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, autonomous third-generation OSINT system in Germany. Technological gaps, especially in the planning and direction and 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, the process of gathering intelligence from publicly available data, has gained considerable attention, particularly since the 2022 Russian invasion of Ukraine [1]. Real-time analysis of social media has proven pivotal in revealing valuable insights [2, 3]. Despite numerous attempts to define OSINT [4, 5, 6], controversy persists, influenced by ongoing advancements in computer and data sciences that continuously enhance collection and analysis capabilities [7, 8]. The proliferation of open communication channels has led to an overwhelming ”information explosion” [1, 4, 6], with formerly restricted data sources now publicly accessible [4, 8], fundamentally reshaping intelligence paradigms [9]. Despite this heightened interest, fundamental scientific literature in the field remains limited [10], failing to keep pace with rapid developments [7, 8]. Key questions regarding the existence of autonomous third-generation OSINT systems [11, 5] remain unanswered [7, 5, 6], with a disproportionate focus on cybersecurity within existing studies [4, 11, 6]. Consequently, significant OSINT use cases remain unexplored [12, 9, 7], lacking qualitative field research to bridge theoretical concepts with practical implementation [10, 11]. This study is guided by the overarching research question: *How can the current trends in OSINT, focusing on technologies and their characteristics, maturity levels, and use cases, be presented in a trend radar and validated by experts within the security sector?*

In response to this question, the paper investigates current OSINT trends, adopting the Design Science Research Model (DSRM) [13]. The methodology involves a systematic literature review [14] to analyze and classify relevant OSINT literature. Subsequently, OSINT technologies and their characteristics will be visualized in a trend radar, validated through systematizing interviews with security sector experts [15], and evaluated using qualitative content analysis [16].

2. Theoretical Background

The domain of OSINT is continuously expanding due to the ongoing improvements of collecting and analysis possibilities [7, 8]. In addition, the new means and methods of communication associated with advances in information and communication technology have turned OSINT into a complex discipline [17, 8].

2.1. Open Source Intelligence (OSINT) and its Components

One of the earliest and still frequently referenced definitions [1] was 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, [...] thus applies the proven process of intelligence to the broad diversity of open sources [...] and creates intelligence [18]. However, today the discipline is no longer seen as a purely governmental matter. Private research institutions and organizations [19, 20] are also massively driving the development of such systems [9, 7]. The focus is thereby shifting to developing OSINT into a robust, autonomous solution (referred to as third-generation) [11].

2.2. Intelligence and Intelligence Cycle

The core task of OSINT is to generate intelligence in terms of a profound basis for decision-making [21, 18]. The generation process of such an intelligence product is also referred to as the intelligence cycle [22]. It represents the central element of every intelligence discipline [23]. The link between the phases is that the result of the preceding phase serves as input for the subsequent phase [24]. Furthermore, the individual phases are also continuously iterated due to the fulfillment of previous requirements and new demands[25]. Today, to represent external influences or the assignment of responsibilities [26, 27], numerous variations can be found [23]. The Intelligence Cycle should therefore be seen less as a guideline and more as an informal coordination element[4]. In 2013, the JCS segmented the cycle into 6 phases [24] (see figure 1).

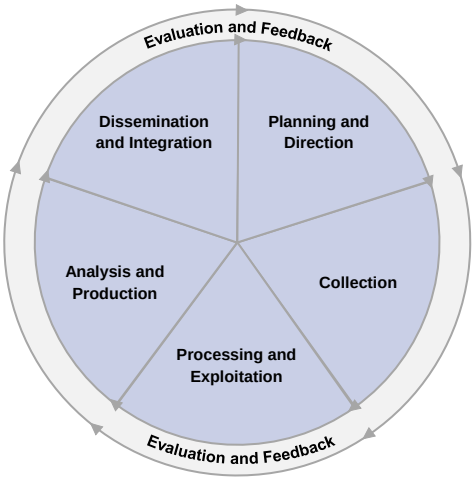

Figure 1. Intelligence Cycle, according to [24]

The planning and direction phase combines the identification, definition, prioritization and monitoring of the requirements for the cycle[24]. The collection phase refers to the gathering of raw data [22]. The core of this phase consists of the iterative repetition of research [18] to make the query more precise with each run [5]. The processing and utilization phase involves condensing these data volumes into action-relevant information [24]. Analysis and production refers to the synthesis of the information obtained into a user-oriented, timely and accurate intelligence product [4, 18]. The final phase consists of handing over the finished product to the ”customer” in a usable form [28, 8]. Evaluation and feedback are not to be regarded as individual phases but take place continuously throughout the entire cycle. The aim is to achieve progressive optimization [24, 18].

2.3. Previous Studies

Eight previous, publicly accessible literature reviews can be identified concerning OSINT. In 2017, Dos Passos [1] showed how big data and data science can make the decision-making process more useful and effective. Pastor-Galindo et al. then described the current state of OSINT in 2019 [11] and 2020 [5] focusing on services and techniques to improve cybersecurity. Moreover, they are responsible for the first and only rudimentary mapping of OSINT trends. They observed that OSINT is used in social opinion and sentiment analysis, cybercrime and organized crime, as well as cybersecurity and cyberdefence. Two further literature reviews were published in 2020. García Lozano et al. [29] identified methods for computer-assisted veracity assessment of public information. Herrera-Cubides et al. [10] investigated how the production of research and educational materials has developed. They concluded that the number of OSINT publications is lower compared to other trending topics. In 2021, Yogish and Krishna [6] explored the state of implementation and use of Artificial Intelligence (AI) technologies in the context of cybersecurity. The result of this study showed that Machine Learning (ML), pattern recognition and Natural Language Processing (NLP) can simplify OSINT given increasing data volumes. In the following year, Hwang et al. [4] investigated security threats and cybercriminality in the context of OSINT misuse. In 2023, Ghioni et al. [7] then examined the political, ethical, legal and social implications of OSINT in conjunction with AI. They discovered that there is still no framework for addressing 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) [13]. It is a theory-based research paradigm for developing an explicitly applicable solution, in the form of an innovative artifact, [30], solving a (practical) problem [13]. The model is therefore ideally suited to create the trend radar. It consists of six successive activities [13]:

1. Problem identification and motivation
2. Objectives of the solution
3. Design and development
4. Demonstration
5. Evaluation
6. Communication

We will discuss steps 2-5 indetail, while the first step (problem identification and motivation) is summarized in section 1 and results of step 6 (communication) are described in sections 4 and 5. Following [31], steps 1-4 were continuously evaluated during the study.

3.1. Design Objectives of the Solution

The design objectives of the solution are divided into content-related objectives (CO) and formal objectives (FO).

Content-related objectives (CO)

CO1 The trend radar must follow a procedural structure that reflects the process of generating intelligence. 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 third-generation OSINT system exists.

CO2 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 research status. Through the use cases, the research directions can be revealed.

Formal objectives (FO)

FO1 The trend radar must follow a simple structure to enable 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.

FO2 The trend radar should be continuously expandable to capture the high field dynamics.

3.2. Evaluation of the Problem Statement and Design Objectives

In Section 2, we define key concepts foundational to our research, focusing particularly on the intelligence cycle. This cycle is crucial as it forms the theoretical basis for the development of our trend radar tool, which we assess for its suitability within the OSINT framework. Additionally, our review of prior studies exposes a notable gap in comprehensive research on OSINT, highlighting the importance and relevance of our inquiry.

3.3. Design and Development

In the third activity of the DSRM, the creation of the artifact involves conducting a systematic literature review, as delineated by [32]. Utilizing Cooper's taxonomy [33] for scoping the literature review, we established classification categories to create concept matrices for a structured analysis of the literature [14].

To ensure a standardized approach across the intelligence cycle, general categories were defined corresponding to each phase, with the evaluation and feedback phases integrated due to their iterative nature. For the collection phase, the following six categories were developed:

- **Use case:** Application areas of the technologies.
- **Data:** Composition and types of data foundations, including data format and source.
- **Process:** Degree of automation in the technologies, categorized into manual, semi-automated, automated, and fully automated/autonomous [34, 16, 35].
- **Technology:** Material and immaterial means used for managing information [36].
- **Technology Complexity:** Assessed through subcategories of Volume, Variety, and Velocity [37, 38].
- **Maturity Level:** Based on the phases of innovation, prototype, and market establishment [39].

Similar categories were adapted for other phases of the intelligence cycle, with complexity measured via the analytics spectrum: descriptive, diagnostic, predictive, and prescriptive [40].

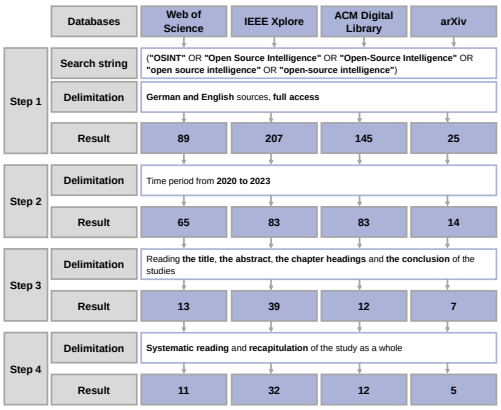

Figure 2. Literature review setup and categorization criteria

The literature search, executed using a broad search string to maximize retrieval, was limited to publications from 2020 to 2023 to reflect recent advancements. A total of 60 studies were analyzed using the SQR3 method [41] and categorized into a meticulously structured Excel spreadsheet for each phase of the intelligence cycle (Fig. 2).

Each technology was then categorized and analyzed for interrelationships within the OSINT framework. Verification of categorization was conducted using a Python script, which scanned the included papers for predefined keywords. The validated categories and relationships informed the development of the trend radar based on the verified concept matrices.

3.4. Evaluation of the Design Specifications

The intelligence cycle underpins the trend radar, providing clarity and an intuitively understandable framework, which simplifies the extraction of technologies and identification of research gaps. The design also supports applicability across various intelligence disciplines. By mirroring the structure of the federal government's trend radar [39], the design achieves robustness, user-friendliness, and an appropriate level of detail, focusing only on essential categories such as use case, technology, and maturity level.

The use of concept matrices facilitates regular updates to the radar, ensuring the design remains current and standardized ("generality"). Internal consistency was rigorously verified to maintain the integrity of categorization. These features collectively meet the critical evaluation criteria set forth in contemporary design research [30].

3.5. Demonstration

Next, the trend radar was demonstrated via guideline-based, systematizing expert interviews [15, 42, 43]. Especially in less structured and sparsely linked subject areas, the method enables dense data collection [15, 43]. Additionally, it is suitable in cases where access to the social field is limited [44, 42].

The experts (table 1) were selected according to the method of theoretical sampling [45]. It was specified that only experts in Germany should be interviewed to validate the trends in this country. It was also determined that at least one expert each from a security authority, the security industry and a start-up would be selected to capture different points of view. A "prestigious" company position is seen as a reliable guarantee that the respondents possess research-relevant knowledge [46].

Table 1. Interviewed experts

Organization	Position	ID
Industry/ Authority	Senior Intelligence Consultant	E1
Industry/ Authority	Referent Corporate Security	E2
Authority	In-House Senior Consultant	E3
Start-up	Co-Founder, Managing Director of a German start-up, for an OSINT platform	E4

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 [15]. The questionnaire used is based on the structure of the Intelligence Cycle. At the beginning of the interview, the trend radar was presented. To compare it with the respondents' practical experience, first, open questions were asked for each phase. These reduce the influence of subjectivity [47]. Exploratory questions were added to direct the flow of conversation [47]. Thirs, specific closed questions for targeted follow-up queries were asked [47]. The interviews lasted up to one hour, with a maximum of three main questions for each phase [15] (see Respository X). The questionnaire was pilot-tested with a domain expert. The interviews were conducted online.

3.6. Evaluation of the First Instance of the Trend Radar

The demonstration of the trend radar confirmed its intuitive comprehensibility ("ease of use"). It was also 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. E1, 14.08.2023; E3, 28.07.2023; E4, 02.08.2023). The trend radar thus proved to be a suitable instrument for identifying research gaps and for serving as a guideline to practitioners (”fidelity with real world phenomenon”). The essential evaluation criteria [31] are thus demonstrably fulfilled.

3.7. Evaluation

The evaluation was carried out using a qualitative data analysis [42]. It extracts, synthesizes and structures the information contained in the interviews using a predefined search grid. This enables the targeted extraction and summarization of relevant, cross-interview information according to a ”top-down approach” [15, 42].

First, the recorded interviews were transcribed. Second, the software MAXQDA was used for the subsequent analysis. The categorization system was therefore established as grid 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 general, the category ”general statements” was added. The categories of the fourth level reflect the individual technologies classified under them. Altogether, 257 statements were categorized in this way. Examples of the coding procedure can be found in table 2.

3.8. 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. Results

The trend radar (figure 3, 4) is read from the outermost to the innermost. Each fifth of the cycle represents an Intelligence Cycle phase. Subdivisions indicate phase-specific use cases, while color gradations show maturity levels. Numbered black and white dots denote grouped technologies, presented in a boxplot-like format reflecting varying maturity levels.

4.1. Intelligence Cycle in Theory-Practice Comparison

Studies could be attributed to each of the Intelligence Cycle phases. However, none of the applications identified covers all phases in the sense of a third-generation OSINT tool. Literature primarily focuses on the collection phase, followed by the analysis and production phase and the processing and exploitation phase. The dissemination and integration phase is covered by far the least after the planning and direction phase.

These findings align with the experts' practical experiences. They regard the Intelligence Cycle as ”state of the art” (cf. E3, 28.12.2023), but note different manifestations of the phases in praxis (cf. E4, 02.08.2023). The planning and direction phase is often neglected, despite its crucial importance, leading to wasteful production (cf. E3, 28.07.2023). Conversely, OSINT is frequently associated solely with the collection phase, resulting in subpar outcomes due to high volumes of low-quality data (cf. E1, 14.07.2023; E2, 19.07.2023; E3, 28.07.2023). The main reason for this is, that the Intelligence Cycle is operated by at least three groups of people. Firstly, the customers, usually located at the ”decision-maker level”, with a primarily legal professional background (cf. E2, 19.07.2023). The second is the technician who carries out the data collection and processing (cf. E2, 19.07.2023; E3, 28.07.2023). Lastly, the analyst evaluates the data and creates the intelligence product (cf. E1, 14.07.2023). The process thereby is rarely transparent between the parties (cf. E1, 14.07.2023; E2, 19.07.2023) and is rarely anchored at the organizational level (cf. E4, 02.08.2023). According to the experts, there is thus no third-generation OSINT tool in use, at least not in German authorities. In addition, the collection focus is driven by concerns about missing vital information, which could later be revealed as publicly available (cf. E1, 14.07.2023).

4.2. Use Cases in Theory-Practice Comparison

Five main use cases emerged from the research: Cyber Security, Health, Security, Journalism, and Competition Analysis. Cyber Security studies primarily focus on Open Source Cyber Threat Intelligence (OSCTI), which involves collecting, monitoring, and analyzing publicly available data to detect potential cyber threats [48, 49]. Health applications mainly pertain to COVID-19, such as investigating the epidemic outbreak [50]. The security use case includes applications such as analyzing violent behavior in

Table 2. Coding examples

Level 1	Level 2	Level 3	Level 4	Transcript example
Collection phase	Theory-supporting	General statement	”web crawler” and/or ”web scraper”	And precisely because there are so many, so simple ways to create web crawlers and web scrapers, [...]”(Cf. E1, 14.07.2023)
Analysis and production phase	Theory-contradictory	Security	AI, ML, DL	”Deep learning, machine learning, artificial intelligence, in some places, I don’t know anyone who has built in a random forest anywhere [...]” (cf. E3, 02.08.2023)

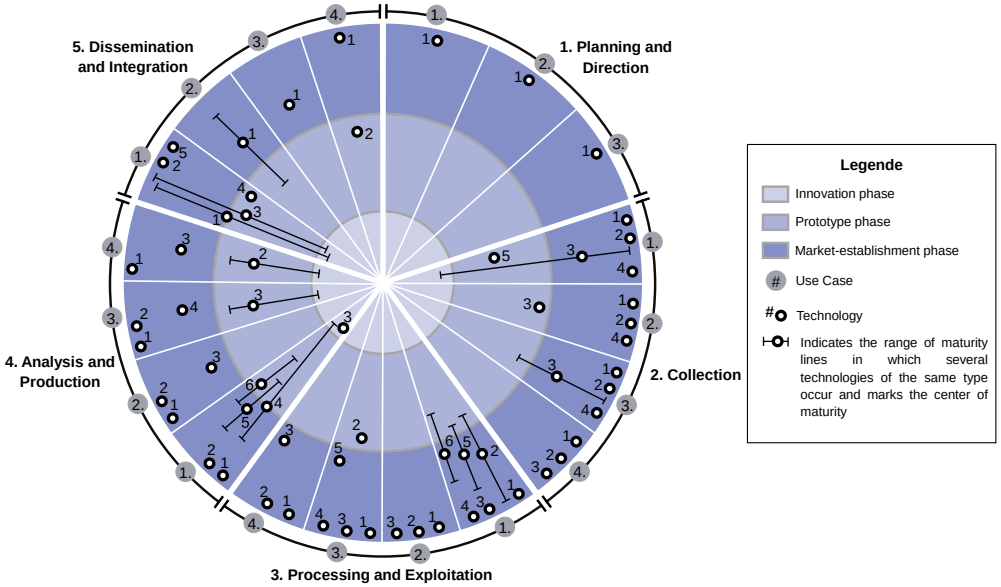

Figure 3. Trend radar

public transport [51]. The identified Journalism study examines the Twitter activities of the OSINT journalists’ association ”Bellingcat” [52]. Competitive analysis involves for example the performance classification of Chinese logistics companies [53]. Additionally, two studies could be identified on general approaches to creating knowledge graphs on OSINF [54, 55].

According to the experts, OSINT is applied in all authorities and has proven itself in numerous use cases, even if not always explicitly labeled as such (cf. E2, 19.07.2023). Most common cases are in cyber security/CTI (cf. E1, 14.07.2023; E2, 19.07.2023), as well as general security, particularly with regard to the German Armed Forces, the (Federal) Intelligence Service, the German domestic intelligence services and the police.

4.3. Technologies and Maturity Levels in Theory-Practice Comparison

Except for the initial phase, automated technologies are utilized across all subsequent phases and use cases. These technologies demonstrate considerable market maturity, yet manual activities remain prevalent. The highest level of automation is observed in the CTI use case.

The most advanced automated technologies in the collection phase are web crawlers and/or web scrapers. Established technologies include ”off the shelf” tools (cf. [56]) and open source solutions like ”Tweepy”, a Python library for Twitter crawlers (e.g., [57]). More advanced prototypes involve combining parallelized, recursive, source-specific web crawlers and scrapers for improved data collection (e.g.,[58]). Another method in the prototype phase is ”focused crawling”, adapting the crawling path dynamically using a content-driven ML algorithm, BERT (”Bidirectional

Encoder Representation from Transformers") (cf. [59]). Technologies for crawling/scraping the dark web, like "Torsion" (cf. [60]), were assigned to the innovation phase. The experts also note the increasing use of open source tools alongside manual work (cf. E1, 14.07.2023; E3, 28.07.2023; E1, 14.07.2023). However, they consider traditional web crawling and scraping outdated due to errors, implementation difficulties, and website resistance. Screenshot-based "web shooting" with subsequent OCR (Optical Character Recognition) extraction is seen as more modern and robust (cf. E3, 28.07.2023).

NLP applications/methods such as "Topic Classifying," "Part-of-Speech Tagging", "Entity and Relation Annotation", and "Named Entity Recognition" demonstrate high automation levels in the processing and utilization phase. Technologies commonly used include the "Python NLTK Toolkit" [61] and the "Stanford CoreNLP Toolkit" [56]. Additionally, deep learning, particularly through "word embedding" using the "word2vec" algorithm, is prominent (e.g., [62]). However, the experts note that this phase within authorities predominantly involves manual work due to the irreplaceable domain knowledge of experts (cf. E1, 14.07.2023; E2, 19.07.2023; E3, 28.07.2023). The degree of automation of technologies thus depends on the abstraction level. Operational tasks, which often require specific individual information, show lower automation levels compared to long-term general strategic analyses requiring extensive data (cf. E3, 28.07.2023).

The highest automation level is observed in the analysis and production phase, where AI, ML, and DL technologies are prevalent. Under DL, vectorization algorithms can also be found. Particularly BERT algorithms in different versions are commonly utilized (e.g., [55]). Furthermore, even under ML vectorization models such as BERT or "Supervised Support Vector Machines" (SVM) (e.g., [63]) are listed. In addition, the algorithms "Random Forest", XGBoost ("eXtreme Gradient Boosting)", lightGBM ("light Gradient Boosting Machine"), "Naive Bayes" and "logistic regressions" are particularly common. Publications thereby often utilize multiple algorithms concurrently for performance comparison (e.g. [53]) or for layered analysis (e.g. [64]). AI technologies are generally less specified, except for [65], who developed a bidirectional recurrent neural network with BiGur ("Bidirectional Gated Recurrent Unit") layers. Due to the modular use of publicly available models, the technologies are mostly classified as market-ready. Despite the potential, practical work in this phase largely relies on manual content analysis due to a lack of technological understanding and acceptance, especially at the contractor/provider level in Germany (cf. E2, 19.07.2023; E3, 28.07.2023; E4, 02.08.2023). Furthermore, ethical and legal barriers, such as GDPR (General Data Protection Regulation), hinder technology adoption (cf. E2, 19.07.2023; E4, 02.08.2023). Additionally, security concerns in German authorities favor standalone systems (cf. E2, 19.07.2023). If smart technologies are used, it is often only inofficially (cf. E4, 02.08.2023). However, there's a need for modular, dynamically expandable systems to keep pace with rapid advancements (cf. E1, 14.07.2023; E3, 28.07.2023; E4, 02.08.2023). Nevertheless, human experience and specialization should not be outweighed, but rather a certain product quality be ensured in a supportive manner. Yet, the revolutionary potential of large language models (LLM) cannot be estimated (cf. E4, 02.08.2023).

In the dissemination and integration phase, tools like "Power BI" [53] are utilized to create dashboards and visualization maps. Furthermore, user interfaces, web applications, and online platforms are developed, including Python GUIs, specific browser applications [66], improved user interfaces and input masks for entire tool stacks [67]. Additionally, Technologies for generating automated alerts, particularly for cyber security risk assessments, are prevalent [48]. Graph-based visualizations are also common, utilizing tools /libraries like "Matplot," "Networkx," "Pygraphistry," or the "Neo4j-Browser" [56]. Except from the alerts, the retrieval of results is largely semi-automated and the technologies are in the market establishment phase. No information on targeted user tests or a new development run involving user feedback could thereby be found in any of the studies. The experts state that there is still very little automation within the authorities during this phase. The final product is often only a PDF document, an email or a verbal report (cf. E1, 14.07.2023), although in many cases no more is required (cf. E3, 28.07.2023). However, outside of the OSINT topic, there are several automated tools, that could be transferred to the authorities in this context (cf. E4 02.08.2023). Moreover, in practice, there is also a lack of necessary feedback for product improvement (cf. E3, 28.07.2023).

5. Discussion and Conclusion

5.1. Contributions and Implications

The investigation into the existence of a robust, automated third-generation OSINT system (e.g., [7]) leads to a negative conclusion, at least for Germany.

Identified applications fall short of fully covering the intelligence cycle, with significant gaps in the planning and direction phase, followed by the dissemination and integration phase. Humans therefore remain the driving (analysis) component. However, the finding by Pastor-Galindo et al. [5] that intelligent OSINT concepts are not yet widespread cannot be confirmed either. Numerous intelligent tools available on the market were identified in the other phases. Nevertheless, practical integration has so far fallen short of the (theoretical) possibilities. Yet this finding likewise does not confirm the thesis of Yogish et al. [6] that automated, AI-driven solutions, largely eliminating the human component, are inevitably required in every area of OSINT. Rather, the key research question should be why proven, available applications whose support is needed have not yet found widespread use, especially in intelligence authorities. In addition, the question of how the first and last Intelligent Cycle phases, alongside the others, can be better supported technically should be investigated.

Addressing these research questions entails resolving numerous underlying research gaps (RGs), directly corresponding to the three key groups involved in the intelligence cycle.

RG1 - Deficiency in Initial Phase Tools: There is a technological gap in tools that cover the initial phase of the intelligence cycle, particularly in frameworks for targeted requirements definition and communication.

RG2 - Lack of Dissemination Mechanisms: There is a dearth of effective dissemination and integration mechanisms tailored for authorities, largely due to insufficient user testing and iterative feedback incorporation. The indispensability of consumer feedback is underscored by established frameworks to enhance product quality and reduce data overload [68, 24, 18, 25, 69].

RG3 - Modular OSINT Systems: The future of OSINT systems hinges on modular concepts, yet only limited research has been conducted in this area [67, 70].

RG4 - Revamping Procurement Procedures: It's crucial to move away from monolithic stand-alone setups in procurement procedures.

RG5 - Ethical and Legal Compliance: Ensuring compliance with ethical and legal principles is vital for product adoption, requiring robust legislative updates and considering both national and international regulations, such as GDPR [71, 72, 7].

RG6 - Technical Understanding among Decision Makers: Addressing challenges necessitates foundational technical understanding at decision-maker levels, fostering openness to technology and cultivating an information-sharing mindset to transcend bureaucratic barriers [18].

RG7 - Use of LLMs in Intelligence: While Large Language Models (LLMs) show promise in intelligence analysis, their application in operational settings is underexplored [73, 74].

RG8 - Technological Tools for Technicians: Technicians often handle significant phases of the intelligence cycle independently, yet there is a notable absence of robust collection tools to match the rapidly evolving media landscape.

RG9 - Coordination between Analysts and Technicians: Coordination gaps between analysts and technicians pose risks of excessive data collection, emphasizing the need for tools that enhance transparency and mitigate collection biases [26].

5.2. Limitations and Future Research

The first limitation relates to the fact that, due to a lack of clarity about the legal and ethical basis [7, 75], it could not be verified whether only public sources [76] were used in the analyzed studies. It was also not verified whether the technologies meet the legal and ethical requirements for the use of the information obtained [5, 75]. The second limitation stems from classification categories not fully aligning with the MECE (Mutually-Exclusive-and-Collectively-Exhaustive) principle [77], particularly evident in the hierarchical dependency of AI, ML, and DL technologies. In addition, the wording of the authors was followed for objective reproduction when identifying the technologies, but the accuracy of the information was not reviewed in detail. Moreover, no fixed limits could be defined for the volume category, as these were not recorded in uniform dimensions in the studies. The third limitation concerns the limited sample size in expert interviews. Due to the extremely difficult-to-access target group, the active user level and the decision-maker level within the authorities were not interviewed. For improved intercoder reliability, independent verification of the coding carried out by at least a second researcher is also recommended [44, 42]. Lastly, the research structure, following the DSRM process, was executed linearly rather than iteratively as recommended [13].

Nevertheless, the study furnishes future researchers with a comprehensive knowledge base on OSINT through a practice-validated trend radar. Initial evaluations reveal two crucial unanswered research questions and identifies nine detailed research gaps, highlighting critical areas for future development and research to enhance the efficiency and effectiveness of intelligence operations. Moreover, the developed trend

radar serves as a guideline for practitioners. The radar is adaptable to the evolving subject area and transferable to other intelligence disciplines.

6. References

References

[1] D. S. Dos Passos, "Big data, data science and their contributions to the development of the use of open source intelligence," *Sistemas & Gestão*, vol. 11, no. 4, pp. 392–396, 2017.

[2] J. M. Hatfield, "There is no such thing as open source intelligence," *International Journal of Intelligence and CounterIntelligence*, pp. 1–22, 2023.

[3] V. Smith-Boyle, "How osint has shaped the war in ukraine," 2023. https://www.americansecurityproject.org/osint-in-ukraine/#:%01:text=Open%2Dsource%20intelligence%2C%20or%20OSINT,synthesized%2C%20and%20analyzed%20into%20intelligence.

[4] Y.-W. Hwang, I.-Y. Lee, H. Kim, H. Lee, and D. Kim, "Current status and security trend of osint," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–14, 2022.

[5] J. Pastor-Galindo, P. Nespoli, F. Gomez Marmol, and G. Martinez Perez, "The not yet exploited goldmine of osint: Opportunities, open challenges and future trends," *IEEE Access*, vol. 8, pp. 10282–10304, 2020.

[6] P. U. Yogish and P. K. Krishna, "Open source intelligence and its applications in next generation cyber security - a literature review," 2021.

[7] R. Ghioni, M. Taddeo, and L. Floridi, "Open source intelligence and ai: a systematic review of the gelsi literature," *AI & society*, pp. 1–16, 2023.

[8] H. J. Williams and I. Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, vol. RR-1964-OSD of *Research reports*. Santa Monica, Calif.: RAND Corporation, 2018.

[9] T. Dokman and T. Ivanjko, "Open source intelligence (osint): issues and trends," in *INFuture2019: Knowledge in the Digital Age*, International Conference The Future of Information Sciences INFuture, Faculty of Humanities and Social Sciences, University of Zagreb Department of Information and Communication Sciences, FF press, 2020.

[10] J. F. Herrera-Cubides, P. A. Gaona-García, and S. Sánchez-Alonso, "Open-source intelligence educational resources: A visual perspective analysis," *Applied Sciences*, vol. 10, no. 21, p. 7617, 2020.

[11] J. Pastor-Galindo, P. Nespoli, F. Gomez Marmol, and G. Martinez Perez, "Osint is the next internet goldmine: Spain as an unexplored territory."

[12] H. AlKilani and A. Qusef, "Osint techniques integration with risk assessment iso/iec 27001," in *International Conference on Data Science, E-learning and Information Systems 2021* (J. A. Lara Torralbo, S. A. Aljawarneh, V. Radhakrishna, and A. N., eds.), (New York, NY, USA), pp. 82–86, ACM, 2021.

[13] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, 2007.

[14] J. Webster, Watson, and T. Richard, "Analyzing the past to prepare for the future: Writing a literature review," *MIS Quarterly*, vol. 26, pp. xiii–xxiii, 2002.

[15] A. Bogner, B. Littig, and W. Menz, *Interviews mit Experten: Eine praxisorientierte Einführung*. Wiesbaden: Springer Fachmedien Wiesbaden, 2014.

[16] C. E. Billings, *Aviation automation: The search for a human-centered approach*. Human factors in transportation, Mahwah, N.J: Lawrence Erlbaum Associates Publishers, 1997.

[17] L. Benes, "Osint, new technologies, education: Expanding opportunities and threats. a new paradigm," *Journal of Strategic Security*, vol. 6, no. 3Suppl, pp. 22–37, 2013.

[18] North Atlantic Treaty Organization, *NATO Open Source Intelligence Handbook*. 2001. https://github.com/lawsecnet/OPSEC/blob/master/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf.

[19] I. Böhm and S. Lolagar, "Open source intelligence," *International Cybersecurity Law Review*, vol. 2, no. 2, pp. 317–337, 2021.

[20] S. C. Mercado, "Reexamining the distinction between open information and secrets," *Studies in Intelligence*, vol. 49, no. 2, 2005.

[21] A. Breakspear, "A new definition of intelligence," *Intelligence and National Security*, vol. 28, no. 5, pp. 678–693, 2013.

[22] Central Intelligence Agency, *Factbook on Intelligence*. 1987. https://www.cia.gov/readingroom/document/cia-rdp90-00530r000701680019-5.

[23] A. Reuser, "The ris open source intelligence cycle," *Journal of Mediterranean and Balkan Intelligence*, vol. 10, no. 2, 2017.

[24] U.S. Joint Force Command, "Joint intelligence," in *Joint Publication 2-0 (JP 2-0)* (Joint Chiefs of Staff U.S. Army, ed.), Joint Publications Intelligence Series. https://irp.fas.org/doddir/dod/jp2_0.pdf.

[25] H. Gibson, "Acquisition and preparation of data for osint investigations," in *Open Source Intelligence Investigation* (B. Akhgar, P. S. Bayerl, and F. Sampson, eds.), Advanced Sciences and Technologies for Security Applications, pp. 69–93, Cham: Springer International Publishing, 2016.

[26] M. M. Lowenthal, *Intelligence: From secrets to policy*. Thousand Oaks, Calif.: SAGE/CQ Press, eighth edition ed., 2020.

[27] M. Phythian, ed., *Understanding the intelligence cycle*. Studies in intelligence, London: Routledge, 2013.

[28] Central Intelligence Agency, *The Intelligence Cycle: Briefing*. 2023.

[29] M. García Lozano, J. Brynielsson, U. Franke, M. Rosell, E. Tjörnhammar, S. Varga, and V. Vlassov, "Veracity assessment of online data," *Decision Support Systems*, vol. 129, p. 113132, 2020.

[30] J. vom Brocke, A. Hevner, and A. Maedche, "Introduction to design science research," in *Design Science Research. Cases* (J. vom Brocke, A. Hevner, and A. Maedche, eds.), Progress in IS, pp. 1–13, Cham: Springer International Publishing, 2020.

[31] C. Sonnenberg and J. vom Brocke, "Evaluations in the science of the artificial – reconsidering the build-evaluate pattern in design science research," in *Design Science Research in Information*, vol. 7286, pp. 381–397, 2012.

[32] A. Cleven, B. Niehaves, R. Plattfaut, K. Riemer, A. Simons, and vom Brocke, Jan, Martin Hilti, "Reconstructing the giant: On the importance of rigour in documenting the literature search process."

[33] H. M. Cooper, "Organizing knowledge syntheses: A taxonomy of literature reviews," *Knowledge in Society*, vol. 1, no. 1, pp. 104–126, 1988.

[34] C. Duncheon, "Product miniaturization requires automation – but with a strategy," *Assembly Automation*, vol. 22, no. 1, pp. 16–20, 2002.

[35] M. R. Endsley and D. B. Kaber, "Level of automation effects on performance, situation awareness and workload in a dynamic control task," *Ergonomics*, vol. 42, no. 3, pp. 462–492, 1999.

[36] S. Bleck, *Entwicklung einer Methodik zur integrierten Planung von Informationstechnologie-Einsatz und intermediären Informationsdienstleistungen im elektronischen Geschäftsverkehr: Zugl.: Aachen, Techn. Hochsch., Diss., 2004*, vol. 72 of *Schriftenreihe Rationalisierung und Humanisierung*. Aachen: Shaker, 2004.

[37] N. Elgendy and A. Elragal, "Big data analytics: A literature review paper," in *Advances in Data Mining*, vol. 8557, pp. 214–227, 2014.

[38] S. Singh and N. Singh, "Big data analytics," in *2012 International Conference on Communication, Information & Computing Technology (ICCICT)*, pp. 1–4, 2012.

[39] V. Stich, M.-F. Stroh, M. Abbas, K. Frings, and S. Kremer, "Digitalisierung der wirtschaft in deutschland: Technologie- und trendradar 2022."

[40] D. Delen and H. Demirkan, "Data, information and analytics as services," *Decision Support Systems*, vol. 55, no. 1, pp. 359–363, 2013.

[41] F. P. Robinson, *Effective study*. New York: Harper & Row, 4th ed. ed., 1970.

[42] J. Gläser and G. Laudel, *Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen*. Lehrbuch, Wiesbaden: VS Verlag für Sozialwissenschaften, 3., überarb. aufl. ed., 2009.

[43] M. Meuser and U. Nagel, "Expertinneninterviews - vielfach erprobt, wenig bedacht: ein beitrag zur qualitativen methodendiskussion," pp. 441–471, 1991.

[44] A. Bogner, B. Littig, and W. Menz, *Das Experteninterview*. Wiesbaden: VS Verlag für Sozialwissenschaften, 2002.

[45] B. G. Glaser and A. L. Strauss, *The discovery of grounded theory: Strategies for qualitative research*. Observations, New York, NY: Aldine, 1967.

[46] A. Bogner and W. Menz, "Das theoriegenerierende experteninterview," in *Das Experteninterview* (A. Bogner, B. Littig, and W. Menz, eds.), pp. 33–70, Wiesbaden: VS Verlag für Sozialwissenschaften, 2002.

[47] M. Saunders, P. Lewis, and A. Thornhill, *Research methods for business students*. Always learning, Harlow and Munich: Pearson, 6. ed. ed., 2012.

[48] K. Ahuja, Khushi, Dipali, and N. Sharma, "Cyber security threats and their connection with twitter," in *2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, pp. 1458–1463, IEEE, 2022.

[49] N. A. Al-Dmour, M. Kamrul Hasan, M. Ajmal, M. Ali, I. Naseer, A. Ali, H. A. Hamadi, and N. Ali, "An automated platform for gathering and managing open-source cyber threat intelligence," in *2023 International Conference on Business Analytics for Technology and Security (ICBATS)*, pp. 1–7, IEEE, 2023.

[50] E. B. Kpozehouen, X. Chen, M. Zhu, and C. R. Macintyre, "Using open-source intelligence to detect early signals of covid-19 in china: Descriptive study," *JMIR public health and surveillance*, vol. 6, no. 3, p. e18939, 2020.

[51] M. Nobili, L. Faramondi, R. Setola, M. Ghelli, B. Persechino, and M. Lombardi, "An osint platform to analyse violence against workers in public trasportation," in *2021 International Conference on Cyber-Physical Social Intelligence (ICCSI)*, pp. 1–6, IEEE, 2021.

[52] D. Bär, F. Calderon, M. Lawlor, S. Lickleder, M. Totzauer, and S. Feuerriegel, "Analyzing social media activities at bellingcat," in *Proceedings of the 15th ACM Web Science Conference 2023*, (New York, NY, USA), pp. 163–173, ACM, 2023.

[53] Z. Tao, P. Charoenkwan, B. Paphawasit, and N. Rujeerapaiboon, "Machine learning-based classification of competitors performance: evidence from chinese logistics companies," in *2023 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON)*, pp. 131–137, IEEE, 2023.

[54] Y. Hu, L. He, X. Tang, G. Luo, S. He, and Q. Fang, "Construction of domain knowledge graph based on open source intelligence," in *2023 IEEE 2nd International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA)*, pp. 1378–1382, IEEE, 2023.

[55] H. Ma, X. Liu, and W. Zhao, "Research on domain-specific knowledge graph based on the roberta-wwm-ext pretraining model," *Computational intelligence and neuroscience*, vol. 2022, p. 8656013, 2022.

[56] S. Middleton, A. Lavorgna, G. Neumann, and D. Whitehead, "Information extraction from the long tail," in *12th ACM Conference on Web Science Companion*, (New York, NY, USA), pp. 82–88, ACM, 2020.

[57] V. Adewopo, B. Gonen, and F. Adewopo, "Exploring open source information for cyber threat intelligence," in *2020 IEEE International Conference on Big Data (Big Data)*, pp. 2232–2241, IEEE, 2020.

[58] D. Jenkins, L. M. Liebrock, and V. Urias, "Designing a modular and distributed web crawler focused on unstructured cybersecurity intelligence," in *2021 International Carnahan Conference on Security Technology (ICCST)*, pp. 1–6, IEEE, 2021.

[59] P. Kuehn, M. Schmidt, M. Bayer, and C. Reuter, "Threatcrawl: A bert-based focused crawler for the cybersecurity domain."

[60] H. S. Sonawane, S. Deshmukh, V. Joy, and D. Hadsul, "Torsion: Web reconnaissance using open source intelligence," in *2022 2nd International Conference on Intelligent Technologies (CONIT)*, pp. 1–4, IEEE, 2022.

[61] J. Hubbard, G. Bendiab, and S. Shiaeles, "Ipass: A novel open-source intelligence password scoring system," in *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*, pp. 90–95, IEEE, 2022.

[62] C. Bai, A. Li, Z. Gao, and X. Cui, "Research on anti-terrorism intelligence mining method based on attention neural networks," in *2020 IEEE 2nd International Conference on Civil Aviation Safety and Information Technology (ICCASIT*, pp. 458–464, IEEE, 2020.

[63] D. Iorga, D. Corlatescu, O. Grigorescu, C. Sandescu, M. Dascalu, and R. Rughinis, "Early detection of vulnerabilities from news websites using machine learning models," in *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pp. 1–6, IEEE, 2020.

[64] J.-Z. Yang, F. Liu, Y.-J. Zhao, L.-L. Liang, and J.-Y. Qi, "Ninsrapm: An ensemble learning based non-intrusive network security risk assessment prediction model," in *2022 7th IEEE International Conference on Data Science in Cyberspace (DSC)*, pp. 17–23, IEEE, 2022.

[65] D. Dale, K. McClanahan, and Q. Li, "Ai-based cyber event osint via twitter data," in *2023 International Conference on Computing, Networking and Communications (ICNC)*, pp. 436–442, IEEE, 2023.

[66] T. Elmas, T. R. Ibanez, A. Hutter, R. Overdorf, and K. Aberer, "Waypop machine: A wayback machine to investigate popularity and root out trolls," in *2022 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, pp. 391–395, IEEE, 2022.

[67] A. V. Arjun, A. K. Buvanasri, R. Meenakshi, S. Karthika, and K. M. Ashok, "Peoplexploit: A hybrid tool to collect public data," in *2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*, pp. 1–6, IEEE, 2020.

[68] Director of National Intelligence, *U.S. National Intelligence: An Overview 2011*. 2011. `https://www.dni.gov/files/documents/IC_Consumers_Guide_2011.pdf`.

[69] T. Day, H. Gibson, and S. Ramwell, "Fusion of osint and non-osint data," in *Open Source Intelligence Investigation* (B. Akhgar, P. S. Bayerl, and F. Sampson, eds.), Advanced Sciences and Technologies for Security Applications, pp. 133–152, Cham: Springer International Publishing, 2016.

[70] T. Wright, S. Whitfield, S. Cahill, and J. Duffy, "Project umbra," in *2020 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, pp. 748–751, IEEE, 2020.

[71] "Document 32016r0679: Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation)," 2016.

[72] "Enforcement and sanctions: What happens if my company processes data in different eu member states?," 18.08.2023.

[73] A. Radford, J. Wu, R. Child, D. Luan, D. Amodel, and I. Sutskever, "Language models are unsupervised multitask learners."

[74] W. X. Zhao, K. Zhou, J. Li, T. Tang, X. Wang, Y. Hou, Y. Min, B. Zhang, J. Zhang, Z. Dong, Du Yifan, C. Yang, Y. Chen, Z. Chen, J. Jiang, R. Ren, Y. Li, X. Tang, Z. Liu, P. Liu, J.-Y. Nie, and J.-R. Wen, "A survey of large language models."

[75] S. Wittmer and F. Platzer, "Zulässigkeit von open source-ermittlungen zur strafverfolgung im darknet."

[76] North Atlantic Treaty Organization, *NATO Open Source Intelligence Reader*. 2002. `https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL%20Oct2002.pdf`.

[77] C.-Y. Lee and B.-S. Chen, "Mutually-exclusive-and-collectively-exhaustive feature selection scheme," *Applied Soft Computing*, vol. 68, pp. 961–971, 2018.

1	**Planning and Direction**	2.3.3	Web crawler and/or web scraper	3.3.4	Statistical methods (e.g. aggregation via mean value, first-difference estimator)	4.3.4	Machine Learning (esp. Random Forest and Naive Bayes algorithms)
1.1	**Cyber Security**	2.3.4	Other open source tools (e.g. Impala shell tool)	3.3.5	Deep learning (text vectorization, e.g. using the word2vec algorithm)	**4.4**	**Journalism, competitive analysis, general approach**
1.1.1	Manual (e.g. manual definition of objectives and requirements)	**2.4**	**Journalism, competitive analysis, general approach**	**3.4**	**Journalism, competitive analysis, general approach**	4.4.1	Manual (expert analysis)
1.2	**Health**	2.4.1	Manually (e.g. via databases)	3.4.1	Manual (manual cleanup, labeling)	4.4.2	Deep learning (especially word embedding, for semantic analysis using different versions of the BERT algorithm)
1.2.1	Manual (e.g. manual requirements definition)	2.4.2	API interface	3.4.2	Standardized methods/algorithms/tools (e.g. parser and other word segmentation tools, for lemmatization, word/character filtering)	4.4.3	Machine learning (in particular Support Vector Machines or Random Forest and XGBoost algorithms)
1.3	**Security**	2.4.3	Web crawler and/or web scraper	3.4.3	Natural language processing filters and labeling methods/tools (e.g. using similarity algorithms and classification algorithms)	4.3.4	Machine Learning (esp. Random Forest and Naive Bayes algorithms)
1.3.1	Manual (e.g. manual hypothesis formulation)	**3**	**Processing and Exploitation**	**4**	**Analysis and Production**	**5**	**Dissemination and Integration**
2	**Collection**	**3.1**	**Cyber Security**	**4.1**	**Cyber Security**	**5.1**	**Cyber Security**
2.1	**Cyber Security**	3.1.1	Manual (e.g. labeling/review/verification/grouping via experts, search parameters in databases/search engines, manual cleansing)	4.1.1	Manual (content analysis)	5.1.1	Files/reports (e.g. CSV file, PDF dossier)
2.1.1	Manually (e.g. via databases and search engines)	3.1.2	Keyword/dictionary/hashtag filter (usually in combination with web crawler and web scraper)	4.1.2	Standardized methods/algorithms and tools (image hashing, open source tools, lexical approaches)	5.1.2	Dashboard/visualization map
2.1.2	API interface	3.1.3	Standardized methods/algorithms/tools (e.g. parser and other word segmentation tools, for normalization, lemmatization, word/character filtering, lowercase conversion and duplicate removal)	4.1.3	Tool stack	5.1.3	Web interface/web application/online platform
2.1.3	Web crawler and/or web scraper	3.1.4	Statistical methods (e.g. oversampling methods, N-gram algorithms, pattern matching)	4.1.4	Deep learning (especially word embedding, for semantic analysis using different versions of the BERT algorithm)	5.1.4	Automated alerts
2.1.4	Other open source tools (e.g. Python tools, data pipelines, stream listeners and lookup features)	3.1.5	Natural Language Processing filters and labeling methods/tools (e.g. heuristic methods, topic classification, part-of-speech tagging, entity and relation annotation, named entity recognition, e.g. using the CoreNLP toolkit or Python NLTK toolkit)	4.1.5	Machine learning (in particular Support Vector Machines or Random Forest, XGBoost, lightGBM, Naive Bayes and logistic regression algorithm)	5.1.5	Graph creation (e.g. using Matplotlib, Networkx, Pygraphistry or the Neo4j browser)
2.1.5	Web application (e.g. for the parallelization of searches in IoT search engines)	3.1.6	Deep learning (text vectorization, e.g. using the word2vec algorithm)	4.1.6	Artificial intelligence (e.g. neural network using BiGRU layers)	**5.2**	**Health**
2.2	**Health**	**3.2**	**Health**	**4.2**	**Health**	5.2.3	Web interface/web application/online platform
2.2.1	Manual (e.g. via databases, search engines and surveys)	3.2.1	Manual (e.g. selection by experts, expert interviews, search parameters in databases/search engines, manual cleansing)	4.2.1	Manual (content analysis)	**5.3**	**Security**
2.2.2	API interface	3.2.2	Keyword/dictionary/hashtag filter (usually in combination with web crawler and web scraper)	4.2.2	Statistical methods (meta-analysis)	5.3.1	Dashboard/visualization map
2.2.3	Web crawler and web scraper	3.2.3	Standardized methods/algorithms/tools (e.g. parsers and other word segmentation tools, for word and character filtering and file conversion tools)	4.2.3	Machine learning (in particular Support Vector Machines or XGBoost and Naive Bayes algorithms as well as Open Source tools)	**5.4**	**Competitive analysis, general approach**
2.2.4	Other open source tools (e.g. social media analysis tool and command line tool)	**3.3**	**Security**	**4.3**	**Security**	5.4.1	Dashboard/visualization map (e.g. using Power BI)
2.3	**Security**	3.3.1	Manual (e.g. verification via experts, search parameters in databases/search engines)	4.3.1	Standardized methods/algorithms and tools (e.g. dictionary comparison)		
2.3.1	Manual (e.g. via databases, search engines and surveys)	3.3.2	Keyword/dictionary/hashtag filter (usually in combination with web crawler and web scraper)	4.3.2	Statistical methods (correlation analysis, time series analysis, panel regression models)		
2.3.2	API interface	3.3.3	Standardized methods/algorithms/tools (e.g. parser)	4.3.3	Deep Learning (in particular vectorization algorithms)		

Figure 4. Trend radar explanation