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 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 remains central to the OSINT process. Future research should develop applications for underserved phases and examine why proven applications aren't widely adopted, focusing on legal, ethical, political, and social factors.

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]. Despite numerous attempts to define OSINT [3, 4, 5], controversy persists, influenced by ongoing advancements in computer and data sciences that continuously enhance collection and analysis capabilities [6, 7]. The surge in open communication channels has led to an "information explosion" [1, 3, 5], making previously restricted data publicly accessible [3, 7], reshaping intelligence paradigms [8]. Despite this heightened interest, fundamental scientific literature in the field remains limited [9], failing to keep pace with rapid developments [6, 7]. Key questions regarding the existence of autonomous third-generation OSINT systems [10, 4] remain unanswered [6, 4, 5] and significant OSINT use cases unexplored [11, 8, 6], lacking qualitative field research to bridge theoretical concepts with practical implementation [9, 10]. This study addresses the research question: question: *How can current OSINT trends, focusing on technologies, characteristics, maturity levels, and use cases, be presented in a trend radar and validated by security sector experts?*

This paper investigates current OSINT trends, adopting the Design Science Research Model (DSRM) [12]. The methodology involves a systematic literature review [13] 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 [14], and evaluated using qualitative content analysis [15].

2. Theoretical Background

The domain of OSINT is continuously expanding due to the ongoing improvements of collecting and analysis possibilities [6, 7]. In addition, the new means and methods of communication associated with advances in information and communication technology have turned OSINT into a complex discipline [16, 7].

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 [17]: *"OSINT is information that has been deliberately discovered, discriminated, distilled, and disseminated to a selected 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." However, today the discipline is no longer seen as a purely governmental matter. Private research institutions and organizations [18, 19] are also massively driving the development of such systems [8, 6]. The focus is thereby shifting to developing OSINT into a robust, autonomous solution (referred to as third-generation) [10].

2.2. Intelligence and Intelligence Cycle

The core task of OSINT is to generate intelligence as a basis for decision-making [20, 17]. The generation process of such an intelligence product is referred to as intelligence cycle [21]. It represents the central element of every intelligence discipline [22]. The link between the phases is that the result of the preceding phase serves as input for the subsequent phase [23], continuously iterated due to the fulfillment of previous requirements and new demands [24]. Today, to represent external influences or the assignment of responsibilities [25, 26], numerous variations can be found [22]. The Intelligence Cycle should therefore be seen less as a guideline and more as an informal coordination element[3]. In 2013, the JCS segmented the cycle into 6 phases [23] (see figure 1).

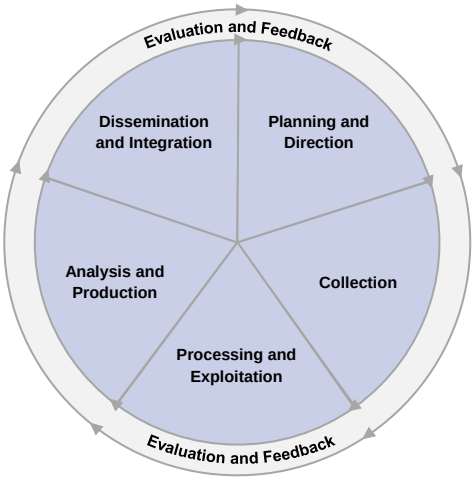

Figure 1. Intelligence Cycle, according to [23]

The planning and direction phase combines the identification, definition, prioritization and monitoring of the requirements [23]. The collection phase refers to the gathering of raw data [21]. It consists of iterative repetition of research [17] to make the query more precise with each run [4]. The processing and utilization phase involves condensing these data volumes into action-relevant information [23]. Analysis and production refers to the synthesis of the information obtained into a timely and accurate intelligence product [3, 17]. The final phase consists of handing over the finished product to the "customer" in a usable form [27, 7]. Evaluation and feedback are not to be regarded as individual phases but take place continuously, to achieve progressive optimization [23, 17].

2.3. Previous Studies

Eight publicly accessible literature reviews exist on OSINT. In 2017, Dos Passos [1] showed how big data and data science enhance decision-making. Pastor-Galindo et al. provided insights into OSINT's state in 2019 and 2020 [10, 4], focusing on cybersecurity enhancements. They conducted the first rudimentary mapping of OSINT trends, observing its use in social opinion and sentiment analysis, cybercrime and organized crime, as well as cybersecurity and cyberdefense. In 2020 García Lozano et al. [28] identified methods for computer-assisted veracity assessment of public information and Herrera-Cubides et al. [9] research and educational material production. They concluded that OSINT publications are fewer compared to other trending topics. In 2021, Yogish and Krishna [5] explored AI implementation in cybersecurity, showing its potential to simplify OSINT given increasing data volumes. In the following year, Hwang et al. [3] investigated security threats and cybercriminality through OSINT misuse. In 2023, Ghioni et al. [6] examined the political, ethical, legal and social implications of OSINT in conjunction with AI, highlighting the absence of a of a comprehensive framework and the early stage of third-generation OSINT, with irreplaceable human components.

3. Research Methodology

The study follows the iterative Design Science Research Model (DSRM), a theory-based research paradigm for developing a directly applicable solution in the form of an innovative artifact [29] to solve a (practical) problem [12]. Hence, the model is ideally suited for creating the trend radar and comprises six successive activities [12]:

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

Section 1 summarizes step 1, while sections 4 and 5 present the outcomes of step 6. Steps 2-5 will be discussed in detail. Continuous evaluation of steps 1-4 occurred throughout the study [30].

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 mirror the intelligence generation process, facilitating structured mapping of identified technologies based on their usage. This enables direct assignment of research gaps to respective phases, verifying the existence of third-generation OSINT systems.

CO2 Key characteristics, particularly technology maturity levels and use cases, must be considered. Technology maturity informs research status determination, while use cases unveil research directions.

Formal objectives (FO):

FO1 The trend radar must follow a simple structure for quick identification of research gaps and high standardization for applicability across intelligence disciplines.

FO2 The trend radar should be continually expandable to capture field dynamics effectively.

3.2. Evaluation of the Problem Statement and Design Objectives

In Section 2, key concepts foundational to the research are defined, focusing on the intelligence cycle. The cycle is crucial as it underpins the development of the trend radar tool, which is evaluated for its compatibility within the OSINT framework. Furthermore, the review of prior studies reveals a significant gap in comprehensive OSINT research, emphasizing the importance and relevance of the inquiry.

3.3. Design and Development

The third activity involves conducting a systematic literature review, guided by Cleven et al. [31]. Cooper's taxonomy [32] is used to scope the review, establishing classification categories for creating concept matrices to structure the literature analysis [13].

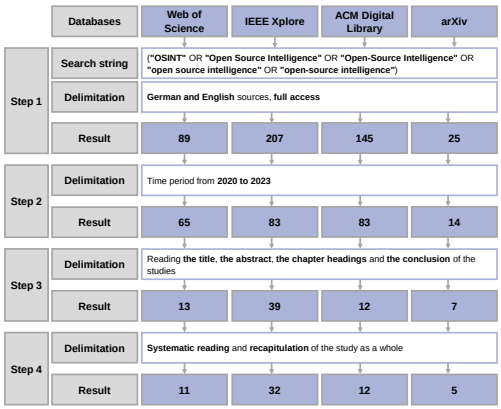

Figure 2. Literature review setup and categorization criteria

To standardize the approach across the intelligence cycle, general categories were defined for each phase, integrating the evaluation and feedback phase due to its iterative nature. For the collection phase, 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 [33, 15, 34].
- **Technology:** Material and immaterial means used for managing information [35].
- **Technology Complexity:** Assessed through subcategories of Volume, Variety, and Velocity [36, 37].
- **Maturity Level:** Based on the phases of innovation, prototype, and market establishment [38].

Similar categories were adapted for the other phases of the intelligence cycle, with complexity measured via the analytics spectrum: descriptive, diagnostic, predictive, and prescriptive [39].

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 [40] 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 forms the foundation of the trend radar, offering clarity and an intuitive framework that simplifies technology extraction and research gap identification. Its design also ensures applicability across diverse intelligence disciplines. By emulating the structure of the federal government's trend radar [38], it achieves robustness, user-friendliness, and appropriate detail, focusing on essential categories like use case, technology, and maturity level.

The concept matrices enable regular updates to the radar, ensuring current and standardized design. Rigorous verification of internal consistency maintains categorization integrity, meeting critical evaluation criteria in contemporary design research [29].

3.5. Demonstration

Next, the trend radar was demonstrated via guideline-based, systematizing expert interviews [14, 41, 42]. Particularly in less structured and sparsely linked subject areas, this method enables dense data collection [14, 42], especially when access to the social field is limited [43, 41].

Experts (table 1) were selected using theoretical sampling [44], focusing on Germany to validate trends in the country. At least one expert from a security authority, the security industry, and a startup was chosen to capture diverse perspectives. A "prestigious" company position ensures respondents possess relevant research knowledge [45].

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	Managing Director of a German start-up, for an OSINT platform	E4

The qualitative data collection utilized semi-structured interviews, ideal for uncovering underlying theoretical relationships [14]. The questionnaire, based on the Intelligence Cycle, commenced with a presentation of the trend radar. Open questions were initially posed for each phase to compare it with respondents' practical experience, reducing subjectivity [46]. Exploratory questions guided conversation flow [46], followed by specific closed questions for targeted follow-up [46]. The Interviews lasted up to an hour, with a maximum of three main questions per phase [14] and were conducted online. The questionnaire underwent pilot testing with a domain expert.

3.6. Evaluation of the First Instance of the Trend Radar

The trend radar demonstration affirmed its intuitive usability and usefulness in providing an overview of OSINT technologies. Practitioners also confirmed its completeness and internal consistency (cf. E1, 14.08.2023; E3, 28.07.2023; E4, 02.08.2023). As a result, the radar proved suitable for identifying research gaps and guiding practitioners. Thus, it meets the essential evaluation criteria [30].

3.7. Evaluation

The evaluation utilized qualitative data analysis [41], which extracts, synthesizes, and structures interview information using a predefined search grid. This facilitates targeted extraction and summarization of relevant, cross-interview information, following a "top-down approach" [14, 41].

First, the interviews were transcribed, followed by analysis using the MAXQDA software. The categorization grid was established within MAXQDA (see repository X), with first-level categories corresponding to the phases of the intelligence cycle. Second-level categories indicate support or contradiction of the experts to the theory, while third-level categories reflect identified use cases. A "general statements" category was thereby added for overarching remarks. The fourth-level categories classify the individual technologies. In total, 257 statements were categorized.

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 align with each phase of the Intelligence Cycle, but no application covers all phases as a third-generation OSINT tool. Literature mainly focuses on the collection phase, followed by analysis and production, and processing and exploitation. The dissemination and integration phase is least covered, followed closely by planning and direction.

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 public data to detect potential cyber threats [47, 48]. Health applications mainly address COVID-19 outbreak investigations [49]. The security use case includes applications such as analyzing violent behavior in public transport [50]. The identified journalism study examines the Twitter activities of the OSINT journalists' association "Bellingcat" [51]. Competitive analysis involves for example the performance classification of Chinese logistics companies [52]. Additionally, two identified studies focus generally on creating knowledge graphs on OSINF [53, 54].

The Experts indicate that OSINT is used in all authorities and various use cases, even if not explicitly labeled as such (cf. E2, 19.07.2023). It is most commonly applied in cybersecurity/CTI (cf. E1, 14.07.2023; E2, 19.07.2023) and general security, especially within the German Armed Forces, the (Federal) Intelligence Service, 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. [55]) and open source solutions like "Tweepy", a Python library for Twitter crawlers (e.g., [56]). More advanced prototypes involve combining parallelized, recursive, source-specific web crawlers and scrapers for improved data collection (e.g., [57]). 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") [58]. Technologies for crawling/scraping the dark web, like "Torsion" [59], 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 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" [60] and the "Stanford CoreNLP Toolkit" [55]. Additionally, deep

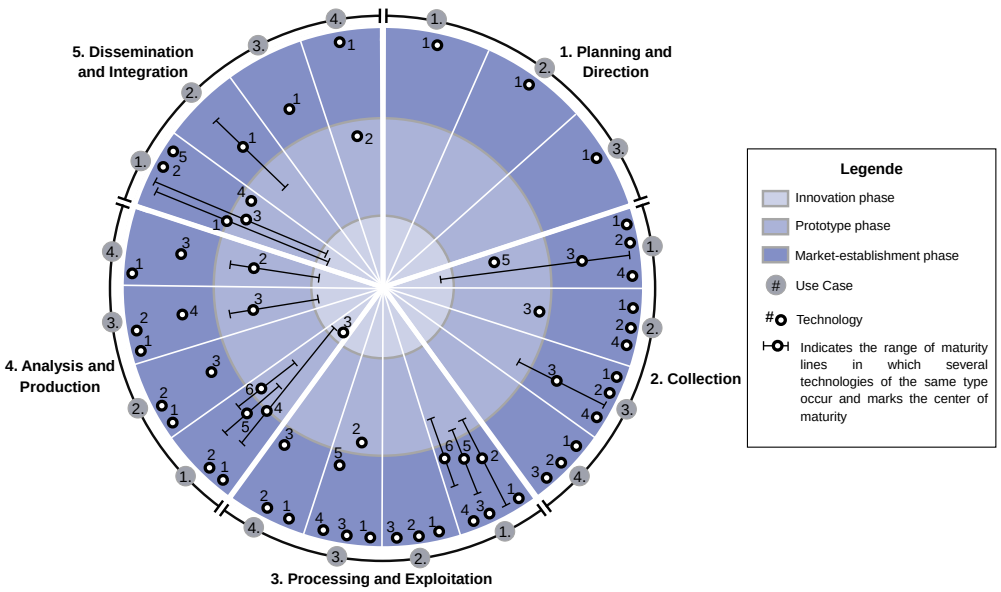

Figure 3. Trend radar

learning, particularly through ”word embedding” using the ”word2vec” algorithm, is prominent (e.g., [61]).

However, the experts note that within authorities this phase predominantly involves manual work due to irreplaceable domain knowledge (cf. E1, 14.07.2023; E2, 19.07.2023; E3, 28.07.2023). The degree of automation depends on the abstraction level: operational tasks needing specific information show lower automation than long-term 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., [54]). Furthermore, even under ML vectorization models such as BERT or ”Supervised Support Vector Machines” (SVM) (e.g., [62]) 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., [52]) or for layered analysis (e.g, [63]). AI technologies are less specified, except for Dale et al. [64], 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. The experts note, that this phase largely relies on manual content analysis due to limited technological understanding and acceptance, in german authorities (cf. E2, 19.07.2023; E3, 28.07.2023; E4, 02.08.2023). Also, ethical and legal barriers, like GDPR (General Data Protection Regulation), hinder technology adoption (cf. E2, 19.07.2023; E4, 02.08.2023). Additionally, security concerns favor standalone systems, with smart technologies often used unofficially (cf. E2, 19.07.2023; E4, 02.08.2023). However, there is a need for modular, expandable systems to keep pace with advancements (cf. E1, 14.07.2023; E3, 28.07.2023; E4, 02.08.2023). Nevertheless, human experience and specialization remain crucial to ensure product quality. Yet, the potential of Large Language Models (LLM) remains uncertain (cf. E4, 02.08.2023).

In the dissemination and integration phase, tools like ”Power BI” [52] are utilized to create dashboards and visualization maps. Furthermore, user interfaces, web applications, and online platforms are developed, including Python GUIs, specific browser applications [65], improved user interfaces and input masks for entire tool stacks [66]. Additionally, automated alert technologies for cybersecurity risk assessments are prevalent [47]. Graph-based visualizations are also common, utilizing tools /libraries like ”Matplot,” ”Networkx,” ”Pygraphistry,” or the ”Neo4j-Browser” [55]. Except from the alerts, the retrieval of results is largely semi-automated, with technologies in the market establishment phase. No information on targeted user tests or new development runs involving user feedback was found in any of the studies. The experts

1	Planning and Direction	2.3.3	Web crawler and/or web scraper	3.3.4	Statistical methods	4.3.4	Machine Learning
1.1	Cyber Security	2.3.4	Other open source tools	3.3.5	Deep Learning	4.4	Journalism, competitive analysis, general approach
1.1.1	Manual	2.4	Journalism, competitive analysis, general approach	3.4	Journalism, competitive analysis, general approach	4.4.1	Manual
1.2	Health	2.4.1	Manual	3.4.1	Manual	4.4.2	Deep Learning
1.2.1	Manual	2.4.2	API interface	3.4.2	Standardized methods/algorithms/tools	4.4.3	Machine Learning
1.3	Security	2.4.3	Web crawler and/or web scraper	3.4.3	Natural Language Processing filters and labeling methods/tools	4.3.4	Machine Learning
1.3.1	Manual	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	4.1.1	Manual	5.1.1	Files/reports
2.1.1	Manual	3.1.2	Keyword/dictionary/hashtag filter	4.1.2	Standardized methods/algorithms and tools	5.1.2	Dashboard/visualization map
2.1.2	API interface	3.1.3	Standardized methods/algorithms/tools	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	4.1.4	Deep Learning	5.1.4	Automated alerts
2.1.4	Other open source tools	3.1.5	Natural Language Processing filters and labeling methods/tools	4.1.5	Machine Learning	5.1.5	Graph creation
2.1.5	Web application	3.1.6	Deep Learning	4.1.6	Artificial Intelligence	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	3.2.1	Manual	4.2.1	Manual	5.3	Security
2.2.2	API interface	3.2.2	Keyword/dictionary/hashtag filter	4.2.2	Statistical methods	5.3.1	Dashboard/visualization map
2.2.3	Web crawler and web scraper	3.2.3	Standardized methods/algorithms/tools	4.2.3	Machine Learning	5.4	Competitive analysis, general approach
2.2.4	Other open source tools	3.3	Security	4.3	Security	5.4.1	Dashboard/visualization map
2.3	Security	3.3.1	Manual	4.3.1	Standardized methods/algorithms and tools		
2.3.1	Manual	3.3.2	Keyword/dictionary/hashtag filter	4.3.2	Statistical methods		
2.3.2	API interface	3.3.3	Standardized methods/algorithms/tools	4.3.3	Deep Learning		

Figure 4. Trend radar explanation

state that there is still very little automation within the authorities during this phase. The final product often comprises only a PDF document, email, or verbal report (cf. E1, 14.07.2023), which suffices in many cases (cf. E3, 28.07.2023). However, beyond OSINT, various automated tools exist that could be applied to the authorities (cf. E4, 02.08.2023). Moreover, there is a lack of necessary feedback for product improvement in practice (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., [6]) concludes negatively for Germany. Identified applications do not fully cover the intelligence cycle, particularly lacking in the planning and direction phase, followed by dissemination and integration. Hence, human analysis remains crucial. However, the finding by Pastor-Galindo et al. [4] 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. [5] that automated, AI-driven solutions, largely eliminating the human component, are indispensable in all OSINT domains. The key research question should be why proven, available applications whose support is needed have not yet found widespread use, especially in german intelligence authorities. Additionally, research should explore how to enhance technical support for the initial and final phases of the Intelligence Cycle

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: Effective dissemination and integration mechanisms tailored for authorities are deficient, primarily due to inadequate user testing and iterative feedback incorporation. The importance of consumer feedback is underscored by established frameworks to enhance product quality and mitigate data overload [23, 17].

RG3 - Modular OSINT Systems: The future of OSINT systems hinges on modular concepts, yet only limited research has been conducted in this area [66, 67].

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 [68, 69, 70].

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 [17].

RG7 - Use of LLMs in Intelligence: While LLMs show promise in intelligence analysis, their operational application remains underexplored [71, 72].

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 [25].

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 [6, 70], it could not be verified whether only public sources [73] 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 [4, 70]. The second limitation stems from classification categories not fully aligning with the MECE (Mutually-Exclusive-and-Collectively-Exhaustive) principle [74], 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, interviews were not conducted with active users and decision-makers within authorities. Also, independent verification of coding by a second researcher is recommended for improved intercoder reliability [43, 41]. Lastly, the research structure followed a linear execution rather than the suggested iterative approach [12].

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] V. Smith-Boyle, "How osint has shaped the war in ukraine," 2023.

[3] 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.

[4] 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.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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

[11] 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.

[12] 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.

[13] 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.

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

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

[16] 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.

[17] North Atlantic Treaty Organization, *NATO Open Source Intelligence Handbook*. 2001.

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

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

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

[21] Central Intelligence Agency, *Factbook on Intelligence*. 1987.

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

[23] 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.

[24] 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.

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

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

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

[28] 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.

[29] 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.

[30] 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.

[31] 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."

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

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

[34] 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.

[35] 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.

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

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

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

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

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

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

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

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

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

[45] 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.

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

[47] 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.

[48] 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.

[49] 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.

[50] 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.

[51] 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.

[52] 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.

[53] 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.

[54] 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.

[55] 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.

[56] 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.

[57] 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.

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

[59] 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.

[60] 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.

[61] 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.

[62] 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.

[63] 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.

[64] 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.

[65] 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.

[66] 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.

[67] 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.

[68] "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.

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

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

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

[72] 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."

[73] North Atlantic Treaty Organization, *NATO Open Source Intelligence Reader*. 2002.

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