Cybersecurity and Law

2025 Nr 1(13)

DOI: 10.35467/cal/214564

Advantages and Disadvantages of Data Collection Through Open Source Intelligence Tools

Katarzyna POPŁAWSKA-BARAN
War Studies University
ORCID: 0009-0008-6662-4832
E-mail: k.poplawska@akademia.mil.pl

Grzegorz PILARSKI
War Studies University
ORCID: 0000-0001-9728-2611
E-mail: g.pilarski@akademia.mil.pl

Abstract

The development of the Internet and the dynamic growth in the number of digital data sources have resulted in a strong need for appropriate tools to facilitate and streamline the collection and processing of information. The response to this need is the widely available Open Source Intelligence (OSINT) tools. The aim of this article is to identify the advantages and disadvantages of using widely available OSINT software to acquire, collect, analyse, process and share data.

In order to address the above issue, an analysis of the subject literature, online publications and press sources was carried out. The literature analysis consisted of compiling, organising and interpreting the content contained therein with regard to the use of OSINT tools.

The right choice of tools, combined with a well-thought-out long-term strategy, can significantly support processes such as the rapid acquisition of necessary data and information, facilitating project management and key decisions relevant to the security of both small and medium-sized enterprises and multinational corporations.

However, the use of this type of software also has certain limitations that should be taken into account when planning a long-term strategy. Data redundancy and difficulties in analysing and interpreting information are just some of them, so it is worth paying attention to both the advantages and disadvantages of OSINT tools

Keywords

Open Source Intelligence, open source, information, data, OSINT tools

Introduction

Current civilisational progress has largely facilitated everyone's access to a virtually unlimited amount of information, but the sheer volume of data that surrounds us means that it has become a real art to obtain information that is reliable, consistent and up to date. There are many techniques for obtaining information, which is why it is so important to select the right methods and sources to avoid chaos and confusion[1]. One way is to use open sources of information through Open Source Intelligence. Open Source Intelligence (OSINT) is the process of analyzing publicly available information to produce actionable intelligence, while an „open source of information" is the raw, unprocessed data itself.

The term was defined in the 2002 NATO Open Source Intelligence Reader document. OSINT is „the result of performing certain activities on information. It is specifically sought out, compared in terms of content, and the most important information for the recipient of the process is selected"[2]. OSINT itself is much older, as governments have long used newspapers, and later radio and television broadcasts, to track the military, political and economic plans and activities of their potential adversaries.

Cameron Colquhoun, director of Neon Century, a corporate intelligence company, pointed out in an article on the history of OSINT that OSINT fell out of favour after the Second World War as intelligence agencies focused on more spectacular and dangerous human intelligence (HUMINT) and signals intelligence (SIGINT)[3]. However, OSINT has made a strong comeback with the development of the Internet, social media and online tools that can sift through vast amounts of information. As Colquhoun noted, and it is difficult to disagree with him, OSINT is now more relevant than ever, and at the same time it is low-risk, inexpensive and often extremely effective.

Open Source INTelligence makes it possible to track trends in information technology and provides selected entities with the tools and technologies needed to acquire and use information more effectively and efficiently[4]. It allows for early warning and prevention of threats to security in the broadest sense. Open Source INTelligence offers enormous possibilities of searching for, collecting and preliminarily analysing information, but it is not without its drawbacks.

The biggest problems in using open source intelligence techniques include the enormous volume of information, the lack of qualified personnel dealing with

[1] A. Schenko, Procesy informacyjne w zarządzaniu https://slidetodoc.com/1-procesy-informacyjne-w-zarzdzaniu-wykad-1-rola/ [access: 11.10.2025].
[2] NATO Open Source Inteligence Reader, https://www.slideshare.net/slideshow/nato-osint-reader-final-11-oct02/28741968 [access: 11.10.2025], translation for K. Jarczewska-Walendziak, Wykorzystywanie otwartych źródeł informacji przez służby śledcze, „Toruńskie studia bibliologiczne" 2017, no. 1(18).
[3] C. Colquhoun, A Brief History of Open Source Intelligence, 2014 https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/ [access: 11.10.2025].
[4] M. Meller, Praktyczny OSINT z wykorzystaniem technologii internetowych, [in:] S. Cisek, A. Januszko-Szakiel (ed.), Zawód infobroker. Polski rynek informacji, Warsaw 2015, pp. 311–323.

OSINT issues, and the diversity of the information flooding us. All of the identified obstacles are a reason to consider effective solutions that would minimise or even eliminate the threats presented. Despite the wide range of options in the area of Open Source Intelligence, there is a lack of systematic knowledge on how to effectively use the available software to carry out intelligence tasks.

The main objective of this publication is to identify the advantages and disadvantages of using publicly available OSINT software to acquire, collect, analyse, process and share data. The research problem was defined in the form of the following question: what are the advantages and disadvantages of using publicly available Open Source Intelligence programmes to obtain data using white intelligence methods, and what challenges do its users and developers face?

In order to address the above research problem, the authors carried out an analysis of the literature on the subject, online publications and press sources. The literature analysis consisted of compiling, organising and interpreting the content contained therein in relation to the research problem. The following theoretical methods were used to systematise the materials: analysis, synthesis, analogy, comparison and inference.

Open Source INTelligence

The development of the Internet and the exponential growth of information we have been dealing with in recent decades has caused a real problem for specialists in searching for information using overt methods[5]. In the current information age, most sources are digital formats of former traditional media and dynamically growing social media. We must also not forget the development of the Internet of Things (IoT), i.e. systems of electronic devices "that can automatically communicate and exchange data via a network without human intervention"[6]. The current acquisition of information is greatly facilitated by the far-reaching automation of the entire open source intelligence process and the use of sophisticated analytical software designed to acquire, collect, analyse, process and present information in a clear graphical format[7].

It is also worth focusing on the issue of information gathering itself. Basically, there are three ways to collect information[8]:

- passive, which involves collecting data with the use of publicly available resources;

[5] B. Sarmak, Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy, Warsaw 2015, p. 37.
[6] M. Jaskólski, Co to jest Internet Rzeczy (IoT)? https://www.benchmark.pl/aktualnosci/co-to-jest-internet-rzeczy-iot.html [access: 15.10.2025].
[7] T. Serafin, Automatyzacja procesu wywiadu jawnoźródłowego w ramach działalności wywiadowczej i walki z terroryzmem, [in:] (ed.) K. Liedel, P. Piasecka, T.R. Aleksandrowicz, Analiza informacji w zarządzaniu bezpieczeństwem: zarządzanie bezpieczeństwem, Warsaw 2013, p. 83.
[8] A. Rachamalla, Know about OSINT and how it is used, https://telanganatoday.com/know-about-osint-and-how-it-is-used [access: 20.10.2025].

- semi-passive, i.e. sending internet traffic to the target server to obtain information;
- active, i.e. in direct contact with the system from which the data is collected, this type of data collection leaves a clear trace.

In the case of open-source intelligence, this is passive collection, characterised by two factors[9]:

1) the data comes exclusively from open sources of information;
2) the search is completely anonymous from a technical point of view, as the methods used to collect data in the passive category do not send any traffic/packets to the target servers, so the target is unaware of the activities being carried out.

The downside of this type of information gathering may be the limited amount of data that will be obtained, but the risk of detection is very low. The data collection itself can take place on a small scale, using single, very specific queries, or on a large scale, using sophisticated paid tools and resources that are not available to everyone.

Advantages and disadvantages of using OSINT software

OSINT software has its strengths and weaknesses, like any tool. Table 1 summarises the main advantages and disadvantages, which are discussed in detail below.

Table 1. *Advantages and disadvantages of OSINT software*

Advantages	Disadvantages
large amounts of data from multiple sources	information noise
global reach	diversity of information
constant access	unqualified/inexperienced staff
wide range of tools	echo effect
legal aspects	language barrier
cost	false information
ease of access and simplicity of use	lack of versatility

Source: *own elaboration*.

[9] Z. Suski, Rekonesans pasywny w testach penetracyjnych [in:] „Przegląd teleinformatyczny" 2017, no. 3, p. 6.

Since these tools have many areas of application, the pros and cons will be considered from a slightly broader perspective, as what is a positive for one user may be a serious problem for another. The key area affected by this aspect is the amount of data that we can both search and obtain.

Strengths of OSINT software

The advantages of OSINT software include:

1) availability of large amounts of data from multiple sources - the ability to obtain large amounts of data is one of the key elements of OSINT and an important part of intelligence work. Its search area covers the entire cyberspace[10], including public documents, government reports, electronic press, audio and video materials, as well as data from social networks and deeper Internet resources, i.e. the Deep Web and Dark Web[11], which provide their users with significantly greater privacy and anonymity. It is in this field that the analysed software has enormous potential. Both the Deep Web and the Dark Web are not indexed by popular search engines such as Google or Yahoo[12], so more specialised tools are needed to search for specific information. Using the selected software, it is possible not only to obtain large amounts of data, but also to collect it from many sources, and thus to look at it from a broader perspective in order to proceed to analysis, correlation and finding specific connections[13];
2) global reach - by using OSINT software, you can access news from around the world and obtain data and information across traditional national and continental borders. For intelligence operations, this translates into both time and cost savings;
3) constant access - as Nihad A. Hassan and Rami Hijazi note, „OSINT sources are always available and up to date, and can be used by various parties to draw conclusions”[14]. Information is obtained in real time so that the answer to a given query is provided within minutes or hours, rather than weeks or even months, as is the case with traditional intelligence gathering[15];
4) a wide range of tools - the number of OSINT instruments available has been steadily growing for several years, which translates into the dynamic development of existing solutions. Depending on the needs of a given case,

[10] G. Pilarski, Cyberprzestrzeń – relacje w wojnie hybrydowej, Warsaw 2020, pp. 14-24.
[11] G. Kalpakis, T. Tsikrika, N. Cunningham, C. Iliou, S. Vrochidis, J. Middleton, I. Kompatsiaris, OSINT Dark Web, [in:] Open Source Intelligence Investigation, Switzerland 2016, p. 132.
[12] Deep Web, Dark Web i Darknet: czym się różnią, co się w nich znajduje i w jaki sposób działają? https://resilia.pl/blog/dark-web-dark-web-darknet-informacje [access: 21.10.2025].
[13] G. Kalpakis, el.al., , op.cit, p. 168.
[14] N. A. Hassan, R. Hijazi, Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence, Apress 2018, p. 3.
[15] G. Małecki, Współczesny OSINT i jego potencjał w dziedzinie kierowania państwem, https://www.infosecurity24.pl/wspolczesny-osint-i-jego-potencjal-w-dziedzinie-kierowania-panstwem [access: 21.10.2025].

analysts can choose between simple programmes designed for a single type of query, such as TinEye.com[16], and sophisticated tools such as Maltego[17];

5) legal aspect - since the data obtained comes from public sources, there are no legal issues with further disclosure of information to other entities. Information collected in this way can also be used in legal proceedings. Unlike in the case of classified intelligence, we do not cause or increase the risk of exposing intelligence assets (agents or personal sources of information). There is also no need to engage spies, agents, or use proprietary techniques or covert activities. This issue is also important because OSINT software forms the basis of pentesting[18], a field related to cybersecurity and responsible for testing cyber systems and network security[19];
6) cost - what distinguishes OSINT from traditional intelligence gathering tools and methods is its price. It is significantly cheaper than traditional intelligence gathering tools and methods, but low price does not mean low quality. A vast number of OSINT tools are free, while paid solutions allow data to be obtained at a much lower cost than traditional intelligence activities such as the use of personal sources of information or spy satellites. Even the smallest entities with limited budgets are able to obtain the data they are interested in this way[20];
7) ease of access and simplicity of use - a big advantage of using this type of software is that it is widely available and, for the most part, easy to use. A computer with Internet access and basic knowledge of computer networks is all you need to get started. As a result, OSINT has begun to move beyond the closed world of special services and is increasingly being used by various types of companies who, recognising its potential, are creating their own separate units qualified in this area[21].

Weaknesses of OSINT software

The weaknesses of OSINT software include:

1) information noise - the enormous amount of data is also a weakness of OSINT tools, as it is easy to overlook certain information and data in the flood of information. The problem of information noise, i.e. data overload, makes it difficult to distinguish the beginning and end of information, as it is

[16] It is an image search engine that allows you to check where a given photo or graphic has been used, and also allows you to track their sources.
[17] A tool for open source link intelligence and graphical analysis. It allows you to easily and simply extract data from distributed sources, automatically merge matching information into a single graph, and visually map it for convenient exploration of the data landscape.
[18] Pentesting, or penetration testing, is a process during which the security of IT infrastructure is checked by means of a controlled attack.
[19] V. Kumar Velu, Kali Linux. Testy penetracyjne i bezpieczeństwo sieci dla zaawansowanych, Gliwice 2018, p. 25.
[20] N. A. Hassan, R. Hijazi, op.cit, p.15.
[21] G. Małecki, op.cit.

continuous and flows in an uninterrupted stream. For this reason, it is difficult to diagnose what is part of it and what is not, what should be analysed, and what can possibly be omitted. This fact forces us to engage additional resources, means and effort to analyse the material, i.e. an adequate amount of analytical work;

2) diversity of information - the data obtained and collected is extremely diverse, which makes it difficult to examine, combine and classify in order to extract relevant relationships and knowledge[22]. In order to fully exploit the potential offered by OSINT, appropriate mechanisms for text analysis and data exploration are therefore required to enable data standardisation[23];
3) unqualified/inexperienced staff - although most single-source information gathering programmes are not very complicated to use, more sophisticated tools require appropriate training to ensure that they are used efficiently and effectively. Another important issue is that the researcher should have the necessary analytical skills and not only specialist knowledge in a given field, but also a very broad general knowledge, which will allow for a comprehensive overview of the material[24];
4) echo effect - when using OSINT software, we cannot avoid a phenomenon known as the echo effect[25]. Information posted on the web is constantly duplicated and posted in many places without mentioning its source. This causes enormous problems in determining the actual date of posting on the Internet, thus affecting the reliability and timeliness of such data[26];
5) language barrier - there are over seven thousand languages in the world, but English is not the most widely spoken language in the world. Chinese ranks first, followed by Spanish, English, Hindi and Arabic, with a large number of dialects[27]. And although English is the international language of business, it does not enjoy a privileged position in the world of OSINT[28]. It is true that the programmes themselves are written in English, but, as has already been shown, in order to make full use of open sources, it is necessary to analyse and interpret the data appropriately, and therefore to have a broad knowledge of more exotic foreign languages, especially those of interest to the services and intelligence;

[22] G. Bello-Orgaz, J.J. Jung, D. Camacho, Social big data: Recent achievements and new challenges, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7106299/ [access: 25.10.2025].
[23] J. Pastor-Galindo, P. Nespoli, F. Gómez Mármol, G. M. Pérez, The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends, https://ieeexplore.ieee.org/document/8954668 [access: 25.10.2025].
[24] B. Sarmak, op.cit, p. 37.
[25] R.A. Best, A. Cumming, Open Source Intelligence (OSINT): Issues for Congress, CRS Report for Congress, Congressional Research Service, 2007, https://sgp.fas.org/crs/intel/RL34270.pdf [access: 26.10.2025].
[26] B. Sarmak, op.cit, p. 35.
[27] Najczęściej używane języki świata, https://www.ef.pl/blog/language/najczesciej-uzywane-jezyki-swiata/, [access: 26.10.2025].
[28] B. Sarmak, op.cit, p. 36.

6) false information - the reliability of information is definitely key to success in all OSINT investigations[29]. Ideally, the data collected should come from trusted and verified sources, but in practice, data also comes from social networks[30], unauthorised media and other places whose reliability cannot be absolutely guaranteed and which are susceptible to various types of manipulation. In this case, too, the reliable work of an analyst is essential, which will translate into the effective use of OSINT software;
7) lack of versatility - although a wide selection of tools is a huge advantage, for many individuals and organisations, the lack of a single universal solution can be a serious disadvantage and limitation in the use of such instruments. This requires analysts to have a broad understanding of all available programmes, a high degree of flexibility, and the ability to select the necessary tools for each intelligence project.

Challenges for users and developers

Regardless of the advantages and disadvantages described above, users and developers of software for obtaining information from open sources also face many challenges. Overcoming these challenges will allow for even more effective use of such tools, which should translate into greater intelligence effectiveness.

One of the most important challenges is effective data selection, so that information that is irrelevant or incorrect can be filtered out at an early stage. This is important because, as mentioned earlier, the amount of data to be searched is enormous and every day more terabytes of various types of data are added, with 188 million emails alone being sent every minute[31]. An effective programme should allow for very specific and detailed information searches in order to minimise the problem of information noise described above. Analysts also need to know whether the information collected is reliable, as many governments deliberately post incomplete or false information online to mislead the other side[32]. The same applies to information posted on social media or online forums, where users post highly subjective opinions. An appropriate solution could be the ability to automatically compare information with, for example, classified data[33]. This would be particularly important in the case of military or economic intelligence.

Another challenge for OSINT is the broadly understood globalisation of applications[34], as there is currently a lack of comprehensive solutions that focus

[29] S. Gong, J. Cho, C. Lee, A reliability comparison method for OSINT validity analysis, „IEEE Transactions on Industrial Informatics" 2018, vol. 14, no. 12, pp. 5428 -5435.
[30] K. Baumgarth Secondary Research, Design Methodology, https://medium.com/@kellyaba umgarth/secondary-research-design-methodology-5fc4009a79f6 [access: 11.10.2025].
[31] K. Śledziewska, R. Włoch, Wielki wybuch danych, https://nauczycielka-informatyki.pl/wp-content/uploads/2021/10/GospodarkaCyfrowaPrezentacja.pdf [access: 28.10.2025].
[32] N.A. Hassan, R. Hijazi, op.cit., p. 16.
[33] Ibidem, p. 17.
[34] Globalization, also known as localization or multicultural support, is the process of organizing an application so that it can be configured to work in different countries and in different languages,

on universality, internationality and multiculturalism. Individual countries have their own proprietary sources and databases tailored not only to their needs, but also to their legal, moral and cultural conditions. In the case of specialised programming, they often use solutions created by other countries, which does not always go hand in hand with proper implementation and adaptation to the needs of a given country[35]. The ideal solution is a tool that enables immediate reconnaissance around the world, automatically connecting and correlating dispersed data sources. Such solutions would greatly facilitate the tracking and analysis of the activities of international criminal groups, terrorists and criminals who move around the world[36].

When discussing internationality, it is worth considering issues of ethics, morality and law in relation to the data obtained. OSINT is, in principle, public and legal information, but its use must not violate the privacy of users, nor should it in any way harm the private life of a given person or their loved ones, such as family, friends or colleagues[37]. In certain parts of the world, revealing a person's political beliefs, religion or sexual orientation could have serious consequences for them[38]. When considering the legal aspect, it is important to bear in mind the EU's General Data Protection Regulation (GDPR)[39] on the protection of personal data, which is currently in force in European Union countries. According to this directive, personal data includes specific information that may concern any citizen. Importantly, personal data also includes various types of information which, when collected together, can lead to the identification of a natural person, even if it has been encrypted or anonymised[40]. In this case, software development projects should be adapted to these types of restrictions so that no legal conflicts arise in the course of the work.

The final challenge in the use of OSINT tools is the risk of their use by cybercriminals. Using publicly available software, they can obtain data about potential victims as well as plan and carry out attacks on ICT infrastructure. An appropriate step would be to control the use of such tools or develop appropriate access restrictions at the stage of creating a given solution[41].

Definition from: https://www.ibm.com/docs/en/tap/5.0.0?topic=applications-options-globalization [access: 28.10.2025].

[35] J. Pastor-Galindo, et al., op.cit.

[36] Ibidem.

[37] Ibidem.

[38] P. Kubiak, Najcięższe przestępstwa szariatu (hudud) w świetle uwag zawartych w klasycznym podręczniku „umdat al-salik" al-misriego, „Zeszyty Prawnicze" 2019, no. 19(3), p. 165.

[39] GDPR (General Data Protection Regulation) is Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. It entered into force on 17 May 2016 and has been in force in Poland since 25 May 2018.

[40] 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, point 26.

[41] L. Benes, OSINT, new technologies, education: Expanding opportunities and threats. A new paradigm, „Jurnal of. Strategic Security" 2013, vol. 6, no. 3, pp. 22-23.

Summary

Undeniably, the importance of software used to obtain information through open-source intelligence methods has grown enormously in recent times. Both analysts involved in intelligence aimed at internal and external state security, as well as corporate analysts, have recognised the potential inherent in OSINT. The use of OSINT instruments has proven to be a very useful intelligence tool, enabling efficient data acquisition and collection, and is an excellent complement to conventional intelligence[42], especially since it is mostly free of charge.

The right choice of appropriate tools combined with a well-thought-out long-term strategy can help in areas such as[43]:

- obtaining a large amount of necessary data and information in a short time to facilitate project management;
- identifying potential hazards;
- making key decisions that are important for the security of small and medium-sized enterprises as well as international corporations;
- managing national and international security.

However, despite its many advantages, we must also remember that when deciding to use this type of software, we will encounter certain limitations and should take them into account when planning a long-term strategy. Data redundancy and difficulties in analysing and interpreting information are just a few of them.

OSINT still faces many challenges but given the dynamically developing market and the huge demand for this type of service and tool, we should believe that more and better solutions will appear in the near future.

Bibliography

Baumgarth K., Secondary Research, Design Methodology, https://medium.com/@ kellyabaumgarth/secondary-research-design-methodology -5fc4009a79f6.

Benes L., OSINT, new technologies, education: Expanding opportunities and threats. A new paradigm, „Jurnal of. Strategic Security" 2013, vol. 6, no. 3.

Bello-Orgaz G., Jung J. J., Camacho D., Social big data: Recent achievements and new challenges, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC 7106299/.

Best R.A., Cumming A., Open Source Intelligence (OSINT): Issues for Congress, CRS Report for Congress, Congressional Research Service, 2007, https://fas.org/sgp/crs/intel/RL34270.pdf.

Colquhoun C., A Brief History of Open Source Intelligence, 2014 https://www.bellingcat.com /resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence.

[42] The tactical application of open source intelligence (osint), https://cove.army.gov.au/article/tactical-application-open-source-intelligence-osint [access: 28.10.2025].

[43] P. Taleski, The open source future of intelligence, https://www.youngausint.org.au/post/2019/06/15/the-open-source-future-of-intelligence [access: 28.10.2025].

Deep Web, Dark Web i Darknet: czym się różnią, co się w nich znajduje i w jaki sposób działają? https://resilia.pl/blog/dark-web-dark-web-darknet-informacje.

Gong S., Cho J., Lee C., A reliability comparison method for OSINT validity analysis, „IEEE Transactions on Industrial Informatics" 2018, vol. 14, no. 12.

Hassan N. A., Hijazi R., Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence, Apress 2018.

Jaskólski M., Co to jest Internet Rzeczy (IoT)? https://www.benchmark.pl /aktualnosci/co-to-jest-internet-rzeczy-iot.html.

Kalpakis G., Tsikrika T., Cunningham N., Iliou C., Vrochidis S., Middleton J., Kompatsiaris I., OSINT Dark Web, [in:] Open Source Intelligence Investigation, Switzerland, 2016.

Kubiak P., Najcięższe przestępstwa szariatu (hudud) w świetle uwag zawartych w klasycznym podręczniku „umdat al-salik" al-misriego, „Zeszyty Prawnicze" 2019, nr 19(3).

Kumar Velu V., Kali Linux. Testy penetracyjne i bezpieczeństwo sieci dla zaawansowanych, Gliwice 2018.

Małecki G., Współczesny OSINT i jego potencjał w dziedzinie kierowania państwem, https://www.infosecurity24.pl/wspolczesny-osint-i-jego-potencjal -w-dziedzinie-kierowania-panstwem.

Meller M., Praktyczny OSINT z wykorzystaniem technologii internetowych, [in:] S. Cisek, A. Januszko-Szakiel (ed.), Zawód infobroker. Polski rynek informacji, Warsaw 2015.

Najczęściej używane języki świata, https://www.ef.pl/blog/language/najczesciej-uzywane-jezyki-swiata/.

Pastor-Galindo J., Nespoli P., Gómez Mármol F., Pérez G. M., The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends, https://ieeexplore.ieee.org/document/8954668.

Pilarski G., Cyberprzestrzeń – relacje w wojnie hybrydowej, Warsaw 2020.

Rachamalla A., Know about OSINT and how it is used, https://telanganatoday.com/ know-about-osint-and-how-it-is-used.

Sarmak B., Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy, Warsaw 2015.

Serafin T., Automatyzacja procesu wywiadu jawnoźródłowego w ramach działalności wywiadowczej i walki z terroryzmem, [in:] K. Liedel, P. Piasecka, T.R. Aleksandrowicz (ed.), Analiza informacji w zarządzaniu bezpieczeństwem: zarządzanie bezpieczeństwem, Warsaw 2013.

Schenko A., Procesy informacyjne w zarządzaniu https://slidetodoc.com/1-procesy-informacyjne-w-zarzdzaniu-wykad-1-rola.

Suski Z., Rekonesans pasywny w testach penetracyjnych, „Przegląd teleinformatyczny" 2017, no 3.

Śledziewska K., Włoch R., Wielki wybuch danych, https://nauczycielka-informatyki.pl/wpcontent/uploads/2021/10/GospodarkaCyfrowaPrezentacja.pdf

Taleski P., The open source future of intelligence, https://www.youngausint. org.au/post/2019/06/15/the-open-source-future-of-intelligence.

The tactical application of open-source intelligence (osint), https://cove.army.gov.au/article/tactical-application-open-source-intelligence-osint.