Global Research Review in Business and Economics [GRRBE]
ISSN (Online) 2454-3217, ISSN (Print) 2395-4671
| Open-Access | Volume 11, Issue 01,
Pages 87-94 ||2025||

OPEN-SOURCE INTELLIGENCE IN EDUCATION AND DIGITAL COMPETENCY DEVELOPMENT

[1]Marta Stoian, [2]Maxim Cetulean
[1,2]*Department of Economics and Economic Policy, Bucharest University of Economic Studies, Romania*

ABSTRACT

In a digital age marked by broad access to information, Open-Source Intelligence has emerged as critical to analysis, security, and contemporary education. This paper outlines the function and use of OSINT in education, specifically how it contributes to the formation of digital skills, critical thinking, and media literacy. The tools and techniques of OSINT are explored in detail throughout this study to demonstrate their value in the educational process. Yet, this very use raises a number of issues concerning data protection, methodological constraints, and the absence of an educational infrastructure. Integrating OSINT into academic programs and encouraging a responsible, ethical information culture are among the recommendations made in this paper. Thus, the present research stresses the importance of a strategic approach to the integration of OSINT so that future learners may be equipped with adequate knowledge to face the impending challenges posed by the digital society.

KEYWORDS - Open-Source Intelligence (OSINT), Education, Digital Competencies, Tools and Strategies.

1. INTRODUCTION

The digital revolution of the late 20th century has fundamentally altered the information environment, bringing spectacular progress in data analysis. Open-Source Intelligence (OSINT) contributes significantly to cyberspace security by offering advanced tools for detecting, assessing, and responding to threats in ever-changing digital environments. The growth of the World Wide Web and rapid globalization has led to an enormous increase in the amount of information available online, facilitating the use of OSINT for predicting cyber threats. As a result, this has led to the development of advanced data collection methods, contributing both to the consolidation of international cooperation and the generation of a knowledge-sharing culture (Szymoniak et al., 2024). It, therefore yields many socio-economic advantages, from gathering information from publicly available sources without depending upon classified resources, to analyzing various types of information in real time. This improves the detection of online threats and the process of making appropriate decisions.

Even with its huge possibilities, OSINT is not utilized to its full potential in many fields, including education. This is due to some barriers that hinder the development of needed skills in information analysis and critical thinking, especially as information becomes increasingly complex. OSINT is often thought of as less than private intelligence gathering methods, leading to its undervaluation. Also, many decision-makers believe that open information is not as trustworthy or useful as private intelligence and this leads to limited investment in OSINT development. Concerns about its reliability for major decisions, mixed with unclear rules and fears of breaching basic rights, have stopped it from being widely used in school courses. Due to this, the majority of individuals remain unaware of the advantages OSINT can provide, which in turn restricts its application in crucial areas.

OSINT has a great deal of potential yet it is stymied by many challenges. These include, among others, unanticipated bias in traditional practices, underdeveloped technological infrastructure, cultural, legislative and ethical barriers, technical complexity, and a lack of trained specialists. All of these stand in the way of the wide spread adoption of OSINT, thereby limitating its role in combating disinformation.

Therefore, a significant shift is needed to move beyond these barriers - one that prioritizes structured OSINT education, establishes regulations for its application in educational institutions and other areas, and enhances collaboration among public, private, and academic sectors to foster a robust technological and methodological framework.

2. LITERATURE REVIEW

According to specialized literature, OSINT has been undeniably positioned as a valuable asset in many activities, from security, journalism, and geopolitical analysis to risk management, economics, academic research, and data protection (Zegart, 2022). Also, recent works prove that the availability of open-source data has greatly increased thanks to technological advancements, while the integration of artificial intelligence in data processing has considerably improved analysis and decision-making capabilities (Poursabzi-Sangdeh et al., 2021). All of this led to the optimization of data collection and analysis techniques, enabling faster processing of large volumes of information with greater accuracy in assessments. Today, OSINT is considered a strategic tool against misinformation, frequently used for source verification and tracking information manipulation.

The definition of OSINT has changed over the years as it attempted to grasp the phenomenon and integrate it into the intelligence domain. All its definitions illustrate how OSINT evolved from merely gathering publicly available information to a more complex discipline, now integral to modern intelligence operations. Its importance has grown alongside the rise of the internet and digital technologies, which have made massive volumes of public information accessible. Proper analysis and interpretation of these data can yield very useful insights in several disciplines, including national security and geopolitical analysis, among others.

In education, studies such as those conducted by Smith and Johnson (2020) highlight that incorporating OSINT into academic programs could improve digital literacy, source verification skills, and critical thinking abilities. However, other research identifies numerous challenges, such as low levels of in-service training among teachers, poor technological infrastructure, and unwillingness of educational institutions to embrace different approaches to information analysis.

Yet, earlier studies (Wilson et al., 2022) show that the integration of OSINT into higher learning curricula can greatly assist in cultivating skilled professionals in cybersecurity, investigative journalism, and even risk analysis. As noted by Taylor (2021), the use of OSINT tools within an academic setting provides deeper insights into the mechanisms behind disinformation, while also contributing to the development of practical skills related to open-source data analysis.

According to the existing literature, it is clear that OSINT holds enormous promise in education; however, there is little to no advancement. This is majorly caused by institutional, technological, and ethical constraints. However, research indicates that including OSINT in curricula and encouraging collaboration with the tech industry can transform this field into a fundamental instrument for equipping youth with digital and analytical skills, aiding them in navigating an increasingly complex information landscape, and providing them with the essential skills to critically assess and utilize publicly available information.

3. RESEARCH RESULTS

With the ongoing growth of internet services and digital data, the availability of public information has become a well-established reality. Open-Source Intelligence (OSINT), which relies on the collection and analysis of open-source information, ensures access to a huge volume of legally obtainable data without contravening any regulations on privacy or copyright (Carcaño et al., 2018). Government documents, public reports, budgets, press briefings, professional and academic publications, conferences, commercial data, financial and industrial assessments, different databases, technical reports, or geospatial information, are just some examples of the variety of data available to the public (Herrera-Cubides et al., 2020). A simple online search can reveal sensitive information about anything or anyone, making it crucial to be aware of the associated risks. Especially among students, a lack of understanding of how data is collected and used can create gaps that can be exploited, which further underlines the need for digital literacy and data protection awareness to be seriously considered in today's world (Shaneck et al., 2016).

Christopher Harper and Robert Bassett Cross argue that OSINT will enable future leaders to rapidly develop a comprehensive understanding of the operational environment. They would further incorporate it into a more integrated use of OSINT within the broader intelligence cycle, where adversarial efforts to expand influence and undermine security could be proactively anticipated, deterred, and neutralized.

1. The Evolution of Information Gathering and Analytical Frameworks

The emergence of Open-Source Intelligence (OSINT) has fundamentally redefined the paradigm of information collection and analysis, which traditionally relied on access to classified data. David Wallach states that automated

OSINT platforms have dramatically improved the ability to transform huge quantities of raw data into actionable intelligence, thereby sharpening strategic decision-making frameworks as well as enhancing operational awareness. This not only signifies a transformation in the traditional security analysis but also indicates its critical role in cyber and cognitive warfare, where OSINT takes center stage as a key element in identifying and countering disinformation, psychological operations, and strategic influence activities. Therefore, in the fast-paged digital age, nurturing a professional workforce in open-source intelligence within information security is crucial to maximizing the utilization of all available resources. Some argue that such structures are a leap forward in the fight against cybercrime but that they too face challenges of a peculiar nature. These include massive volumes of data to be handled, legal and ethical constraints, dealing with censorship and political restrictions, as well as ensuring operational security (OPSEC).

Thus, the use of Open Source Intelligence with the incorporation of Artificial Intelligence is very relevant to gain optimal benefit from OSINT due to the scale, complexity, and diversity of data. While AI facilitates analytical processes, it also empowers intelligence professionals, accelerating the analysis cycle and improving the understanding of strategic threats. There are several barriers that hinder the effective application and use of OSINT, including methodological constraints in information analysis, challenges in evaluating and disseminating intelligence, and resource constraints caused by underinvestment in tools and technologies. All these constraints not only restrict OSINT's effective use but also shape perceptions about its reliability and strategic value.

The primary goal of OSINT is to legally and ethically collect and analyze data from open sources, such as the web, social media, mass media, online scanners, and public databases created by government administrations. According to Golden Owl's specialists, OSINT has greatly evolved, becoming an integral part of the digital world and expanding its application into civilian fields such as education, business, and law enforcement.

2. The Integration of OSINT in Education: Developing Digital Competencies

When it comes to education, OSINT tools facilitate the detection and interpretation of global trends, which aids in the improvement and adjustment of academic curricula. The corporate world leverages OSINT for strategic intelligence gathering as well as market analysis and risk management. Similarly, NGOs and international organizations employ OSINT in monitoring humanitarian crises, investigating human rights violations, and optimizing aid operations. However, all of this calls for a responsible application in all these fields, in order to mantain public trust and to properly protect individual rights. Open-source investigations by non-state actors need to have some of the best practices, precisely defined and uniformly standardized, due to the unique challenges posed by the digital landscape regarding online privacy and ethical concerns. Comprehensive frameworks on digital norms and potential risks must first be established to develop strong legal and ethical principles that protect digital rights and ensure responsible collection and dissemination of information (Szymoniak et al., 2024).

From an educational perspective, OSINT can be considered a very fruitful tool for promoting digital literacy and critical thinking, through which vast amounts of information, from various open sources, can be accessed. In today's world, where information spreads rapidly, filtering, verifying, and correctly interpreting it require essential digital literacy skills. Integrating OSINT into curricula advances the educational process by allowing students to analyze real-world case studies, deepening their knowledge and understanding of cybersecurity and geopolitical analysis. However, OSINT must be applied responsibly and ethically, as it comes with some challenges, such as exposure to misinformation and data privacy risks. Therefore, a well-structured framework for OSINT integration in education needs to be adapted to each stage of the learning process, in order to foster the requisite competencies, including critical thinking, source verification, and open-source data responsibility (Pune, 2023). Further development of these practices requires educational institutions to adopt more engaging teaching methods-such as simulations and case studies, fact-checking exercises, or online courses-enabling students to learn how to recognize trends and patterns in the misinformation flow, validate real media content, and critically evaluate online sources. Advanced search techniques, including Google Dorking and web archives, will aid in discovering obscured information, while data analysis tools will enhance students' understanding of data collection, correlation, and interpretation processes (Pastorino et al., 2019).

The successful integration of this practice strongly depends on the enthusiastic participation of teachers and the whole academic community. Instructors ought to be trained in advanced OSINT methodologies so they can better integrate these practices into the teaching system. Therefore, collaboration with various OSINT companies will be valuable as they can offer instructor-led training and mentoring. Also, partnerships with universities, security firms, and media organizations will help create new academic programs like OSINT hackathons that support the real acquisition of these competencies through hands-on learning. At this stage, it is crucial for both educators and learners to have a solid understanding of the legal and ethical aspects of open-source information. In this way, OSINT could serve as a simple yet powerful teaching tool, helping to cultivate a generation that understands how to meaningfully and responsibly navigate its way through the online world.

3. OSINT Tools And Techniques

OSINT tools are very significant in today's learning environment by developing critical thinking and gaining digital skills. Different search engines, including Yandex and Baidu, can be integrated into the learning process to demonstrate how various indexing algorithms distribute web resources geographically. Bing Images can be useful for academic projects involving image analysis and visual content verification. Additionally, Satellite.pro can support geospatial education by providing students and researchers with tools for satellite image analysis, mapping, or distance measurement.

Shodan can help demonstrate how devices are indexed and assist in evaluating critical infrastructure vulnerabilities. ExifTool is valuable for digital forensics and validation of data authenticity, enabling students to perform metadata analysis on image, video, and document files. Maltego can exemplify network analysis and relationship mapping by introducing advanced data visualization techniques for investigating interconnectivity between resources.

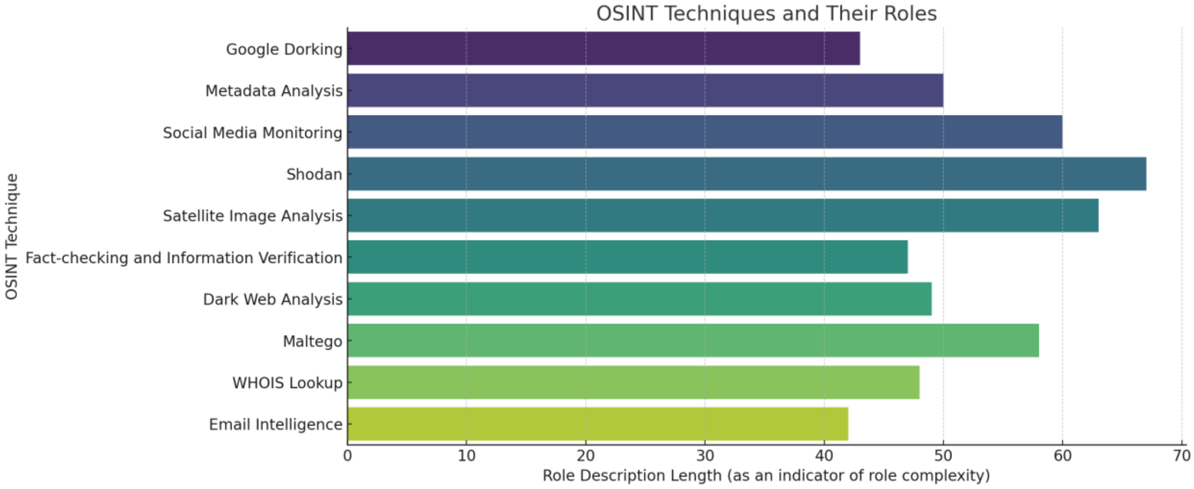

Figure 1:The Role and Complexity of OSINT Techniques

Integrating all these techniques into education will not only enhance students' digital abilities, but will also provide them with firsthand experiencing in advanced research/data analysis methodologies. Some of the skills students will gain are related to assessing social networks for tracking disinformation campaigns, applying advanced search methods to access credible sources, and verifying documents and images to mitiggate cybersecurity risks. In a setting characterized by serious threats such as fake news and cyberattacks, robust OSINT skills become crucial for making informed decisions. OSINT-based education prepares future professionals for the dynamic digital world, inspiring them to take part in the creation of a responsible and ethical information culture (Mäses et al., 2020).

OSINT Techniques	Role	Benefits for Students	Countries with Predominant Use (Europe)
Google Dorking	Advanced search techniques for uncovering hidden online information	Enhances critical thinking and deep web searching skills	Germany, France, Netherlands
Metadata Analysis	Extraction and analysis of metadata from files, images, and documents	Teaches digital forensics and data validation methods	France, Germany, Spain

Geospatial Intelligence (GEOINT)	Use of satellite imagery and mapping tools for location intelligence	Develops geographical and environmental analytical skills	Germany, Italy, France
Social Media Intelligence (SOCMINT)	Monitoring and analyzing public social media data	Improves media literacy and social awareness	Germany, Spain, Netherlands
Domain and Network Analysis	Investigating website domains, IPs, and server infrastructures	Enhances cybersecurity knowledge and investigative skills	Germany, Netherlands, France
Image Reverse Search	Identifying original sources of images and tracking online presence	Improves verification of visual content and source credibility	France, Italy, Spain
Public Database and Registry Research	Accessing legal, corporate, and governmental records	Promotes transparency and data-driven decision-making	Germany, France, Belgium
Dark Web Monitoring	Tracking cyber threats and illicit activities on the dark web	Introduces ethical hacking and cyber investigation techniques	Germany, Netherlands, France
Real-time Information Monitoring	Gathering and analyzing real-time data from news, social media, and forums	Develops real-time situational awareness and trend analysis	France, Germany, Spain
Data Correlation and Link Analysis	Mapping connections between entities, individuals, and organizations	Teaches relational data analysis and pattern recognition	Germany, France, Netherlands

Table 1: OSINT Techniques: Roles, Benefits and European Adoption

This will help learners grasp the extent of enormous personal data available online and how easily it can be correlated and analyzed. Specifically, they will understand that a seemingly innocuous detail, like a username, can be used to correlate disparate datasets and, hence, reveal a person's identity across multiple platforms-dramatically shaping their perception of digital security. A significant lesson for students is that, rather than requiring sophisticated search processes, years of experience, and advanced skills to gather information about a person's identity, such data can now be quickly acquired by anyone with an internet connection. This will make them reconsider how safe they are online, leading them to actually think about how they can protect themselves. This insight will reinforce the understanding that safeguarding personal information does not arise from a single decision but rather from a shared responsibility shaped by the awareness and actions of everyone. Many will become more cautious about sharing information online, and some may significantly reduce their usage of social media platforms. Furthermore, understanding that online safety does not solely belong to an individual, being a collective responsibility, will make people more mindful of how their actions can affect other's privacy. Additionally, individuals engaged in advanced OSINT activities will not only seek to maintain their information secure, but they will also feel a duty to educate and warn others about the risks associated with being online. Within the European Union, Germany, France, and the Netherlands have integrated OSINT practices into their national security strategies to detect misinformation and cyber threats. Moreover, open-source intelligence in Spain and Italy supports investigative journalism and public awareness of digital risks.

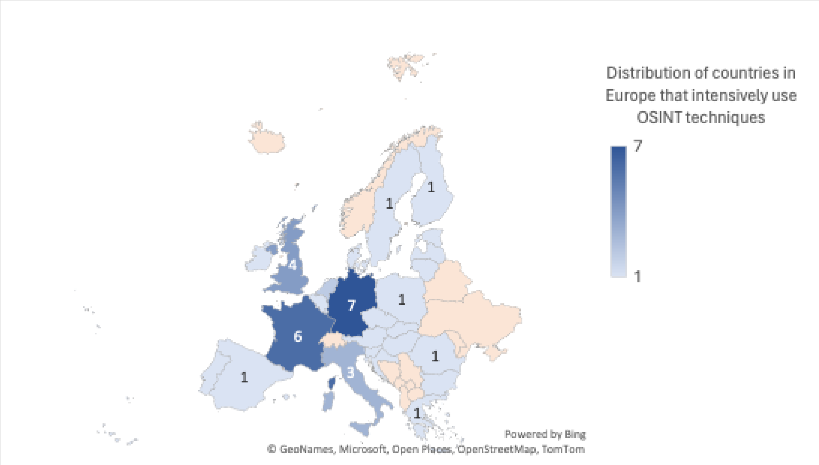
Distribution of countries in Europe that intensively use OSINT techniques
7
1
1
1
4
7
1
6
1
1
3
1
Powered by Bing
© GeoNames, Microsoft, Open Places, OpenStreetMap, TomTom

Figure 2: Distribution of countries in Europe that intensively use OSINT techniques

Fundamentally, this will result in better digital consciousness, changing students' behaviour from being passive internet users into dynamic participants in their own cybersecurity. They will change their ways of using the internet, advocating for a more cautious approach regarding the use of digital tools. In the current geopolitical situation, neglecting the potential of OSINT would represent a major security risk, since open sources are increasingly crucial for providing critical information across numerous levels of analysis and comprehension. With ongoing technological and methodological advances, OSINT's ability to meet user needs are rapidly expanding. This is why integrating academic expertise into OSINT initiatives is essential. To adress these issues, intelligence service development strategies should therefore incorporate the creation of favorable conditions for universities to adapt their curricula, expanding studies in security, artificial intelligence, and OSINT. In other words, if OSINT is controlled by organizations that are primarily focused on classified information, then it will not receive the proper resources, attention, and environment to evolve (Norton, 2020). For this reason, OSINT could remain undeveloped and be treated as a minor sphere of operations since it does not get the necessary institutional support for its integration into analytical functions.

4. OSINT Strategy 2024-2026

In this context, OSINT Strategy 2024-2026 explicitly highlights steps to disentangle the deadlock and make OSINT an integral part of the decision-making process. It emphasizes the establishment of a unified management system for collecting open sources, aimed at improving the process of data gathering and information sharing, both within and between intelligence agencies. The report includes provisions to enhance open-source data collection and usage within the intelligence community. The document defines four areas of interest: coordinating open-source data acquisition and expanding data sharing, establishing an integrated management system for open-source collection, promoting innovation in OSINT to provide new capabilities, and developing the next generation of OSINT professionals and methodologies (U.S. Department of State, 2024). Training a new generation of OSINT analysts requires close collaboration with both academia and the private sector, as well as the development of strategic partnerships for the exchange of best practices.

The OSINT Strategy 2024-2026 represents one of the most important steps in the development of this new discipline and, as such, indicates the imperative need to separate OSINT from the traditional binary model of classified intelligence. It nurtures a more open approach that reflects modern challenges in today's geopolitical and technological landscapes. To highlight the key aspect of developing a specialized community for gathering and analyzing open-source information, the strategy should outline concrete steps for the next generation of OSINT experts, while integrating specialized methodologies into university curricula. The implementation would allow universities and other educational institutions to advance their expertise in the area of information acquisition and analysis, equipping future practitioners with the necessary skills to navigate an environment of perpetual change (Office of the Director of National Intelligence and CIA, 2024).

The strategy also highlights the importance of fostering strong partnerships between industry and academia to facilitate knowledge-sharing and nurture new talent in the field of OSINT. Such an integrated approach would serve to greatly enhance the quality of intelligence education while simultaneously ensuring that the succeeding workforce is adequately prepared to meet the demanding requirements of security and defense. Thus, the OSINT Strategy 2024-2026 expresses a strong commitment to education and training, recognizing OSINT as instrumental in developing a competent and resourceful intelligence workforce.

4. CONCLUSION

That being said, in the current geopolitical context, ignoring the potential of OSINT utilization represents a significant security vulnerability. The ability of open sources to respond to the needs of beneficiaries across all levels of information and knowledge, continues to grow alongside the advancements in this field. The inclusion of academic representatives in OSINT-specific activities is particularly important, especially due to their expertise and access to new sources of information. Intelligence service development strategies should encourage universities to expand their curricula in the fields of security studies, artificial intelligence, and OSINT. A security culture requires the participation of the entire society in ensuring national security by promoting and strengthening democratic values, developing a shared understanding of challenges and opportunities in national security at both the state and societal levels. Advancements in the academic and commercial sectors, along with the development of government-provided tools, offer the possibility of reducing the time required to exploit open-source data. Consequently, dedicated and sustained training programs will be necessary to ensure that the workforce can optimize the use of OSINT. Even though the initial stages may be slow, requiring repeated efforts to acquire the expertise needed for handling more complex and sensitive workflows, prioritizing trust and adopting a structured change management plan are essential. Every educational institution must develop the capacity to monitor and analyze disinformation in real time. Meanwhile, investing in OSINT tools and collaboration with technology companies are crucial for building the technical expertise necessary for students and educators in the digital era. Implementing dedicated OSINT educational programs will foster the development of analytical and critical thinking skills, which are essential for identifying credible sources and objectively evaluating information.

REFERENCES

1. A. B. Zegart, "*Spies, Lies, and Algorithms: The History and Future of American Intelligence*", Princeton University Press, 2022.

2. C. Pastorino, *“Técnicas y Herramientas OSINT Para la Investigación en Internet”*, Welivesecurity by ESET, 2019. Available online: https://www.welivesecurity.com/la-es/2019/10/07/tecnicas-herramientas-osint-investigacion-internet/.

3. C. Wilson, *“University Project - OSINT and Cloud Services Discovery Tools”*, 2022. Available online: https://craigwilson.blog/post/2022/2022-01-30-osintcloud/.

4. F. Carcaño, *“What Is OSINT and What Are Open Sources?”*, FCD Intelligence, 2018. Available online: https://www.fcd-intelligence.com/2018/09/que-es-osint-y-que-son-fuentes-abiertas/

5. F. Poursabzi-Sangdeh, D. G. Goldstein, J. M. Hofman, J. W. Vaughan, and H. Wallach, *“Manipulating and Measuring Model Interpretability”*, in CHI Conference on Human Factors in Computing Systems (CHI '21), Yokohama, Japan, May 8–13, 2021, ACM, New York, NY, USA. https://doi.org/10.1145/3411764.3445315.

6. 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. https://doi.org/10.3390/app10217617.

7. J. Smith and P. Johnson, *“Professional Development and Its Impact on Teacher Effectiveness in Science Education”*, Education and Science, vol. 45, no. 4, pp. 512–529, 2020.

8. M. Pune, *“Open Source Intelligence (OSINT). Market Research Report-Global Forecast to 2023—Market Analysis, Scope, Stake, Progress, Trends and Forecast to 2023”*, Market Research Future, 2020. Available online: https://www.marketresearchfuture.com/reports/open-source-intelligence-market-4545.

9. M. Shaneck and G. Shaneck, *“Teaching Students to Be Internet Stalkers: Experiences From An Open Source Intelligence Class Project”*, Journal of The Colloquium for Information Systems Security Education, vol. 4, no. 1, 2016.

10. Office of the Director of National Intelligence and Central Intelligence Agency, *The IC OSINT Strategy 2024-2026*, May 2024. [Online]. Available: https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf.

11. R. Norton, *“Guide to Open-Source Intelligence”*,Intell. J. US Intell. Stud., vol. 18, pp. 65–67, 2011. Available online: https://www.afio.com/publications/Norton_Open_Source_in_AFIO_INTEL_WinterSpring2011.pdf.

12. S. Mäses and O. Maennel, *“A Method for Teaching Open Source Intelligence (OSINT) Using Personalised Cloud-based Exercises”*, Conference Paper, 2020.
Available: https://www.researchgate.net/publication/340023320.

13. S. Szymoniak and K. Foks, *“Open Source Intelligence Opportunities and Challenges: a Review”*, Advances in Science and Technology Research Journal, vol. 18, no. 3, pp. 123–139, 2024. https://doi.org/10.12913/22998624/186036.

14. Taylor, J., *"Open Source Intelligence: A Comprehensive Guide*", Cybersecurity Publications, 2021. Available: https://www.cybersecuritypublications.com/osint-guide.

15. U.S. Department of State, *“Open Source Intelligence Strategy”*, May 2024. [Online]. Available: https://www.state.gov/wp-content/uploads/2024/05/INR-Open-Source-Intelligence-Strategy.pdf.