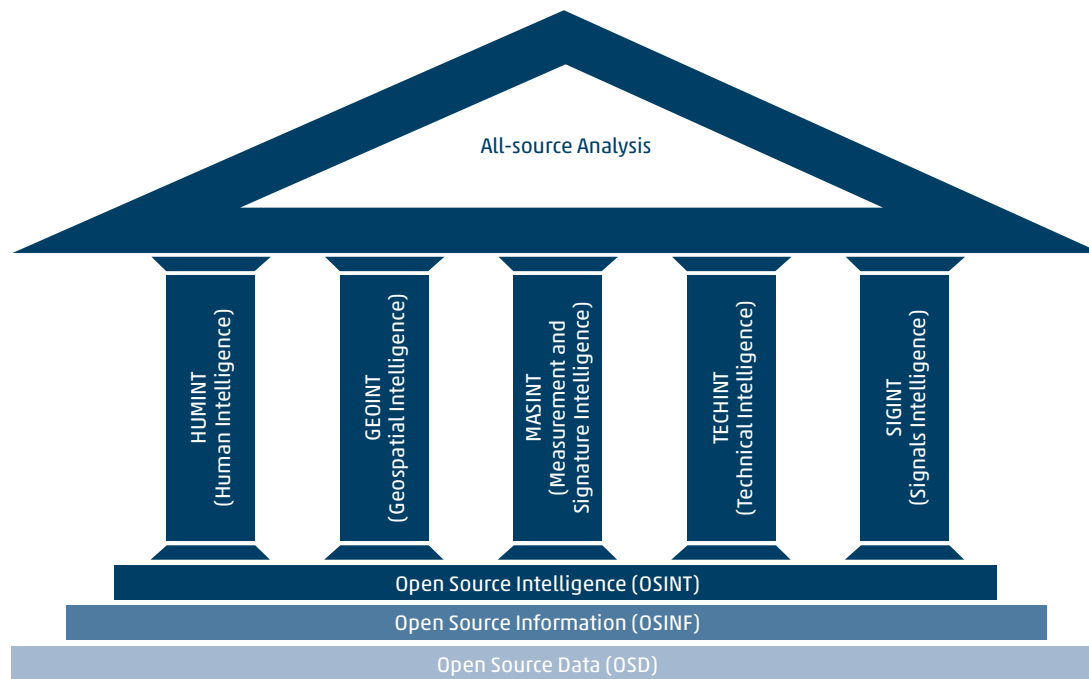


Fig.3: All-source Analysis-temple
Source: Own illustration, design based on NATO [22]

6 Intelligence and Intelligence Gathering Disciplines

The information obtained from the public data [10] is still of limited informative value in itself. It relates to the past and can at best portray the present [44]. Only through targeted analysis substantiated findings about the future can be derived from it [45,46], which then serves as a basis for decision-making [47,48]. The action-relevant knowledge extracted in this respect [19,34,49] is referred to as intelligence [48,1]. Intelligence therefore always consists of information, but not all information represents intelligence [50].

In addition to OSINT, the relevant literature distinguishes between five other disciplines that are concerned with generating intelligence from raw data [34]. These are also commonly referred to as intelligence gathering disciplines [19,38]. The first of these is "Human Intelligence" (HUMINT). HUMINT describes the acquisition of information by humans from human sources in verbal or non-verbal form [18,38]. The second discipline to be listed is "Geospatial Intelligence" (GEOINT). GEOINT refers to the static or time-based analysis of image materials and geodata [18,38]. The third discipline corresponds to "Measurement and Signature Intelligence" (MASINT). MASINT refers to

the quantitative and qualitative analysis of physical properties of target objects and events/phenomena [38,34]. The fourth discipline is "Signals Intelligence" (SIGINT). This refers to knowledge gained from the evaluation of (foreign) communication systems and non-communication-related transmitters [51,38]. The fifth discipline refers to "Technical Intelligence" (TECHINT). TECHINT is understood as the analysis of foreign material/equipment, such as weapon systems, and (related) scientific information and research findings, e.g. engineering techniques [38,31].

The disciplines are thus primarily differentiated according to the specific data sources on which they are based [23,3]. However, in addition to the intelligence agencies, many of these have also become accessible to the public in the course of technological progress [52,16,3,23]. The resulting increasing overlap with OSINT, which is defined only in terms of source accessibility, has provoked numerous controversies. Two concise basic sentiments can be identified in the literature in this regard. The first considers OSINT to be an incoherent concept that stands above and against the clearly classifiable "traditional" intelligence gathering disciplines [3]. The publicly available sources should therefore be subordinated to their traditional domains [53,3]. The second view, attributable to NATO

as well as the US intelligence services and the military, regards OSINT as a necessary complement to the other disciplines [30,23,22]. OSINT is therefore not to be considered as a substitute, as it essentially complements the other disciplines providing a basis and first anchor point [52,31,22]. It thus provides the necessary context in a cost-efficient manner [50,22] and closes (initial) knowledge gaps in order to use the “more aggressive” [18] classified gathering disciplines more effectively [30,22]. This refers to a so-called “All-source Analysis” approach [38]. According to this approach, a more qualitative intelligence product can be generated through the interaction and mutual verification [41,38] of several intelligence gathering disciplines [34,22,38]. In this context, NATO [22] presents OSINT as the foundation on which the classified intelligence disciplines rest, similar to the supporting pillars of a temple (see Fig. 3).

7 Phases of OSINT according to the Intelligence Cycle

The generation process of an intelligence product in the form of temporally and content-relevant findings for decision-making [38] is also synonymously referred to as the Intelligence Cycle [21,54]. It represents the central

element of every intelligence discipline, regardless of the underlying sources or their accessibility [46,19]. The depiction of the process as a dynamic, continuous cycle [34] originates from the CIA’s “Factbook” published in 1987 [54]. The latter defines the process to date [55] as consisting of five successive phases: planning and direction, collection, processing, production and analysis, and dissemination [54]. The inevitable link between the individual phases is that the result of the preceding phase serves as input for the subsequent phase [38,56]. In addition, the product of one cycle in turn serves as a starting point for refinement in the next [19,36]. Even within the cycle, the individual phases are not linear, but continuously iterated based on the fulfillment of previous requirements and new demands [37]. Accordingly, the JCS supplemented the Intelligence Cycle in 2013 with an evaluation and feedback process that is subject to all phases [38] (see Fig. 4). Nowadays, numerous other variations can be found in the literature [46,41]. The representation ranges from one-dimensional linear forms (cf. e.g.: 50,57) to complex network approaches (cf. e.g.: 58,59). The Intelligence Cycle should therefore be seen less as a guideline and more as an informal coordination element that follows a sometimes very intuitive [48] interpretation [12]. Consequently, it should be noted

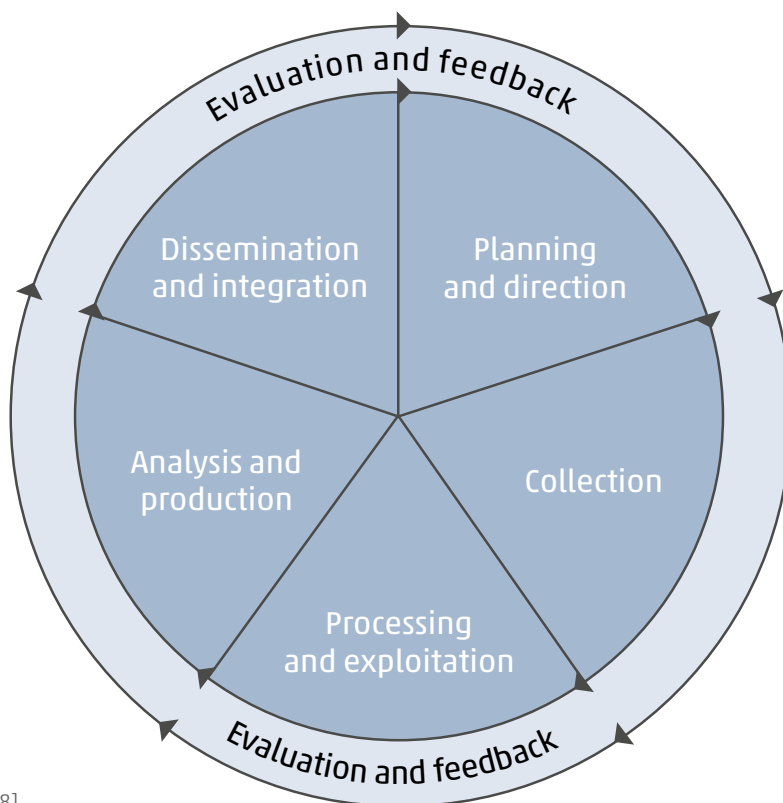


Fig.4: Intelligence Cycle
Source: Based on the JCS [38]

that there is not just one “right” Intelligence Cycle [46] and therefore not just one certified way to generate intelligence [48]

The **planning and direction** phase lays the foundation for the Intelligence Cycle [34]. It combines the identification, definition, and prioritization of the requirements for the cycle or the intelligence product. It is also responsible for developing the activities required to achieve these requirements [31]. The phase is therefore responsible for controlling the entire process [54]. The **collection** phase refers to the collection of raw data [54]. However, the extent to which data should be collected cannot be clearly answered and depends not only on the available resources and budgets, as not every bit has the same information content [50]. The core of this phase therefore consists of the iterative repetition of searches [22] in order to make the research more precise with each run [13]. The raw data collected is usually still of an invalidated, unstructured nature and often contains duplicates [46]. The **processing and exploitation** phase is therefore concerned with condensing these data volumes into valuable and action-relevant information for further processing [34,13,38]. **Analysis and production** refers to the synthesis of the information obtained into a user-oriented, timely and accurate intelligence product


[31,34,12]. The underlying analysis process itself can differ significantly depending on the nature of the information or data type as well as the requirements and may demand a mix of methods [51,45,17]. The final phase, **dissemination and integration**, consists of handing over the finished product to the customer in a usable form [54,17,31]. There are no limits to the design of the product. However, it should be taken into account that the time requirements are met and that the transmission is reduced to the relevant content [31], while at the same time ensuring its completeness [50]. **Evaluation and feedback** should not be viewed as individual phases within the cycle but should take place continuously throughout the entire process. The aim is to achieve progressive optimization [34,22,38]. Systematic communication within and across the individual steps is the most important instrument in this regard [50].

For an in-depth insight into holistic training approaches and methods for operating successfully in this discipline, read our second paper in this series. Publication date: 01.07.2024.


Contacts



Franz Kayser
Author
Project Coordinator Business Development
✉ Franz.Kayser@esg.de



Stefan Vollmer
Vice President Division Cyber and
Information Domain
✉ Stefan.Vollmer@esg.de



Timo Keim
Head of Public Security Academy
✉ Timo.Keim@esg.de



8 References

[1] Dos Passos D. S.: Big Data, Data Science and Their Contributions to The Development of The Use of Open Source Intelligence. S&G, 11 (4) 2017, p. 392-396. doi:10.20985/1980-5160.2016.v11n4.1026.

[2] Smith-Boyle V.: How OSINT Has Shaped the War in Ukraine. Available at: <https://www.americansecurityproject.org/osint-in-ukraine/#:%01:text=Open%2Dsource%20intelligence%2C%20or%20OSINT,synthesized%2C%20and%20analyzed%20into%20intelligence>. Accessed July 24, 2023.

[3] Hatfield J. M.: There Is No Such Thing as Open Source Intelligence. International Journal of Intelligence and Counterintelligence 2023, p. 1-22. doi:10.1080/08850607.2023.2172367.

[4] Bellingcat: Bellingcat auf Deutsch. Available at: <https://de.bellingcat.com/>. Accessed July 26, 2023.

[5] Wiegand R.: Investigative Recherche: Wie das Ressort bei der SZ entstand. Süddeutsche Zeitung 2022, 6 October 2022. Available at:

<https://www.sueddeutsche.de/kolumne/hans-leyendecker-investigative-recherche-panama-papers-pulitzer-preis-uguren-1.5664676>. Accessed July 24, 2023.

[6] Winiecki D. et al.: Validating Bad Entity Ranking in the Panama Papers via Open-source Intelligence. In: 2020 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM). IEEE, 2020, pp 752-759.

[7] Herrmann B. et al.: Mossack Fonseca: Datenleck offenbart letzte Geheimnisse. Süddeutsche Zeitung 2018, 20 June 2018. Available at: <https://www.sueddeutsche.de/politik/mossack-fonseca-neues-datenleck-offenbart-die-letzten-geheimnisse-der-skandal-kanzlei-1.4025000>. Accessed July 24, 2023.

- [8] Obermayer B. et al.: Die Panama Papers - das bisher größte Datenleak. Available at: <https://panamapapers.sueddeutsche.de/articles/56ff9a28a1bb8d3c3495ae13/>. Accessed July 24, 2023.
- [9] Pastor-Galindo J. et al.: OSINT is the next Internet goldmine: Spain as an unexplored territory. Caceres, Spanien, 2019.
- [10] Schaurer F., Störger J.: The Evolution of Open Source Intelligence. Zürich: ETH Zurich, 2010.
- [11] Burke C.: Freeing knowledge, telling secrets: Open source intelligence and development. Research paper series: Centre for East-West Cultural & Economic Studies, (13) 2007.
- [12] Hwang Y.-W. et al.: Current Status and Security Trend of OSINT. Wireless Communications and Mobile Computing, 2022 2022, p. 1-14. doi:10.1155/2022/1290129.
- [13] Pastor-Galindo J. et al.: The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. IEEE Access, 8 2020, p. 10282-10304. doi:10.1109/ACCESS.2020.2965257.
- [14] Yogish P. U., Krishna P. K.: Open Source Intelligence and its Applications in Next Generation Cyber Security - A Literature Review 2021. doi:10.5281/zenodo.5171580.
- [15] Ish D. et al.: Evaluating the Effectiveness of Artificial Intelligence Systems in Intelligence Analysis. Santa Monica, Calif.: RAND Corporation, 2022.
- [16] Ghioni R. et al.: Open source intelligence and AI: a systematic review of the GELSI literature. AI & society 2023, p. 1-16. doi:10.1007/s00146-023-01628-x.
- [17] Williams H. J., Blum I.: Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. Santa Monica, Calif.: RAND Corporation, 2018.
- [18] Ünver H. A.: Digital Open Source Intelligence and International Security: A Primer. 2018.
- [19] Dokman T., Ivanjko T.: Open Source Intelligence (OSINT): issues and trends. In: INFUTURE2019: Knowledge in the Digital Age. Faculty of Humanities and Social Sciences, University of Zagreb Department of Information and Communication Sciences, FF press, 2020.
- [20] Benes L.: OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm. JSS, 6 (3Suppl) 2013, p. 22-37. doi:10.5038/1944-0472.6.3S.3.
- [21] Herrera-Cubides J. F. et al.: Open-Source Intelligence Educational Resources: A Visual Perspective Analysis. Applied Sciences, 10 (21) 2020, p. 7617. doi:10.3390/app10217617.
- [22] North Atlantic Treaty Organization: NATO Open Source Intelligence Handbook. 2001.
- [23] North Atlantic Treaty Organization: NATO Open Source Intelligence Reader. 2002.
- [24] Block L.: The long history of OSINT. Journal of Intelligence History 2023, p. 1-15. doi:10.1080/16161262.2023.2224091.
- [25] British Broadcasting Corporation: BBC Monitoring - Essential Media Insight. Available at: <https://monitoring.bbc.co.uk/>. Accessed May 12, 2023.
- [26] Roop J. E.: Foreign Broadcast Information Service: History Part 1: 1941 - 1947. 1969.
- [27] Central Intelligence Agency: The Office of Strategic Services: America's First Intelligence Agency. Available at: <https://www.cia.gov/legacy/museum/exhibit/the-office-of-strategic-services-n-americas-first-intelligence-agency/>. Accessed May 11, 2023.
- [28] Glassman M., Kang M. J.: Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). Computers in Human Behavior, 28 (2) 2012, p. 673-682. doi:10.1016/j.chb.2011.11.014.
- [29] Mercado S. C.: Reexamining the Distinction Between Open Information and Secrets. Studies in Intelligence, 49 (2) 2005.
- [30] US Department of Defense: National Defense Authorization Act for Fiscal Year 2006: PUBLIC LAW 109-163—JAN. 6, 2006. 06.01.2006.
- [31] Department of the Army: Open-Source Intelligence. Washington, DC, 2012.
- [32] Alkilani H., Qusef A.: OSINT Techniques Integration with Risk Assessment ISO/IEC 27001. In: International Conference on Data Science, E-learning and Information Systems 2021 (Editors: J. A. Lara Torralbo et al.). New York, NY, USA: ACM, 2021, pp 82-86.
- [33] Chen et al.: Business Intelligence and Analytics: From Big Data to Big Impact. MIS Quarterly, 36 (4) 2012, p. 1165. doi:10.2307/41703503.
- [34] Director of National Intelligence: U.S. National Intelligence: An Overview 2011. USA, 2011.
- [35] Bundesnachrichtendienst: Was uns besonders macht: Nachrichtendienste dürfen, was anderen verboten ist: Spionieren. Available at: https://www.bnd.bund.de/DE/Die_Arbeit/Informationsgewinnung/informationsgewinnung_node.html. Accessed May 15, 2023.

- [36] Gibson H.: Acquisition and Preparation of Data for OSINT Investigations. In: Open Source Intelligence Investigation (Editors: B. Akhgar et al.). Cham: Springer International Publishing, 2016, pp 69–93.
- [37] Omand D. et al.: Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security*, 27 (6) 2012, p. 801–823. doi:10.1080/02684527.2012.716965.
- [38] Joint Chiefs of Staff U.S. Army: *Joint Intelligence*. 2nd ed. USA, 2013.
- [39] Bundesamtes für Verfassungsschutz: Glossar - Open Source Intelligence. Available at: <https://www.verfassungsschutz.de/SharedDocs/glosaareintraege/DE/O/osint.html>. Accessed May 15, 2023.
- [40] Aftergood S.: Open Source Center (OSC) Becomes Open Source Enterprise (OSE). Available at: <https://fas.org/publication/osc-ose/>. Accessed May 16, 2023.
- [41] Böhm I., Lolagar S.: Open source intelligence. *International Cybersecurity Law Review*, 2 (2) 2021, p. 317–337. doi:10.1365/s43439-021-00042-7.
- [42] García Lozano M. et al.: Veracity assessment of online data. *Decision Support Systems*, 129 2020, p. 113132. doi:10.1016/j.dss.2019.113132.
- [43] Wittmer S., Platzer F.: Zulässigkeit von Open Source-Ermittlungen zur Strafverfolgung im Darknet. Bonn: Gesellschaft für Informatik, Bonn, 2022.
- [44] Kahaner L.: *Competitive intelligence: How to gather, analyse, and use information to move your business to the top*. 1st ed. New York, NY: Simon & Schuster, 1997.
- [45] Theobald E.: *Marketing Intelligence: Ein Lehrbuch für die Praxis*. Stuttgart: Kohlhammer Verlag, 2018.
- [46] Reuser A.: The RIS Open Source Intelligence Cycle. *Journal of Mediterranean and Balkan Intelligence*, 10 (2) 2017.
- [47] Ackoff R. L.: From Data to Wisdom. *Journal of applied Systems Analysis*, 16 1989.
- [48] Breakspear A.: A New Definition of Intelligence. *Intelligence and National Security*, 28 (5) 2013, p. 678–693. doi:10.1080/02684527.2012.699285.
- [49] Kent S.: *Strategic intelligence for American world policy*. Princeton, NJ: Princeton University Press, 1966.
- [50] Lowenthal M. M.: *Intelligence: From secrets to policy*. Thousand Oaks, Calif.: SAGE/CQ Press, 2020.
- [51] Day T. et al.: Fusion of OSINT and Non-OSINT Data. In: Open Source Intelligence Investigation (Editors: B. Akhgar et al.). Cham: Springer International Publishing, 2016, pp 133–152.
- [52] Mercado S. C.: *A Venerable Source in a New Era: Sailing the Sea of OSINT in the Information Age*. 2005.
- [53] Lowenthal M. M.: OSINT: The State of the Art, the Artless State. *Studies in Intelligence*, 45 (3) 2001, p. 61–66.
- [54] Central Intelligence Agency: *Factbook on Intelligence*. Washington, DC, 1987.
- [55] Central Intelligence Agency: *The Intelligence Cycle: Briefing*. 2023.
- [56] Pellissier R., Nenzhelele T. E.: Towards a universal competitive intelligence process model. *S. Afr. j. inf. manag.*, 15 (2) 2013. doi:10.4102/sajim.v15i2.567.
- [57] Dishman P. L., Calof J. L.: Competitive intelligence: a multiphase precedent to marketing strategy. *European Journal of Marketing*, 42 (7/8) 2008, p. 766–785. doi:10.1108/03090560810877141.
- [58] Oraee N. et al.: The competitive intelligence diamond model with the approach to standing on the shoulders of giants. *Library & Information Science Research*, 42 (2) 2020, p. 101004. doi:10.1016/j.lisr.2020.101004.
- [59] Phythian M. (ed): *Understanding the intelligence cycle*. London: Routledge, 2013.