# Open Source Intelligence - Development of a Trend Radar utilizing a Systematic Literature Review

Franz Kayser
ESG
franz.kayser@esg.de

Thomas Mayer
ESG
thomas3.mayer@esg.de

Michael Bücker
FH Münster – University of Applied Sciences
michael.buecker@fh-muenster.de

## Abstract

*Open Source Intelligence (OSINT) is currently experiencing an intensive discourse, heightened since the Russian invasion of Ukraine. However, despite numerous attempts at standardized definitions, the intelligence discipline remains ambiguous. This paper introduces a practice-validated OSINT trend radar, categorizing technologies by maturity, intelligence cycle phase, and use case. Serving as a profound knowledge base and tool for identifying research gaps, the radar emerges from a structured design process. Sixty studies underwent categorization and validation through expert interviews, revealing the absence of a comprehensive, automated third-generation OSINT system in Germany. Technological gaps, especially in the planning, direction, dissemination, and integration phases, are evident. Although intelligent support technologies were identified, practical implementation lags behind theory. The human factor therefore remains central to the OSINT process. Future research should thus prioritize developing applications for underserved phases, probing reasons for limited widespread implementation of proven applications, with emphasis on legal, ethical, political, and social parameters.*

## 1. Introduction

OSINT is a currently more debated research field than ever before. Obtaining intelligence from publicly available data [**?**] has become undeniably important since the Russian invasion of Ukraine in 2022. In this context, real-time analysis, especially of social media, has revealed highly relevant insights [**?**, **?**]. However, OSINT itself is not a new technique [**?**, **?**] but one of the oldest intelligence disciplines [**?**]. Despite numerous attempts to define OSINT (e.g. [**?**, **?**, **?**]), the concept of intelligent analysis remains controversial to this day [**?**, **?**, **?**]. This is not the least because every definition of OSINT is subject to advances in computer and data science, which are continuously developing improvements in (intelligent) collection and analysis capabilities [**?**, **?**]. Moreover, this is accompanied by numerous novel communication channels, which have led to a veritable ”information explosion” [**?**, **?**, **?**]. Today’s problem therefore no longer lies in acquiring information, but in processing its sheer volume [**?**]. In addition, technologies originally restricted to defense and intelligence services are now accessible to the general public, primarily via the Internet [**?**, **?**]. The understanding of intelligence thus changed completely [**?**]. At the same time, the increasing speed of development makes it almost impossible to predict the future shape of OSINT and its consequences [**?**].

To date, there has been a lack of decisive, fundamental scientific publications to pervade the opacity of the subject area [**?**] and address its rapid developments [**?**, **?**]. In particular, there is a lack of current studies that reveal the actual technologies behind OSINT in detail and determine their characteristics. The question of whether ”third generation” OSINT systems in the sense of robust, self-managing solutions [**?**, **?**] already exist has therefore not yet been clarified citeGhioni.2023, PastorGalindo.2020,Yogish.2021. Moreover, the majority of studies focus exclusively on analyzing the OSINT trend area ”cyber security” [**?**, **?**, **?**]. The literature thus missed to cover the topic in its entirety. Important application scenarios (”use cases”) of OSINT have therefore remained unconsidered in research to date [**?**, **?**, **?**]. In addition, supplementary qualitative field research is absent, for example in the form of expert interviews, which contrast theory with the corresponding practical implementation. Although OSINT has a major impact on topics such as security and defense, there is a lack of insight into these sectors [**?**, **?**]. This paper is hence dedicated to answer the research question: *How can the current trends in OSINT in the form of the technologies used and their characteristics, in particular the maturity level and the use case, be presented in a trend radar and validated by experts within the security sector?*

The aim thereby is to identify the technologies used in OSINT applications and to present them systematically in a trend radar, according to their characteristics. Through expert interviews, the identified trends will then be validated and compared with the common practical ”reality”. In this way, a well-founded knowledge base will be compiled, and existing research gaps of practical relevance will be identified. This will enable a coordinated exploration of the research field. The structure of this study thereby follows the iterative ”Design Science Research Model” (DSRM) [?], an open research paradigm for the creation of an innovative artifact [?]. Within this framework, the relevant literature on OSINT will first be analyzed and classified using a systematic literature review [?]. Based on this, the OSINT technologies and their characteristics identified will be visualized in the form of a trend radar. The radar will then be validated using systematizing interviews [?] conducted with experts in the security sector. Finally, the interviews will be evaluated using a qualitative content analysis [21].

## 2. Theoretical Background

### 2.1. Open Source Intelligence (OSINT)

Despite numerous attempts to define OSINT, it remains controversial in the literature to this day [?]. This is mainly because OSINT is largely dependent on the developments of advancing computer and data science. Its domain is continuously expanding because of the resulting improved recording and analysis possibilities [?, ?, ?]. In addition, advances in information and communication technology and the associated new means of communication have made OSINT an increasingly complex discipline [?, ?, ?, ?]. One of the earliest and still frequently referenced definitions [?] originates from the handbook published by NATO in 2001. OSINT according to this definition is information that has been deliberately discovered, discriminated, distilled, and disseminated to a select audience, [...], in order to address a specific question. OSINT, [...] also applies the proven process of intelligence to the broad diversity of open sources of information and creates intelligence [23]. However, today the discipline is no longer seen as a purely governmental matter. Private research institutions and organizations outside the security sector [?, ?] are also massively driving the development of such systems, e.g. for competitive analyses or marketing activities [?, ?, ?]. The focus is thereby shifting to developing OSINT into a robust, self-managing solution and fully automating the process from data collection to analysis [4,8,9].

### 2.2. Open Source Data (OSD)

The starting point for all OSINT activities lies in data. Data forms the basis of the analysis and the conclusions derived from it [?]. In this context, OSD refers to non-processed [?], general raw data that is openly available [?] as well as legally and ethically accessible [?, ?]. In practice, sources whose access requires additional effort [?] or must be acquired commercially [?, ?, ?] are not excluded.

### 2.3. Open Source Information (OSIF)

OSD are of little use on their own and only become relevant to intelligence when they are aggregated [?]. Before intelligence can be obtained from them, the data must therefore be subjected to a preparation process that includes a certain amount of filtering, validation and summarization [?, ?]. The result of this organization of the data [?] is referred to as OSINF. It provides the basis for the resulting knowledge creation [?, ?].

### 2.4. Intelligenz and Intelligence Cycle

The core task of OSINT is to generate intelligence [?, ?] from the condensed information in the sense of a well-founded basis for decision-making [?, ?]. The generation process of such an intelligence product is also referred to synonymously as the intelligence cycle [?, ?]. It represents the central element of every intelligence discipline, regardless of the underlying sources or their accessibility [?, ?]. The representation of the process as a cycle [?] goes back to the CIA's ”Factbook” published in 1987 [?]. To this day [?], the CIA defines the process as consisting of five successive phases: Planning and Direction, Collection, Processing, Analysis and Production, and Dissemination [?]. The link between the phases is that the result of the preceding phase serves as input for the subsequent phase [?, ?]. Similarly, the product of one cycle serves as a starting point for refinement in the next [?, ?]. Furthermore, the individual phases within the cycle are not linear, but are continuously iterated due to the fulfillment of previous requirements and new demands [?]. Accordingly, the JCS supplemented the Intelligence Cycle in 2013 with an evaluation and feedback process that is subject to all phases [?] (see Figure 1). However, to improve the representation of external influences or the assignment of responsibilities [?, ?, ?], numerous other modifications can be found in the literature today [?, ?]. The Intelligence Cycle should therefore be seen less as a guideline and more as an informal coordination element, with a partly very intuitive [?] interpretation [?]. Thus, as a proven instrument, the original CIA cycle

continues to provide a good starting point for managers and analysts [**?**, **?**].

The planning and direction phase combines the identification, definition and prioritization of the requirements for the cycle and the intelligence product. It is also responsible for developing the activities required to achieve these [**?**] as well as monitoring their coordinated implementation [**?**, **?**]. The phase is therefore responsible for controlling the entire cycle [**?**]. The survey phase refers to the collection of raw data [**?**]. The core of this phase consists of the iterative repetition of research [**?**] to make the query more precise with each run [**?**]. The processing and utilization phase is concerned with condensing these data volumes into valuable and action-relevant information for further processing [**?**, **?**, **?**, **?**]. Analysis and production refers to the synthesis of the information obtained into a user-oriented, timely and accurate intelligence product [**?**, **?**, **?**]. The final phase consists of handing over the finished product to the "customer" in a usable form [**?**, **?**, **?**]. In doing so, it is important to adhere to the deadlines and reduce the product to the relevant content [**?**], while at the same time ensuring its completeness [**?**]. Evaluation and feedback are not to be regarded as individual phases within the cycle but take place continuously throughout the entire process. The aim is to achieve progressive optimization [**?**, **?**, **?**].

### 2.5. Previous Studies

In the literature, eight previous, publicly accessible literature reviews can be identified on the topic of OSINT. In 2017, Dos Passos [**?**] highlighted the benefits of incorporating OSINT into everyday life in his literature review. In particular, he emphasized how big data and data science can make the decision-making process more useful and effective. Pastor-Galindo et al. then published further studies in 2019 [**?**] and 2020 [**?**]. In these, they described the current state of OSINT with a focus on services and techniques to improve cybersecurity. They also examined the role of OSINT in the public sphere of governments, using Spain as an example. Moreover, they are credited with the first and only approach to a rudimentary inventory of trends in OSINT. Their findings show that OSINT is used in the three spheres of social opinion and sentiment analysis, cybercrime and organized crime, as well as cybersecurity and cyber defense. Two further literature reviews were published in 2020. In their research, García Lozano et al. [**?**] identified methods and techniques for computer-assisted veracity assessment of public information. Herrera-Cubides et al. [**?**] investigated how the production of research and educational materials in the field of OSINT has developed. They concluded that the number of publications is lower compared to other trending topics. Finally, in 2021, Yogish and Krishna [**?**] explored the state of implementation and use of AI (Artificial Intelligence) technologies in the context of cybersecurity. The result of this study showed that machine learning (ML), pattern recognition and natural language processing (NLP) can and will simplify OSINT in view of increasing data volumes and are already being used in isolated cases. In the following year, Hwang et al. [**?**] conducted a further literature review on security trends and investigated security threats and cybercriminality in the context of OSINT misuse. Based on this, they proposed preventive security measures. In a literature review published in 2023, Ghioni et al. [**?**] then examined the political, ethical, legal and social implications of OSINT in combination with AI. They came to the conclusion that there is still no framework for discussing these. They also found that third-generation OSINT is still in its early stages and that human components cannot yet be replaced.

## 3. Research Methodology

The structure of the study is based on the iterative "Design Science Research Model" (DSRM), developed by Peffers et al [**?**]. It is a theory-based research paradigm for generating an applicable solution, in the form of an innovative artifact [23], solving a (practical) problem [22][45]. The procedure according to this model is therefore ideally suited to create the trend radar. It consists of six successive activities (see Fig. X) [22]. Moreover, the first three evaluation steps according to Sonnenberg and vom Brocke [46] were applied in order to continuously evaluate the design process.

### 3.1. Problem Identification and Motivation

According to the DSMR, the first step consists in defining the specific research problem and explaining the benefits of the solution. This activity can be found in the intorduction chapter.

### 3.2. Design Objectives of the Solution

The next step entails defining the design objectives of the solution. The objectives can be divided into two content-related objectives (CO) and two formal objectives (FO).CO1 requires the trend radar to follow a procedural structure that reflects the process of generating knowledge from public information. This will allow a structured mapping of the identified technologies according to their use. In doing so, any

research gaps that become apparent can be directly assigned to the respective phase. It will thus be possible to verify if a robust, autonomous OSINT system exists. As CO2, it was defined that the key characteristics, in particular the maturity level of the technologies and their use cases, must be taken into account. The maturity level of the technologies makes it possible to determine the respective state of research. Through the use cases the research directions can be revealed. As FO1, it was determined that the trend radar must follow a simple structure in order to provide an easy-to-understand knowledge base for the immediate identification of research gaps. In addition, the radar should have a high degree of standardization to be transferable to other intelligence (gathering) disciplines in later studies. As FO2, it was set out to design the trend radar in an adaptable and continuously expandable way allowing it to capture the high field dynamics.

### 3.3. Evaluation of the Problem Statement and Design Objectives

In the theoretical background section, the main definitions and, in particular, the intelligence cycle, which serves as a basis for the development of the trend radar (”suitability”), were presented. In addition, the presentation of previous research work showed that there is still a lack of comprehensive studies examining OSINT. Both the relevance of the research question raised and the suitability of the adopted design objectives are thus underpinned, fulfilling the evaluation criteria according to Sonnenberg and vom Brocke [**?**].

### 3.4. Design and Development

The third activity involves the creation of the artifact. For this purpose, the relevant literature on OSINT was analyzed by means of a systematic literature review, following the guidelines of Cleven et al [47]. To clearly determine the scope of the literature review, Cooper’s taxonomy [48] was used. Subsequently, classification categories were defined to establish concept matrices, based on the model of Webster and Watson [24], for systematically analyzing the researched literature. To achieve a high degree of standardization, general categories were defined for each phase of the intelligence cycle. Thereby, the categories of the collection phase differ from those of the remaining phases, as the data basis is also considered here. The evaluation and feedback phase was not treated separately due to its iterative nature.

The following six categories were defined with regard to the survey phase: ”Use case”, ”Data”, ”Process”, ”Technology”, ”Technology complexity” and ”Maturity level”. First of all, the use cases were used to record the area of application of the technologies. The category data reveals the composition of the data foundation. Therefore, it is further subdivided into the data type to record the formats and the source to show the origin of the data. The third category, the process, is used to determine the degree of automation or autonomization of the technologies. For this purpose, the following four levels were defined: manual, semi-automated, automated, [Duncheon 2002] fully automated/autonomous [Billing 1997, Endsley and Kaber 1999]. To improve categorization, the ten levels of automation [Sheridan and Verplank 1978, Parasurama 2000] were additionally used.

The fourth category serves to capture the technologies, according to Bleck’s definition [49], defined as ”the totality of material and immaterial means available for the input, output, conversion, transmission and storage of information”.

The fifth category evaluates the complexity of the technologies examined. For the collection phase, the three subcategories ”Volume”[53], ”Variety” and ”Velocity” were used [50-52]. Variety is further subdivided according to the data structure (structured [54], semi-structured and unstructured [55,56]) [53]. Velocity, is further subdivided into the levels ”Batch” [58], ”Near Real-Time” [59,60] and ”Real-Time” [59].

The sixth category reflects the maturity level of the technologies used. For this purpose, the three macro-maturity phases of the German Federal Trend Radar are used: the innovation phase, the prototype phase and the market establishment phase [61].

For the remaining phases of the intelligence cycle, the categories use case, process, technology, technology complexity and maturity level were likewise defined. However, the complexity within the remaining phases is measured on the basis of the underlying analysis, in ascending order: descriptive analysis, diagnostic analysis, predictive analysis through to prescriptive analysis [63,64].

After defining the classification criteria, the literature research was carried out (see Fig. 15). For this, a search string based on general terms for the highest possible number of hits was determined. The string was then applied to the four databases ”Web of Science”, ”IEEE Xplore”, ”ACM Digital Library” and ”arXiv”. The search results were restricted to publications in German or English. Only studies with full access were considered. As the number of publications increased significantly between 2020 and 2023, the period was reduced to these years to ensure the most up-to-date coverage possible. The studies were downloaded on 05.06.2023 (see Appendix D.B). The SQR3 method

[65] was applied for the systematic analysis and further delimitation. Altogether 60 studies were categorized following this procedure.

For categorization, a dedicated Excel spreadsheet was created for each Intelligence Cycle phase and the OSINT technologies and their characteristics methodically recorded [24,47]. The identified technologies were then grouped according to related technologies in an additional Excel column to enable the clear final illustration in the trend radar (see Repository X). Afterwards, the categorization was reviewed by using a "Python" script (see Appendix A). The script queries the occurrence of predefined keywords in the included papers. If a deviation was found, the study in question was analyzed again (see review matrix X). Finally, the trend radar was created on the basis of the concept matrices.

### 3.5. Evaluation of the Design Specifications

The intelligence cycles as the basis of the trend radar provides a structured overview ("clarity") (Breakspear, 2013, p. 689 f.). This meets the requirement of an intuitively understandable illustration ("under-standability") for ensuring a simple extraction ("simplicity") of technologies and research gaps. Furthermore, the other intelligence disciplines are also derived from the cycle, which enables a later application to these ("applicability"). In addition, by aligning the architecture of the radar with the federal government's trend radar (cf. Stich et al., 2022, p. 11 f.), a proven, robust, user-friendly design ("userfriendliness") with an appropriate level of detail ("level of detail") is used. Moreover, with the concept matrices, a template is used to constantly update the radar in order to reflect the highly dynamic nature of the research topic. Particular attention was paid to the general validity of the categories in order to achieve the highest possible degree of standardization ("commonality"). The categorization was also reviewed using the Python script ("internal consistency"). The decisive evaluation criteria, according to Sonnenberg and vom Brocke (2012, p. 13), are thus fulfilled.

### 3.6. Demonstration

Next, the trend radar was demonstrated in the context of guided, systematizing expert interviews. Especially in less structured and sparsely linked subject areas, the method enables dense data collection [66,25]. Additionally, it is suitable in cases where access to the social field is limited [66,26]. The execution thereby follows the concepts of Bogner et al [25], Meuser and Nagel [67] and Gläser and Laudel [26].

The experts (see Tab. 1) were selected according to the method of theoretical sampling [68,69]. It was specified that only experts in Germany should be interviewed in order to validate the trends in this country. Furthermore, it was determined that at least one expert each from a security authority, the established security industry and a start-up would be selected in order to capture different points of view. Following Meuser and Nagel [70], an expert was considered to be someone with a knowledge advantage in the specific area of interest. A "prestigious" company position is they regarded as a reliable guarantee that the respondents possess research-relevant knowledge [72].

The qualitative data collection that followed was carried out using semi-structured interviews. These are particularly suitable for revealing the underlying relationships of a theory [25]. The questionnaire used is based on the structure of the Intelligence Cycle. At the beginning of the interview, the subjects were introduced to the trend radar. In order to compare this theoretical construct with the practical experience of the participants, higher-level, open questions were asked for each phase. These questions reduce the influence of subjectivity [73]. In order to direct the conversation flow in a targeted manner, the superordinate questions are supplemented by exploratory questions [73]. At the third level, these questions are complemented by specific closed questions for targeted follow-up queries [73]. The interviews were held within a time frame of up to one hour, with a maximum of three main questions for each section [25] (see Respository X). The questionnaire was pilot-tested with a domain expert. The expert interviews were conducted online via platforms with video chat functions.

### 3.7. Evaluation of the First Instance of the Trend Radar

The demonstration of the trend radar confirmed its intuitive comprehensibility ("ease of use"). It was furthermore perceived by the practitioners as a useful tool for providing an overview of OSINT technologies ("effectiveness"). In addition, they confirmed its completeness ("completeness") and internal consistency ("consistency") (cf. expert E1, 14.08.2023; expert E3, 28.07.2023; expert E4, 02.08.2023). The design of the trend radar thus proved to be a suitable instrument for identifying research gaps in theory-practice comparisons and for serving as a guideline to practitioners ("fidelity with real world phenomenon"). The essential evaluation criteria, according to Sonnenberg and vom Brocke (2012, pp. 15-18), are thus demonstrably fulfilled in practice.

### 3.8. Evaluation

The evaluation was carried out using a qualitative data analysis according to Gläser and Laudel [26]. The aim of this is to extract, synthesize and structure the information contained in the interviews on the basis of a predefined search grid. This enables the targeted extraction and summarization of relevant, cross-interview information according to a ”top-down approach” [26,25]. The established category system was applied for this purpose.

First, the recorded interviews were transcribed. Second, the software MAXQDA [75] was used for the subsequent categorization and analysis. The categorization system was therefor established within MAXQDA (see repository X). The categories of the first level correspond to the individual phases of the intelligence cycle. The categories of the second level allow a classification of whether the experts express themselves in support of or in contradiction to the theory. The categories of the third level reflect the identified use cases. As many of the experts' statements were of a general nature, the category ”General statements” was added at this level. The categories of the fourth level reflect the individual technologies classified under them. Altogether, 257 statements from the experts were assigned to corresponding categories by this method. Examples of the coding procedure can be found in (Table 3).

### 3.9. Communication

The research results are communicated in the form of this study. A new iteration, proceeding from this chapter, is therefore not carried out.

## 4. Graphics/Images

All images must be embedded in your document or included with your submission as individual source files. The type of graphics you include will affect the quality and size of your paper on the electronic document disc. In general, the use of vector graphics such as those produced by most presentation and drawing packages can be used without concern and is encouraged.

- Resolution: 600 dpi
- Color Images: Bicubic Downsampling at 300dpi
- Compression for Color Images: JPEG/Medium Quality
- Grayscale Images: Bicubic Downsampling at 300dpi
- Compression for Grayscale Images: JPEG/Medium Quality
- Monochrome Images: Bicubic Downsampling at 600dpi
- Compression for Monochrome Images: CCITT Group 4

If your paper contains many large images they will be down-sampled to reduce their size during the conversion process. However, the automated process used will not always produce the best image, and you are encouraged to perform this yourself on an image by image basis. The use of bitmapped images such as those produced when a photograph is scanned requires significant storage space and must be used with care.

## 5. Main text

Type your main text in 10-point Times, single-spaced. Do not use double-spacing. All paragraphs should be indented 1/4 inch (approximately 0.5 cm). Be sure your text is fully justified—that is, flush left and flush right. Please do not place any additional blank lines between paragraphs.

**Figure and table captions** should be 9-point boldface Helvetica (or a similar sans-serif font). Callouts should be 9-point non-boldface Helvetica. Initially capitalize only the first word of each figure caption and table title. Figures and tables must be numbered separately. For example: “Figure 1. Database contexts”, “Table 1. Input data”. Figure captions are to be centered below the figures. Table titles are to be centered above the tables.

**Figure 1. Sample figure with caption.**

## 6. First-order headings

For example, “1. Introduction”, should be Times 12-point boldface, initially capitalized, flush left, with one 12-point blank line before, and one blank line after. Use a period (“.”) after the heading number, not a colon.

### 6.1. Second-order headings

As in this heading, they should be Times 11-point boldface, initially capitalized, flush left, with one blank line before, and one after.

**6.1.1. Third-order headings.** Third-order headings, as in this paragraph, are discouraged.

However, if you must use them, use 10-point Times, boldface, initially capitalized, flush left, followed by a period and your text on the same line.

## 7. Footnotes

Use footnotes sparingly and place them at the bottom of the column on the page on which they are referenced. Use Times New Roman 8-point type, single-spaced. To help your readers, try to avoid using footnotes altogether and include necessary peripheral observations in the text (within parentheses, if you prefer, as in this sentence). asdöfj

## 8. References

List and number all bibliographical references in 9-point Times, single-spaced, at the end of your paper. When referenced in the text, enclose the citation number in square brackets, for example [**?**, **?**] and [**?**]. Where appropriate, include the name(s) of editors of referenced books.