

BARTŁOMIEJ TEREBIŃSKI*

Akademia Sztuki Wojennej, Warszawa, Polska

OSINT VS. ENSURING THE SECURITY OF LEGALLY PROTECTED INFORMATION

ABSTRACT: The rapid development of civilization causes the circulation of information in the information space every day to take place at a geometric and precisely defined pace, transmitting and processing petabytes of data. Information used to be just an interdisciplinary term that was the denial of the unknown, but now it is a key factor underpinning the information civilization. Each source of information has its own characteristics and is perceived individually by particular people. Therefore, obtaining information must be systematic and using proven methods. The evolution of the use of open source, publicly available data has led to the development of another intelligence method called Open-Source Intelligence. This study aims to describe ways of legally analyzing publicly available information, while maintaining ethical and legal constraints. To identify the indicated research areas, analysis and criticism of the literature and analysis of data taken from media reports regarding information leaks into the public space were used.



KEYWORDS: OSINT, methods of obtaining information, passive reconnaissance, active reconnaissance.

INTRODUCTION

In the modern world, defined as an information civilization (see Fig. 1), information, assessed as a value constituting capital, not only intellectual capital, becomes a strategic raw material. It is not without reason that it is said that the one who has the power has knowledge, or in a narrower sense – information.

We should agree with James Gleick that information is everywhere, it rules the world, it is its blood and fuel¹. In 2016, the United Nations General Assembly issued recommendations in the form of a resolution² that access to the Internet, which should be considered the largest source of information, should be treated on an equal footing with the right to life and as one of the basic human rights. Information is becoming an element of information warfare, a modern weapon with a global range of destruction, used to achieve an advantage over the opponent, specific strategic goals and, finally, domination in the security environment. Glynn Harmon, in

* ppłk dr inż, Bartłomiej Terebiński, War Studies University, Warsaw, Poland

 <https://orcid.org/0000-0002-6124-9905>  b.terebinski@akademia.mil.pl

Copyright (c) 2024 Bartłomiej Terebiński. This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

¹ J. Gleick, *Informacja. Bit, wszechświat, rewolucja [Information – beat, universe, revolution]*, 2012, p. 14.

² The promotion, protection and enjoyment of human rights on the Internet, Resolution adopted by the Human Rights Council on 1 July 2016. Source: <https://digitallibrary.un.org/record/845728> (accessed: 10 May 2024).

turn, assumes that information is a type of meta-energy that moves larger amounts of energy and determines the vibrancy of actions undertaken by humans³.



Figure 1. Information civilization

Source: own study based on⁴.

Each source of information has its own characteristics and is perceived individually by particular people. Information found on the Internet is characterized as trustworthy and available at any time, television information as impartial and current, and press information as balanced and reliable. The literature on the subject indicates that the most important elements in assessing the credibility of a given piece of information are: trust in the source that provides it, timeliness, logical connection of information with other facts or news, and transmission of the same information by several independent sources. In addition to credible, reliable and up-to-date information, there is also misleading, sometimes even intentionally misleading information. The amount of information may have nothing to do with its credibility, but on the contrary- it happens that many of them are false and disinformative, which reduces their value (see Fig. 2).

³ G. Harmon, *The measurement of information*, „Information Processing and Management”, 1984, vol. 1-2.

⁴ P. Dela, *Teoria walki w cyberprzestrzeni [Cyberspace warfare theory]*, 2020, pp. 40-41.

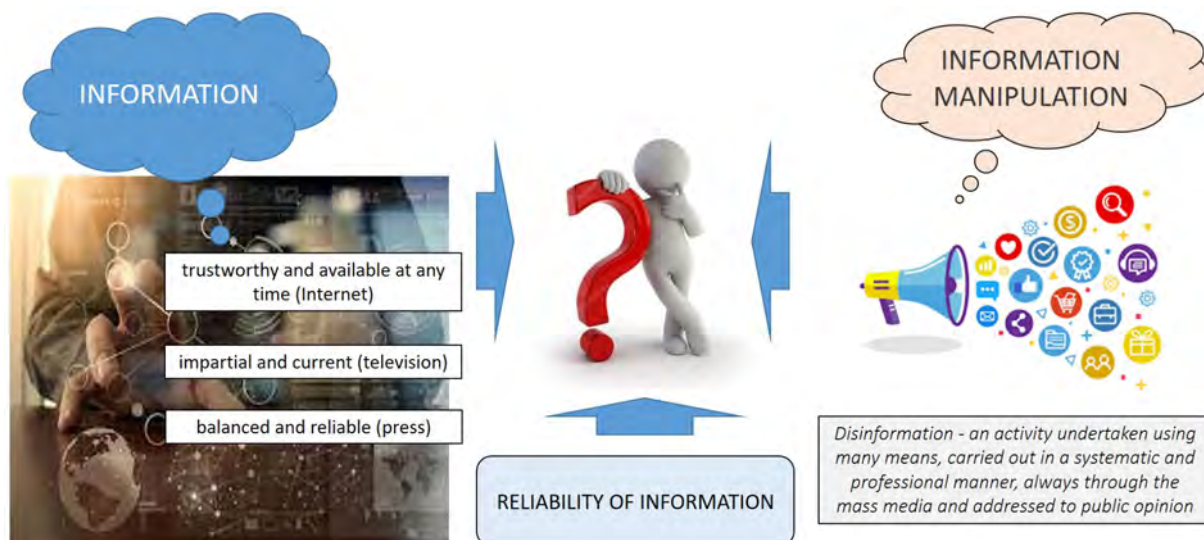


Figure 2. Features of information

Source: own study based on⁵.

What is visible here is the manipulation of information, which is expressed in its evaluation, selection, which is due to the fact that, thanks to the specificity of Web 2.0 technology, information can be posted by any participant of the virtual community. Hence, we can observe the appearance of false information. An example of this would be the fact that anonymous Wikipedia editors killed the living: Senator Ted Kennedy and politician Robert Byrd. In turn, the article about the civil war in Syria, which was published in 2012, had over 7.5 thousand views due to the dynamically changing situation in the region, edited times by Wikipedia users, which made it difficult to reliably assess the conflict. However, this is not a record, because the biography of US President George W. Bush was updated over 20 thousand times in 2005 only. Referring to the origins of building situational awareness based on publicly available sources, it should be noted that the value of open sources was noticed by George Washington already in the 18th century during the American Revolution⁶. He obtained current information about the strength of British troops and the activity of spies from press publications and publicly available news.

Apart from the history of the use of OSINT at the turn of the century, the literature on the subject cites events related to the contemporary "Arab Spring" as proof that publicly available information, views and assessments published on the Internet are powerful tools that can

⁵ K. Stankiewicz, *Wpływ Internetu na percepcję wiarygodności informacji* [The influence of the Internet on the perception of information credibility], [in:] *Spółeczeństwo informacyjne – wizja czy rzeczywistość?* [Information society. Vision or reality?], L. Haber [ed.], 2004, p. 409; K. Polańska, K., *Informacja, jej wiarygodność i co z nich dla nas wynika* [Information, its credibility and what it means for us], [in:] *Informacja – dobra lub zła nowina*, [Information – good or bad news], 2004; V. Volkoff, *Dezinformacja – oręż wojny* [Disinformation: a weapon of war], 1991, pp. 6-8.

⁶ *A Look Back... George Washington: America's First Military Intelligence Director*, <https://www.cia.gov/news-information/featured-story-archive/2007-featured-storyarchive/georgewashington.html> (accessed: 30.05.2024).

influence the fate of countries and societies⁷. To meet the challenges, analysts of the American Open Source Center⁸, described as "nosy librarians", apart from monitoring the media and press, read up to 5 million posts on social networking sites every day. They prepare reports containing descriptions of the current social mood in selected countries around the world and predict the possibility of a given threat occurring. The British Government Communications Center⁹ is also on par with its ally thanks to the Network Analysis Center, which collects over 50 billion records every day regarding Internet users' visits to news websites and online radio portals around the world, mostly related to Islam.

How, then, can a legal analysis of publicly available information be carried out, while respecting ethical and legal constraints? The aim of this study is to answer the main research problem formulated in this way.

SYSTEMATICS OF METHODS OF OBTAINING INFORMATION

Among the methods of obtaining information, five types of reconnaissance are most often mentioned (see Fig. 3): HUMINT, SIGINT, IMINT, MASINT and, finally, OSINT, which is the subject of ongoing research.

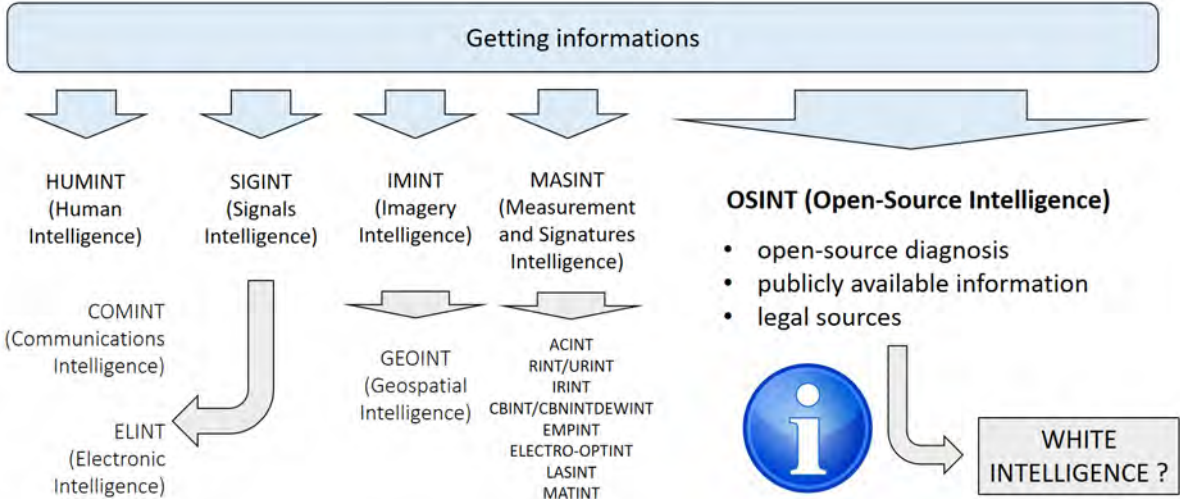


Figure 3. Getting informations
 Source: own study based on¹⁰.

⁷ K.Z. Meral, Y. Meral, *The role of social media in Arab Spring*, "e-Journal of New Media", January 2017, Vol. 5, Issue 1, pp. 26-34, https://doi.org/10.17932/IAU.EJNM.25480200.2021/ejnm_v5i1003.
⁸ *Director of National Intelligence Open Source Center*, <https://irp.fas.org/dni/osc/> (accessed: 30.05.2024).
⁹ *GCHQ Official Website*, <https://www.gchq.gov.uk/> (accessed: 30.05.2024).
¹⁰ AAP-06- NATO Glossary Of Terms And Definitions (2021), K. Matela, K., *Wybrane aspekty systemów wywiadu, obserwacji i rozpoznania (ISR) [Selected aspects of intelligence, surveillance and reconnaissance (ISR) systems]*, "Wiedza Obronna" [Defense Knowledge], 2021, Vol. 276 No. 3. pp. 238-253; M.M. Lowenthal, R.M. Clark, *The Five Disciplines of Intelligence Collection*, CQ Press, 2015; p. xi.

HUMINT deals with obtaining information from personal sources, most often through typical intelligence activities, but also through diplomatic reconnaissance or through overt contacts with people who can provide important information. While technological development makes it possible to obtain more and more information about the resources of a recognized organization or state through other intelligence techniques, HUMINT is still a source of information about planned activities. SIGINT is a general term defining radio and electronic intelligence. It includes COMINT, i.e. interception of voice, telephone and fax communications (as well as e.g. signals sent in Morse code) and ELINT, i.e. interception of information emitted using electromagnetic waves, e.g. radar signals, in order to determine the location and the operation of the analyzed infrastructure. Another way of obtaining information is IMINT, which means image recognition, based on both physical materials (such as films or photos) and electronic ones. In addition to photos and videos (PHOTOINT), it also includes, among others: radar, infrared, laser and electro-optical images. The term GEOINT refers to the analysis of geospatial information aimed at identifying and assessing terrestrial objects. MASINT, in turn, includes quantitative and qualitative analyzes of data obtained from various sources in order to determine features specific to the sources of the captured signal. Its scope includes such areas of reconnaissance as: Acoustic Intelligence (ACINT), Unintentional Radiation Intelligence - accidental revealing emission (RINT/URINT20), Infrared Intelligence (IRINT), Chemical and Biological Intelligence (CBINT/CBNINT), Directed Energy Weapons Intelligence, i.e. beam weapons (DEWINT), Nuclear Intelligence (NUCINT), Electromagnetic Pulse Intelligence (EMPINT), Electro-optical Intelligence (ELECTRO-OPTINT), including Laser Intelligence (LASINT), Materials Intelligence (MATINT21), as well as Spectroscopic Intelligence and atmospheric pollution analysis (Effluent/Debris Collection).

The subject of this study, Open-Source Intelligence (OSINT), is open-source intelligence based on publicly available information (e.g. through observation or requesting access to it), collected using legal sources, both free and available for a fee. In the literature on the subject, OSINT is also often called "white intelligence"¹¹. OSINT deals with the collection, analysis and use of data from publicly available sources to generate intelligence information. These sources may include the Internet, social media, online forums, press publications, and even leaflets or publicly available information. OSINT aims to obtain information that is publicly available without requiring penetration, hacking or invasion of privacy.

At this point it is worth explaining why OSINT is important for ensuring information protection? First, it uses a wide range of data. OSINT provides access to vast amounts of data that can be useful in identifying threats to information. This makes it possible to track various areas, including the company's reputation, competitors' activities, public opinion and the activities of criminal groups. Secondly, it uses frequently updated sources. Much of the data available within OSINT is constantly updated. Thanks to this, you can constantly monitor changes and new information, which allows you to quickly respond to potential threats. Thirdly, it is done at a relatively low cost. Most OSINT data is available for free or at low cost, making it a relatively inexpensive tool compared to other information collection methods. Fourthly, it is

¹¹ The Interagency OPSEC Support Staff, *Operations Security Intelligence Threat Handbook*, Federation of American Scientists, 1996, <https://irp.fas.org/nsa/ioss/threat96/index.html> (accessed: 10.06.2024).

done in a way that ensures legality and ethics. OSINT uses only publicly available information sources, which means it does not violate privacy or violate the law. This is important both from the point of view of ethics and legal aspects of intelligence activities. Fifth, it can be used in a variety of areas. Thanks to the diversity of information sources, OSINT can be used in all fields, from business to national security. This allows its applications to be adapted to various needs and situations. And finally, sixthly, OSINT provides decision support. Information obtained using OSINT can support the decision-making process, enabling more informed and accurate actions. This may include risk assessment, identifying market trends, or assessing the reputation of business partners. As such, OSINT is a key tool in ensuring information protection, enabling organizations to quickly respond to changing conditions and identify potential external threats.

STAGES OF ANALYZING OPEN INFORMATION SOURCES

The literature on the subject¹² distinguishes three stages of analyzing open sources of information, defined as: Open Source Data (OSD), Open Source Information (OSIF) and Validated Open Source Intelligence (OSINT-V). OSD is a stage of collecting of open source data, which is in a sort of "raw state", coming from the original source in printed or digital form, in the form of photos, recordings, satellite images, etc. OSIF is a stage of creating of open source information, broadly developed, collected into one document, edited, verified, filtered due to its presentation (e.g. press, books, publications, reports). The last stage, OSINT-V, means verified white intelligence with a high degree of credibility thanks to the analysis of information from classified sources carried out by an analyst.

It is worth emphasizing here that OSINT can be extended to include further terms. *Open Source Acquisition* is the acquisition of open source information from available open sources that have previously been collected and provided by the researcher. Open source which may be either a single person or a group providing information, while the information itself and the relationship connecting it with the entity whose interest in obtaining it is not covered by the secrecy clause. Data from open sources may be publicly available, but not all information made public is open source. The term open source refers to publicly available resources and should not be limited only to natural persons. And finally, *Publicly available information*, i.e. data, facts, instructions, materials published or transmitted for general public use, presented at the request of every citizen, obtained through observation, heard or provided at meetings open to the general public.

There are two intelligence areas within OSINT (see Fig. 4):

- 1) *Social Media Intelligence* (SOCMINT)- focused on identifying and monitoring profiles of social networking site users and the posts they publish, as well as collecting information from open and closed social groups,

¹² Tylutki, K. *Informacja masowego rażenia – OSINT w działalności wywiadowczej* [Information of mass destruction- OSINT in intelligence activities], "Przegląd Bezpieczeństwa Wewnętrznego" [Internal Security Review] 19/18, Warsaw (Poland) 2018, p. 174.

2) *Web Intelligence* (WEBINT)- data mining and searching and storing information on the Internet.

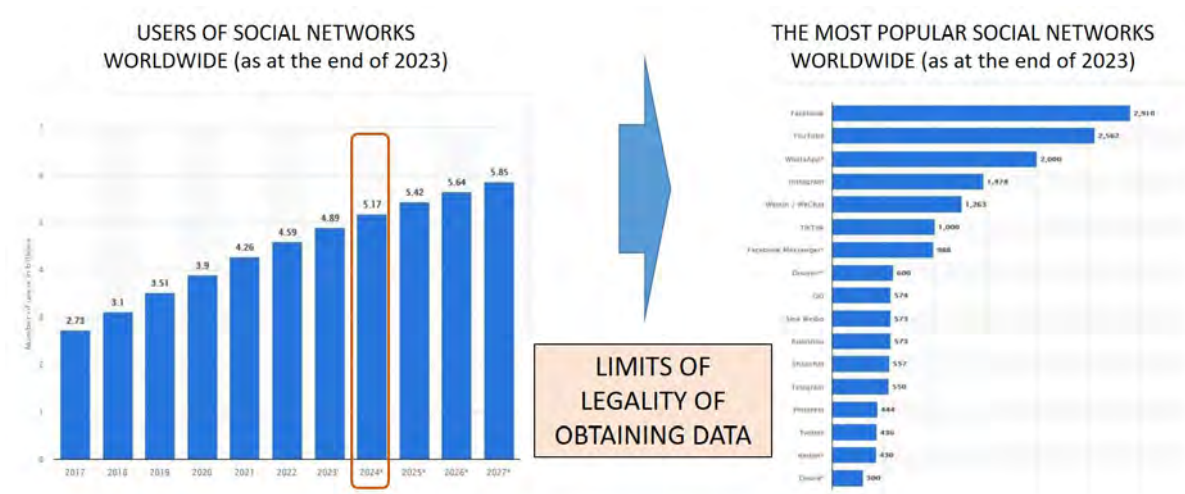


Figure. 4. SOCMINT and WEBINT- intelligence on the Internet

Source: own study based on¹³.

In 2024, the total number of people using social networking sites is estimated at 5.17 billion, and by 2027 this number is expected to increase to 5.85 billion, which will double the number of users within 10 years. The most popular social networking site, according to the ranking available at *statista.com*, is Facebook, followed by websites such as YouTube, WhatsApp, Instagram and the Chinese WeChat.

Due to the continuous development of this type of information exchange on the Internet, SOCMINT offers great opportunities to obtain current data from many corners of the world in various forms- text information, photos, videos, opinions, data about people, companies and organizations, and also enables narrowing down the search by analyzing only media on a specific topic or from a specific location. It can even be considered that SOCMINT combines OSINT, IMINT and HUMINT, because on the one hand it is based on publicly available data, and on the other it uses image data analysis techniques and obtaining information from personal sources.

Sometimes the limits of intelligence conducted in social media may go slightly beyond the limits of the legality of obtaining data (and therefore one of the basis of OSINT). When information is obtained, for example, from closed groups to which the people conducting the reconnaissance managed to gain access, although this issue may be debatable, because crossing privacy barriers does not always have to mean breaking the law. However, data obtained from social media must be verified in the same way as from any other source. Despite

¹³ Number of global social network users 2018-2027, <https://www.statista.com/statistics/278414/number-ofworldwide-social-network-users/> (accessed: 01.06.2024).

moderation (which in many places is limited to verifying whether entries do not violate the law and website regulations), information published by Internet users may be a personal point of view, unconfirmed facts or even attempted manipulation and disinformation.

THE PRACTICAL SIDE OF OSINT – PASSIVE AND ACTIVE RECONNAISSANCE

The stage of searching for information as part of open-source reconnaissance can be generally divided into two categories, depending on the level of interaction with the object (goal) of the activities in question:

- *passive reconnaissance*, which assumes no direct interaction with the object in order to hide the fact of reconnaissance from it,
- *active reconnaissance*, which allows interaction with the object, at the same time introducing the risk of detection.

It should also be noted that passive activities are subject to a much greater error due to the need to use only previously collected data about technology (e.g. from network infrastructure scans performed by services such as Shodan¹⁴ or Censys¹⁵) and people (e.g. data available in documents and public registers or originating from leaks). Collected data may not be complete, adequate to the purpose of the reconnaissance and current at the time of its implementation. For information collected passively, the level of the so-called information noise, which also adversely affects the course of subsequent analytical activities, in which it is more difficult to separate important from irrelevant information.

Active reconnaissance gives much faster and more accurate results, but carries the likelihood of revealing not only information about the fact of being analyzed. It also applies to revealing details about the person, organization or tracking infrastructure.

Conducting passive OSINT includes activities that can be performed using appropriate tools, examples of which are presented in Figure 5. The selection of specific tools was made based on their popularity on the Internet.

¹⁴ Shodan – Search Engine for the Internet of Everything, <https://www.shodan.io> (accessed: 01.06.2024).

¹⁵ Censys, <https://search.censys.io> (accessed: 01.06.2024).

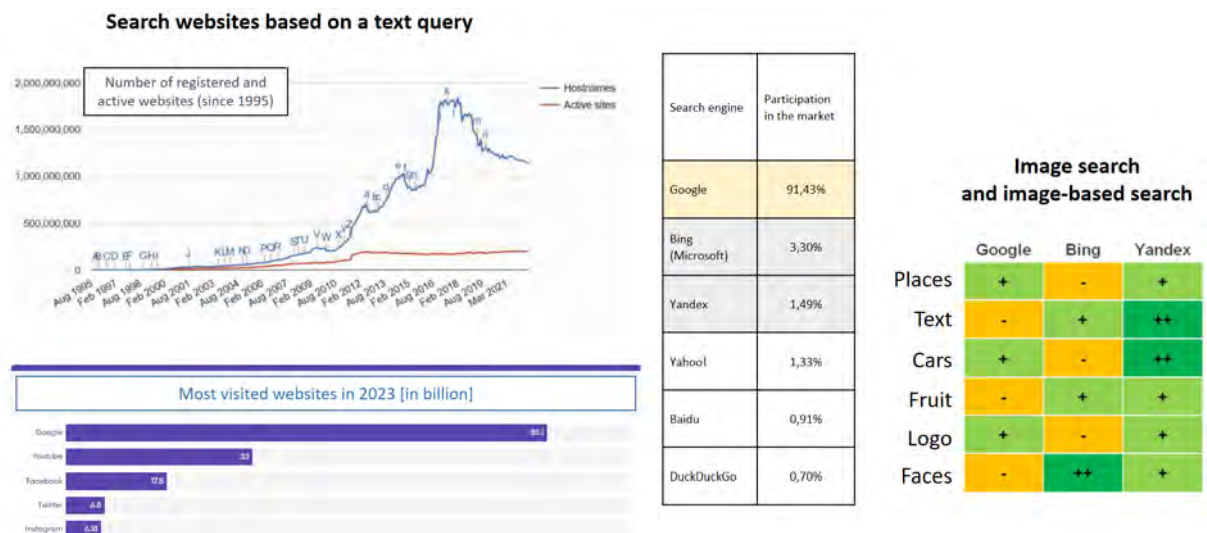


Figure 5. Passive reconnaissance – Internet search engines

Source: own study based on¹⁶.

As of December 31, 2023, there were over 1.13 billion websites, of which 82% were inactive. However, the popularity of individual search engines shows Google's huge advantage over other companies' search engines. Due to its popularity, Google is the main source of information searches in the indexed network, but due to the variety of ways of indexing information by various search engines, it is not advisable to rely solely on this search engine. There are possible cases in which information that will not be in Google databases, will be presented in other services, for example, by Microsoft's search engine called Bing (see Fig. 5). A similar situation is with image search and image-based search. Based on the research conducted, the leader in this area is not clear- here, in turn, three entities on the market are important: Google, Bing and Yandex.

Another area within passive reconnaissance is IoT (Internet of Things) searching. Reconnaissance of devices connected to the Internet, regardless of their level of technological advancement or the function they perform, is possible thanks to search engines that scan the publicly available network in search of open ports and services running on them. The presented tools have the functionality of scanning all types of devices that are available on the Internet under public IP addresses. It makes possible to find information not only about typical web servers, but also about: cameras with a web interface exposed to the Internet, computers with a shared a remote desktop or even industrial controllers that control both home installations and large systems, e.g. in power plants or sewage treatment plants. It is worth emphasizing that this type of reconnaissance is not possible using ordinary search engines (such as Google or

¹⁶ K. Haan, *Top Website Statistics For 2024*, "Forbes", <https://www.forbes.com/advisor/business/software/website-statistics/> (accessed: 02 June 2024).; K. Wosiński, *Jak wyszukiwarki radzą sobie z analizą zawartości obrazów – OSINT hints* [How Search Engines Deal with Image Content Analysis – OSINT Hints], „Sekurak”, 08 March 2021, <https://sekurak.pl/jak-wyszukiwarki-radza-sobie-z-analiza-zawartosci-obrazow-osint-hints> (accessed: 02.06.2024).

Bing), because they search for information only in the textual representation of pages, and not in their source code.

Other ways of obtaining information through passive reconnaissance are (see Fig. 6): searching for information based on a certificate, searching for information about an organization based on analyzed files, URL addresses and domains, search engines for accounts on websites, searching for profile photos (avatars).

As part of active reconnaissance, the main techniques are network scanning methods- not only the Internet, but also internal networks. These activities are intended to result in obtaining as much information as possible about a given goal. However, it should be remembered that interacting with the examined infrastructure may be considered a cyber attack, so you should always be sure about the legality of the actions performed (e.g. by signing a contract with the client for whom the vulnerability of its infrastructure is being identified, containing the exact scope of possible actions). Examples of active reconnaissance methods include:

- port/service scanning- often performed as part of security tests to discover what ports and services running on them are available to each network user; by analyzing server responses (e.g. based on response codes or text banners, it is possible to recognize details about the technology in which a given infrastructure is built)- one of the most frequently used and most versatile¹⁷,
- enumeration of subdomains- this type of reconnaissance aims to extract information from DNS servers that are responsible for changing domain names to IP addressing- it is therefore possible to obtain information both about subdomains within a given address, which can be used to expand the scope of the reconnaissance, and about ranges of IP addresses used in a given infrastructure or organization,
- SMTP enumeration- allows you to obtain information about e-mail accounts in a given organization,
- non-technical types of active reconnaissance - they involve direct interaction with people who are the subject of the investigation or are related to it- examples of the use of this type of reconnaissance include joining a group of friends on social media, joining thematic or local groups, sending messages to surveyed persons or interacting with them by reacting to their entries, as well as more hidden techniques, e.g. contact on portals such as LinkedIn as a recruiter, which usually does not arouse suspicion due to the large number of attempts at similar contacts initiated by actual recruiters.

¹⁷ *DNSDumpster.com – a FREE domain research tool*, <https://nmap.org>, dnstool.com (accessed: 02.06.2024).

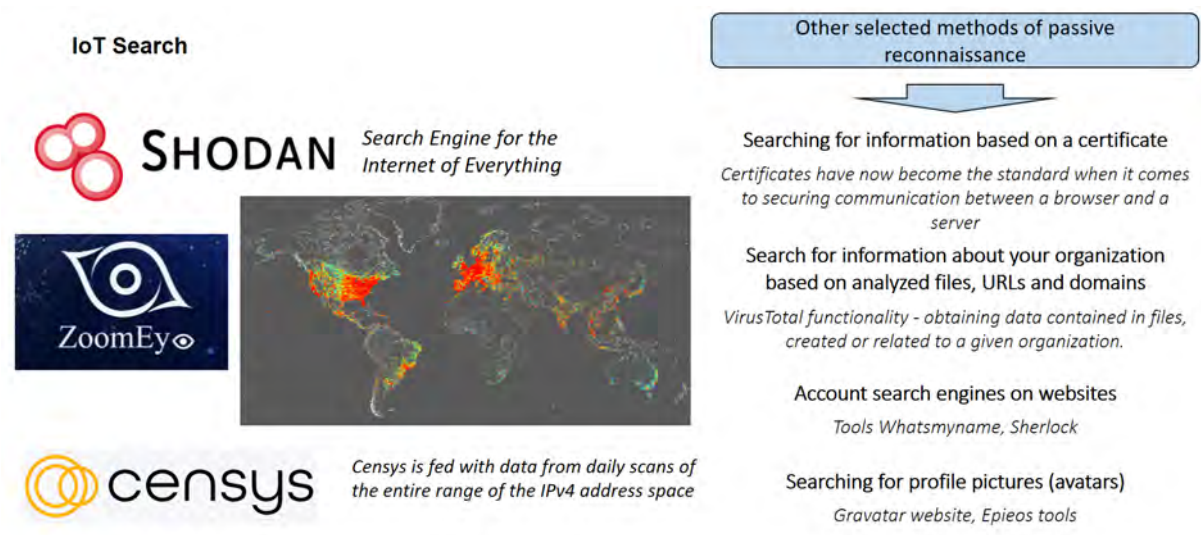


Figure 6. Passive reconnaissance- search methods

Source: own study based on¹⁸.

ETHICAL AND LEGAL RESTRICTIONS

When conducting OSINT activities, one of the key aspects is the legality of the techniques and tools used. In addition to the legality regulated by law, the ethics of the activities should also be taken into account. Lack of top-down supervision may result in the disclosure of redundant data or drawing incorrect conclusions.

Events that cause great emotions also cause a great stir among the Internet community. On the one hand has positive effects, as it gives the opportunity to persuade a large number of people to share their photos, videos and observations about a given event with law enforcement agencies and services. On the other hand, however, the desire to quickly accuse and judge those responsible, or generally speaking, to "do justice", results in skipping the stage of analysis of the collected evidence. Quickly publishing circumstantial evidence as conclusions and succumbing to the hooking effect, in turn, leads to unjust judgments. In extreme cases, such as during the first weeks of fighting in Ukraine, that thoughtless actions can lead to serious consequences (see Fig. 7).

¹⁸ Online tools consisted of: Censys, Epieos, Gravatar, Zoomeye and Github projects: Sherlock, Web Breacher and WMN screenshooter and are available at: <https://github.com/sherlock-project/sherlock>, <https://gravatar.com>, <https://epieos.com>, <https://search.censys.io/> https://github.com/swedishmike/WMN_screenshooter, <https://github.com/WebBreacher/WhatsMyName>; <https://www.zoomeye.hk/> (accessed: 02.06.2024).



Figure 7. Aspects of ethical and legal restrictions

Source: own study based on¹⁹.

Another type of ethical dilemma encountered during OSINT reconnaissance is the use of information from data leaks. This dilemma should also be considered from a legal perspective. Information that has become public through theft or accidental disclosure, mainly caused by human errors, is a very good basis for searching for information about people. But its use in official orders for which investigators receive remuneration may be considered as profiting from a crime. Therefore, you should always approach these types of sources with caution.

Open sources of information, in which you can also find top secret information, are a huge source of knowledge, as shown by the bizarre mistake of an FBI agent, who previously served as the head of the anti-terrorism department²⁰. In 2010, he decided to reserve the copyright to a manual written for agents interrogating suspects. However, he did not realize that with the entry in the register, this document would be made available to a wide range of recipients. In order to register the manual, he submitted a copy to the patent office, which is now available to anyone at the Library of Congress.

The mistake made by a secret service officer, although it seems not to have been intentional from the point of view of the rules for protecting classified information, is no different from the leak made by Edward Snowden - classified information was made available to unauthorized persons. The weakest link in ensuring information security against unauthorized leakage is not technology, but humans. An example of this would be the White House exposing its spy in

¹⁹ Retired Chicago Firefighter Wrongly Accused of Participating in Capitol Violence, <https://chicago.suntimes.com/crime/2023/12/1/23983972/retired-chicago-firefighter-joseph-pavlik-sentenced-jan-6-capitol-attack-tunnel-siege>; <https://www.aljazeera.com/news/2013/4/16/deadly-explosions-hit-boston-marathon>; <https://www.facebook.com/SecurSerUkraine/videos/3153483434931349/> (accessed: 02.06.2024).

²⁰ N. Baumann, *You'll Never Guess Where This FBI Agent Left a Secret Interrogation Manual*, "Mother Jones", 20 December 2013, <https://www.motherjones.com/politics/2013/12/fbi-copyrighted-interrogation-manual-unredacted-secrets/> (accessed: 02.06.2024).

Afghanistan²¹. Due to his function, he certainly had knowledge, the disclosure of which could have had dangerous consequences for the security of the United States and its allies. The name and function of "Chief of Stadion" appeared on a list sent to journalists in connection with Barack Obama's visit to the Bagram base in Afghanistan. This information immediately hit Twitter, where it was widely commented on.

There remains another, but fundamental legal issue related to the performance of open source reconnaissance activities based on publicly available information. The collected, public factual material as a result of the interpretation process results in the creation of new knowledge regarding a given entity. This knowledge may already be covered by legal protection - whether resulting from the acts on the protection of classified information or data regulation protection.

SUMMARY

OSINT can help identify potential threats to data and information in many different ways. There are several main ways OSINT can assist in this process. First, it supports social media monitoring. Much information about the activities, interests and intentions of individuals and organizations can be found on social media platforms. Using OSINT, you can monitor these platforms to identify potential threats, such as public statements about planned attacks, phishing attempts, and data leaks. Secondly, it enables analysis of public opinion. OSINT allows you to track public opinion about a given company, products or services. Negative comments or discussions about security breaches may indicate potential threats to data and information. Another area is monitoring competitors' activities. Analyzing the activities of competing companies can provide information about their strategies, products and development plans. OSINT can collect information about infiltration attempts, attacks or even data theft by competitors. OSINT also allows you to track press reports. The press often reports on data security incidents, information leaks and hacker attacks. OSINT allows you to track these reports, allowing you to identify trends and patterns in data threats. OSINT provides the opportunity to analyze the dark web. Some criminal activities related to data theft and cyberattacks take place on the dark web. OSINT can be used to monitor the dark web for data leaks, the sale of stolen information or planned attacks on company data. The last subject mentioned in the literature is the study of online data streams. With OSINT, you can monitor various online data sources, such as online forums, newsgroups, and websites, to identify potential data threats. For example, discussions about a security vulnerability in popular software may indicate the need to update a company's systems. In this way, OSINT plays an important role in identifying potential threats to data and information, enabling rapid response and preventive actions to protect valuable data from attacks and other undesirable events.

To summarize the considerations about OSINT and the measurable benefits derived from it, it is worth noting that thanks to technological progress and the constant development of IT

²¹ G. Miller, *White House to investigate inadvertent naming of CIA officer*, "Washington Post", 27 May 2014, http://www.washingtonpost.com/world/national-security/white-house-to-investigate-inadvertent-naming-of-cia-officer/2014/05/27/5d5f41f0-e5e6-11e3-afc6-a1dd9407abcf_story.html (accessed: 02.06.2024).

infrastructure, open sources of information, especially virtual ones, have an increasingly strong impact on the global reality. Also due to the high availability of tools and techniques indicated in this article.

Therefore, education in the field of ethics of OSINT activities remains a very important issue, because their use in an ill-considered way may expose people, companies, and military operations to negative consequence It may also result in sanctions for unauthorized disclosure of information, even if it is done it happened unintentionally.

In the case of analytical activities during reconnaissance at the level of an organization that would not ensure detailed verification of published conclusions from analyses, the result may be not only a negative impact on the results or reputation of a given organization. It may also result in unnecessary discovery of its own activities to possible persons who could be affected by such reconnaissance. The selection of appropriate criteria for drawing conclusions, as well as their thorough analysis by experienced analysts, domain experts and people with a different point of view, is therefore of great importance in performing analyses. This is even more important if human health and life depend on these decisions.

OSINT, in terms of identifying possible vulnerabilities, applies not only to infrastructure, but also to the employee sphere related to the publication of information on the Internet and other media. It is possible that the attack carried out will be a combination of two areas of reconnaissance, i.e. information about employees may be used to attempt to attack the infrastructure (e.g. using logins created on the basis of a recognized list of employees on social networking sites). Or vice versa- the information obtained about the infrastructure will be used in attacks on employees (e.g. by trying to obtain login details to a specific platform using a social engineering attack carried out via a telephone call).

REFERENCES LIST

LITERATURE

- Baumann, N. *You'll Never Guess Where This FBI Agent Left a Secret Interrogation Manual*, "Mother Jones", 20 December 2013, <https://www.motherjones.com/politics/2013/12/fbi-copyrighted-interrogation-manual-unredacted-secrets/>
- Dela, P., *Teoria walki w cyberprzestrzeni [Cyberspace warfare theory]*, War Studies University, Warsaw (Poland) 2020
- Director of National Intelligence Open Source Center*, <https://irp.fas.org/dni/osc/>
- GCHQ Official Website*, <https://www.gchq.gov.uk/>
- Gleick, J., *Informacja. Bit, wszechświat, rewolucja [Information – beat, universe, revolution]*, Dom Wydawniczy Znak, Cracow (Poland) 2012
- Haan K., *Top Website Statistics For 2024*, "Forbes", <https://www.forbes.com/advisor/business/software/website-statistics/> [Accessed: 02 June 2024]
- Harmon, G., *The measurement of information*, „Information Processing and Management” 1984, vol. 1-2.

- A Look Back... *George Washington: America's First Military Intelligence Director*, CIA Official Website, <https://www.cia.gov/news-information/featured-story-archive/2007-featured-storyarchive/georgewashington.html>
- July 2022 Web Survey, "Netcraft", <https://news.netcraft.com/archives/2022/07/28/july-2022-web-serversurvey.html>
- Lowenthal, M. M., Clark, R. M., *The Five Disciplines of Intelligence Collection*, CQ Press, 2015.
- Matela, K., *Wybrane aspekty systemów wywiadu, obserwacji i rozpoznania (ISR) [Selected aspects of intelligence, surveillance and reconnaissance (ISR) systems]*, "Wiedza Obronna" [Defense Knowledge], 2021, Vol. 276 No. 3.
- Meral K.Z., Meral Y., *The Role of Social Media in Arab Spring*, "e-Journal of New Media", January 2017, Vol. 5, Issue 1, https://doi.org/10.17932/IAU.EJNM.25480200.2021/ejnm_v5i1003
- Miller G., *White House to investigate inadvertent naming of CIA officer*, "Washington Post", 27 May 2014, http://www.washingtonpost.com/world/national-security/white-house-to-investigate-inadvertent-naming-of-cia-officer/2014/05/27/5d5f41f0-e5e6-11e3-afc6-a1dd9407abcf_story.html
- Number of social media users worldwide from 2017 to 2028*, "Statista", <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/>
- Operations Security Intelligence Threat Handbook*, Published by The Interagency OPSEC Support Staff, April 1996, Revised May 1996 <https://irp.fas.org/nsa/iOSS/threat96/index.html>
- Polańska, K., *Informacja, jej wiarygodność i co z nich dla nas wynika [Information, its credibility and what it means for us]*, [in:] Szewczyk A. (ed.), *Informacja – dobra lub zła nowina [Information – good or bad news]*, Uniwersytet Szczeciński, Szczecin (Poland) 2004.
- Stankiewicz, K., *Wpływ Internetu na percepcję wiarygodności informacji [The influence of the Internet on the perception of information credibility]*, [in:] Haber L., *Spółczesność informacyjna – wizja czy rzeczywistość? [Information society. Vision or reality?]*, Cracow (Poland) 2004.
- The Interagency OPSEC Support Staff, *Operations Security Intelligence Threat Handbook*, Federation of American Scientists, 1996.
- Tylutki, K., *Informacja masowego rażenia – OSINT w działalności wywiadowczej [Information of mass destruction - OSINT in intelligence activities]*, "Przegląd Bezpieczeństwa Wewnętrznego" [Internal Security Review] 19/18, Warsaw (Poland) 2018.
- Volkoff, V., *Dezinformacja – oręż wojny [Disinformation: a weapon of war]*, Dom Wydawniczy Delikon, Warsaw (Poland) 1991.
- Wosiński K., *Jak wyszukiwarki radzą sobie z analizą zawartości obrazów – OSINT hints [How Search Engines Deal with Image Content Analysis – OSINT Hints]*, „Sekurak”, 08 March 2021, <https://sekurak.pl/jak-wyszukiwarki-radza-sobie-z-analiza-zawartosci-obrazow-osint-hints>.

SOURCES

AAP-06 (2021) - NATO Glossary of Terms And Definitions.

Censys, <https://search.censys.io/>.

DNSDumpster.com – a FREE domain research tool, <https://nmap.org/dnsdumpster.com>

EPIEOS – The ultimate OSINT tool for email and phone reverse lookup, <https://epieos.com>.

Gravatar, <https://gravatar.com>.

Project Sherlock at Github, <https://github.com/sherlock-project/sherlock>.

Shodan – Search Engine for the Internet of Everything, <https://www.shodan.io/>.

The promotion, protection and enjoyment of human rights on the Internet, Resolution adopted by the Human Rights Council on 1 July 2016. Source: <https://digitallibrary.un.org/record/845728>

Web Breacher at Github, <https://github.com/WebBreacher/WhatsMyName>

WMN_screenshooter at Github, https://github.com/swedishmike/WMN_screenshooter

ZoomEye– advanced cyberspace search engine, <https://www.zoomeye.hk/>



Copyright (c) 2024 Bartłomiej Terebiński.



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.