Tomasz Goryca, PhD
Military Technical University
e-mail: tomasz.goryca@wat.edu.pl
ORCID: 0000-0002-1671-7386

DOI: 10.26410/SF_1/23/6

THE USE OF OPEN SOURCES OF INFORMATION IN THE ACTIVITIES OF THE FORMATIONS RESPONSIBLE FOR PROTECTION OF THE EXECUTIVE BODIES OF THE STATE

Abstract

The aim of this study is to present issues related to the possibilities of using so-called open-source information by security formations to ensure the security of facilities and persons subject to special protection. Acquisition of as much information as possible that can have an impact on increasing the security level of the executive administrative bodies of each state has become one of the key tasks for the formations responsible for their protection and security. Units set up to protect key people in the state must not only be properly trained and equipped, but also prepared for the systematically changing information technologies as well as digital development. The main aim of conducted analyses from public sources is to obtain information about potential threats to people and facilities of strategic importance for the functioning of the state (organization) and, in the long run, to plan preventive measures related to the implementation of protective actions. The aim of the paper is to present science-based benefits of using open sources of information in the functioning of protective formations, which can become a starting point for further analysis, decisions, or research. Theoretical research methods were used in the preparation of this paper. The considerations presented indicate that the ability to obtain information from open sources by institutions responsible for the security of the executive bodies of the state requires scientific research, the conclusions of which can have an impact on reducing the risk level and increasing the security level of people and facilities of strategic importance for the state security.

Key words

security, threats, information, open-source intelligence, protection

Introduction

Planning, organizing[1] and commanding[2] protective activities related to the acquisition of information from open sources of information is an extremely important issue from the point of view of institutions the main task of which is to ensure the broadly understood security of people and facilities of key importance for the state functioning[3].

It is not without reason that it is considered that the one who has the power has the knowledge, or in more narrow reasoning – information. Acquisition, collection, processing, and use of various types of information determine, among others, the directions and elements of modern information warfare and is also used to achieve an advantage over the enemy. Acquisition, monitoring, and analysis of information from unclassified sources by protective formations to ensure the safety and security of persons and facilities subject to special protection is one of the basic tasks and depending on the evaluation of potential risks or threats, different variants of planned protective undertakings are developed.

The effectiveness and efficiency of the protective formation in any country is implied by many factors. One such factor is the ability to acquire, process, analyze and use information from public sources, which can lead, among others, to the prevention of life- and/or health-threatening situations or the avoidance of threats[4]. The analysis effectiveness of the collected and processed information is influenced by the regularity of its searching and updating. The leading factor in the analysis process is primarily the acquisition, transmission, and exchange rate of collected and processed information. The study of the relationship between threat identification, risk evaluation and the safety of protected persons and facilities are of great interest in the context of issues related to the use of open-source information by protective formations.

Lack of information on a potential threat or improper use of information held can lead to errors in the implemented protective activities, and consequently to the exposure of protected person to loss of health or/and life.

The issue of obtaining and using information was appreciated in ancient times by one of the greatest thinkers of the Far East, the author of "The Art of War" – Sun Tzu. In a chapter entitled "Intelligence," he described the importance of acquiring information about the enemy and using it properly[5].

The unlimited volume and variety of open sources of information is the greatest advantage in the process of acquiring information alone. This "richness" can

[1] T. Goryca, *Risk and threats in protective measures of the units responsible for security of executive states bodies*, "Security Forum" 2022, 6 (1), p. 138.

[2] B. More, T. Wiśniewski, Zwęgliński, R. Socha, *The Theory of Commanding*, "Вісник Львівського Державного Університету Безпеки Житттєдіяльності" 2016, No 14/2016, p. 47-52.

[3] T. Goryca, *Theory and practical aspects of state authorities protection organization*, "Security Forum" 2021, 5(2), p. 53.

[4] T. Goryca, *Identyfikacja i ocena zagrożeń dla bezpieczeństwa VIP*, [in:] *Różnorakie perspektywy bezpieczeństwa*, ed. M. Banasik, Warszawa 2019, p. 73.

[5] S. Tzu, S. Pin, *Sztuka Wojny,* 3rd edition, translation: K. Bakalarz, Gliwice 2013, p. 99-105.

also pose a major problem in the process of analyzing the collected information. Proper selection of reliable information unfortunately takes a lot of time and requires specialized skills.

It should not be forgotten that the same tools are used by criminal or terrorist groups, which follow the social media of important personalities and analyze their plans for daily life, meetings with voters, domestic or foreign travel.

The security of policymakers or diplomatic and consular employees under protection is correlated with the knowledge that analysts of protective formations will gain, as terrorist organizations or criminal groups constantly intensify their propaganda activities, while intensifying the amount of information disseminated and its availability[6].

Methodology

The main problem, the solution of which is presented in this paper is expressed in the form of a question: how to use open sources of information effectively and efficiently in the protective activities of the formations responsible for security of the governing bodies of the state?

Theoretical research methods were used in the research process, which include: analysis (allowed to distinguish individual components, special features of the subject under study), synthesis (thanks to synthesis, relationships between individual elements of the subject under study were established), defining (helped to clarify definitions related to the subject under study) and inference (helped to derive new conclusions on the subject under study)[7].

The available literature on the research subject was analyzed[8], in particular, Polish, and foreign-language monographs, printed scientific papers and Internet sources, as well as specialized textbooks, manuals and guidelines, and applicable laws.

Characteristics of "open-source intelligence"

The possibilities offered by the so-called "open-source intelligence", i.e., "a body of publicly available, open information that anyone can legally obtain" has already been appreciated by humanity since the advent of primary communication[9]. While the method was and is widely known and used by various institutions around the world, the very concept of "open-source intelligence" is a Polish idea. Outside the Republic of Poland (and especially in the West), the American acronym OSINT (Open Source Intelligence). It is worth noting that this acronym is much younger than the Polish concept of "open-source intelligence.[10]" Most researchers equate "open-source intelligence" with OSINT

[6] More: K. Liedel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej*, Warszawa 2011, p. 9-15.

[7] More,: *Bezpieczeństwo. Teoria-Badania-Praktyka*, A. Czupryński, B. Wiśniewski, J. Zboina (Ed.), Józefów 2015, p. 32.

[8] More: *Nauki o bezpieczeństwie. Wybrane problemy badań*, A. Czupryński, B. Wiśniewski, J. Zboina (Ed.), Józefów 2017.

[9] K. Tylutki, *Informacja masowego rażenia – OSINT w działalności wywiadowczej*, „Homeland Security Review" 2018, No. 10 (19), p. 174.

[10] B. Saramak, *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*, Warszawa 2015, p. 15.

in the broadest sense. This type of intelligence is also referred to as agentless, public, open, passive intelligence or open source monitoring[11], or as literary intelligence (LITINT)[12].

In the Polish subject literature, "open-source intelligence" is defined as: "conducting intelligence activities on the basis of publicly available, open sources, such as analysis of media coverage, journalism. Sometimes the term is used to describe the collection of information in a legal manner, in accordance with the Vienna Convention on Diplomatic Relations. British journalists sometimes refer to such activities as soft intelligence.[13]" Most researchers emphasize that this type of intelligence work "unlike other methods of obtaining and analyzing information by state agencies, is not covert, secret, illegal in nature. On the contrary, it makes use of publicly available, open sources of information, and no operational activities are used.[14]"

B. Sienkiewicz points out that the main purpose of the organizational units in uniformed formations responsible for "open-source intelligence" is "to deal with the legal acquisition of information from the public space and process it in a way that gives the operational divisions the ability to respond in situations that require it.[15]"

Another point of view is presented by the following definition: "open-source intelligence" is the result of carrying out certain activities in relation to information. They are specifically searched for, compared with each other as to content, and the most important ones for the recipients of the processes are selected[16].

A large contribution to the development of obtaining information from open sources was made by the US special services. The counterpart of the Polish "open-source intelligence" is defined, among others, as a planned search, selection, inference, and distribution of information directed to a specific recipient group (e.g., staff, decision-makers, or protective formations), according to a previously reported, demand. It is worth noting that the methodology for dealing with acquired data and information from open sources is developed by each institution (including protective formations) on its own. The result of such publications are analytical studies, which contain specific conclusions or guidelines[17].

In conclusion, it can be pointed out that "open-source intelligence" consists of planned (thematically) acquisition of information from open sources, their selection, collation, digitization, translation and transcription, analysis, and inference based on them, as well as

[11] J. Larecki, *Wielki leksykon służb specjalnych świata: organizacje wywiadu, kontrwywiadu i policji politycznych świata, terminologia profesjonalna i żargon operacyjny*, Warszawa 2007, p. 749-750.

[12] R. Omilianowicz, *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej*, [in:] *Wywiad i kontrwywiad w świecie*, W. Wróblewski (Ed.), Szczecin 2009, p. 146.

[13] M. Minkina, *Gry wywiadów. Sztuka wywiadu w państwie współczesnym*, Warszawa 2014, p. 41.

[14] *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, W. Filipkowski, W. Mądrzejowski (Ed.), Warszawa 2012, p. 14.

[15] B. Sienkiewicz, *Historia pewnego złudzenia*, „Przegląd Bezpieczeństwa Wewnętrznego" 2021, p. 52.

[16] G. Dobrowolski, W. Filipkowski, M. Kisiel-Dorohnicki, W. Rakoczy, *Wsparcie informatyczne dla analizy otwartych źródeł informacji w Internecie w walce z terroryzmem. Zarys problemu*, [in:] *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu*, L. K. Paprzycki, Z. Rau (Ed.), Warszawa 2009, p. 279.

[17] *NATO Open Source Intelligence Handbook*, Norfolk November 2001, p. 2.

collection and distribution to a predetermined audience[18]. The main purpose of analytical cells in protective formations responsible for monitoring open sources is to provide information or data used in the course of implementing protective actions and predicting potential threats and/or forecasting developments with respect to persons and facilities subject to mandatory protection.

Selected open sources of information

In the subject literature, open sources are usually defined as any publicly available information that can be used for intelligence purposes. The collection of information from open sources operates at all levels of intelligence activities (civilian, military, private). Such sources of information can be used for early warning and situational, strategic, tactical, or operational awareness[19].

The basic division of open sources of information is based on two groups: primary sources and secondary sources. Primary sources contain a description of observations, insights or investigations, and the secondary sources collect, process and present information that is derived from primary sources[20].

There are many divisions and classifications in the subject literature that indicate the large number of open sources of information. Below only those that may be useful in the work of security formations are presented.

1. Traditional media:
   - printed press (e.g., daily newspapers, trade journals, government documents),
   - news television, radio stations,
   - literature (books, journalism, analysis, journalistic investigations).
2. Internet:
   - online editions of newspapers and magazines,
   - blogs, microblogs,
   - social networks,
   - wikis (Wikipedia, Wikileaks),
   - video services (e.g., YouTube),
   - photo services,
   - business websites,
   - maps, satellite images, aerial photos.
3. Commercial services:
   - business entities that prepare profiled reports and analyses for a fee,
   - marketing publications.
4. Niche literature – analysis, information available only through specialized channels, generated by academia, state organizations and NGOs.
5. Databases and directories21.

It seems impossible to mention all the open sources of information through which security formations can obtain information important to them. This is, of course, due to the dynamic development of digital technologies and information technology.

[18] K. Liedel, T. Serafin, *Otwarte źródła informacji…*, p. 54-55.

[19] A. Ziolkowska, *Open source intelligence (OSINT) as an element of military recon*, "Security Defence Quartely" 2018, vol. 19(2), p. 75.

[20] B. Saramak, *Wykorzystanie otwartych źródeł informacji…*, p. 63.

[21] B. Stromczyński, P. Waszkiewicz, *Biały wywiad w praktyce organów ścigania na przykładzie wykorzystania serwisów społecznościowych*, „Prosecutor's Office and Law" 2014, nr 5, p. 150.

Metadata is also worth mentioning at this point. This is data about data, i.e., detailed information describing information resources. The ability of security formation analysts to extract metadata can provide a lot of information, e.g., about a person's residence, interests, habits, etc. The simplest example is the data that can be obtained from a photo that has not been cleared of metadata (e.g., information on the date and place it was taken)[22].

Despite some limitations, the use of open sources of information in the activities of security formations creates extremely valuable information potential. Taking into account the understood analytical skills combined with digital and technological competence, it is possible to safely conclude that this type of activity plays a key role in the implemented protection tasks against the state's governing bodies and the facilities serving them.

The use of "open-source intelligence" in the protection activities of the state's governing bodies

The planning and organizational processes of protective actions are aimed at developing the optimal way to implement protective tactics and thwart a potential attack in its initial phase[23], taking into account not only the experience, but above all the awareness of possible actions. The level of this awareness and the effectiveness of protective actions depends on proper planning procedures based primarily on collection, gathering and analysis of the information at hand[24]. The basis for the effectiveness of protective actions is reliable and up-to-date information resources about a person or a particular facility.

It is worth noting that for many years there have been developed analytical programs useful for monitoring open sources of information, which were created for services and institutions responsible for security[25]. Such software allows combining, among others, linkage analysis, geographic analysis, monitoring, various databases, reports, and documents. The developers' idea behind such software was primarily to identify and alert users early on to new threats, suspicious persons, and other anomalies[26].

One of the key challenges for the security policy of any country is access to information[27], and an element of the functioning of any security formation is the collection, gathering, analysis, storage, and use of information.

The use of open sources of information in security operations around the

[22] M. Tomaszewska-Michalak, *Prawne aspekty pozyskiwania informacji w Internecie*, „Studia Politologiczne" 2019, vol. 54, p. 128.

[23] J. Kaczyński, *Taktyka działań ochronnych,* Gdańsk 2009, p. 33.

[24] T. Goryca, *Planning of VIP protection in the aspect of the continuity of the State Protection Service operation*, [in:] *Dimensions of regional and global security,* M. Górnikiewicz, I. Mucha (Ed.), Toruń 2019, p. 106.

[25] T. Serafin, *Automatyzacja procesu wywiadu jawnoźródłowego w ramach działalności wywiadowczej i walki z terroryzmem*, [in:] *Analiza informacji w zarządzaniu bezpieczeństwem*, K. Liedel, P. Piasecka, T.R. Aleksadrowicz (Ed.), Warszawa 2013, p. 83.

[26] B. Saramak, *Wykorzystanie otwartych źródeł informacji…*, p. 38.

[27] M. Górka, *Otwarte źródła informacji – nowa czy klasyczna formuła wywiadu*, [in:] *Służby wywiadowcze jako element polskiej polityki bezpieczeństwa. Historia i współczesność*, M. Górka (Ed.), Toruń 2016, p. 19.

world is an integral part of the tasks of formations and institutions established for this purpose. Nowadays, the effective use of open sources of information has become more important than ever before. The number, but also the variety of open sources of information that a security formation analyst may encounter in his work – ranging from the Internet, television, radio, press and electronic documents – is enormous. In conclusion, the more information that has been acquired – the more knowledge and effort is needed to interpret this information[28].

The essence of "open-source intelligence" is based on the fact that the information acquired by analysts of security formations is not a secret in the sense of the law and is not covered by any confidentiality clause. From the point of view of the protection activities carried out by the formations established for this purpose, "open-source intelligence" has one advantage that cannot be overestimated: the risk that information collection and analysis will be detected is very negligible[29].

In the era of information technology and information development, the main challenge is no longer the mere acquisition of information by security formations or other institutions, but the identification of relevant information and relating it to predetermined knowledge[30].

The enormity of available information that appears every day and may be relevant to persons and facilities subject to special protection determines analysts of security formations to evaluate its reliability. M. Grabowski and A. Zając distinguish the following criteria that should be met for information to be considered reliable[31]:

- efficiency – finding information that is relevant, useful, and providing it on time in a correct and consistent form,
- confidentiality – information should be protected from unwarranted disclosure and use,
- productivity – information should be provided using available resources in an optimal (economical) manner,
- availability – information is available for a specific process, taking into account the time aspect (concerning the present and the future). Information resources should also be protected.
- integrity – refers to the completeness and accuracy of information and its correctness in relation to expectations,
- reliability – the purpose is to ensure that the recipient's information is appropriate for its correct use,
- compliance – must take into account the requirements imposed on the organization by external entities, laws, regulations, contracts, as well as specific requirements and internal policies of the organization.

Evaluation of the criteria met above provide a rationale for analysts responsible for the security of key people and facilities in the country to assess the value of the information being acquired and

[28] J.C. Gannon, *Strategic use of open source information: A corporate strategy that leverages the best practices*, "Vital Speeches of the Day" 2000, vol. 67/5, p. 153-157.

[29] T. Pączkowski, *Biały wywiad*, Katowice 2020, p. 6.

[30] M. Górka, *Wybrane działania polityki bezpieczeństwa w zakresie informacji wywiadowczych na początku XXI wieku,* „Świat Idei i Polityki" 2019, vol. 18, p. 138.

[31] M. Grabowski, A. Zając, *Dane, informacja, wiedza – próba definicji*, "Scientific Journals" 2009, No. 798, p. 99-116.

processed. Particular attention is paid to the reliability of the acquired information, due to the possibility of fabrication or falsification of information.

Summary

Planning of protective actions against persons and facilities of strategic importance for the state functioning should always be preceded by the analysis and preparation of appropriate scenarios for the implementation of protective actions, as a response to the risk evaluation with regard to the occurrence of particular types of threats[32]. Skillful acquisition and analysis of information from open-source materials becomes one of the priority tasks for security formations around the world. The prerequisite for effective use of the collected information is the ability to process it and draw the right conclusions.

The main advantages of open sources of information include the possibility of obtaining information very quickly, its quantity, diversity, quality, as well as easiness and low cost of its analysis. The risk of detection by counterintelligence services of foreign countries or terrorist groups is negligible.

The problem that arises in the implemented protective tasks related to the acquisition of information from public sources by protective formations is the lack of an adequate number of specialists who have language training and education (e.g., lack of knowledge of Chinese, Japanese, Arabic, Hindi, Pashto, etc.). Very often individuals subject to mandatory protection travel to different parts of the world, and then the effectiveness and efficiency of information acquisition by protection formations is very limited.

Disinformation is another obstacle that is very often encountered by analysts of services responsible for the security and protection of government executives. The Internet, television, press and especially social networks very often manipulate media coverage by deliberately misleading the audience. This means that an expert analyzing the available materials must have a great deal of knowledge, experience, and a great distance from the sources under investigation[33].

The considerations carried out allow to conclude that analysts of protective formations who acquire data from open sources make a large contribution at each stage of planning protective actions with respect to persons and facilities of strategic importance for the state functioning. The processes of collecting, analyzing, and processing the acquired data provide real support for those carrying out tasks related to the direct protection of key personalities, and are also a guarantee of the effectiveness and efficiency of protection activities carried out.

It seems reasonable to conclude that a very important premise for the evaluation of effectiveness with respect to the implemented protective actions at the stage of acquiring information from

[32] T. Goryca, *Planning of VIP protection…*, p. 125.

[33] K. Jarczewska-Walendziak, *Wykorzystywanie otwartych źródeł informacji przez służby śledcze,* Toruńskie „Studia Bibliologiczne" 2017, no. 1 (18), p. 144-145.

open sources is the protection level of such resources, collected, analyzed, and processed by protective formations.

To sum up the considerations on the use of open sources of information by protective formations to ensure the security of the executive bodies of the state, it is worth noting that technological progress and the systematic development of information infrastructure strongly determines the development of "open-source intelligence" tools and techniques. In this regard, it is highly desirable for various types of protective formations to cooperate and collaborate with other institutions responsible for security and using the possibilities of acquiring, processing, and analyzing open-source information.

Bibliography

Bezpieczeństwo. Teoria–Badania–Praktyka, Czupryński A., Wiśniewski B., Zboina J. (ed.), Józefów 2017.

Mądrzejowski W., *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, Filipkowski W. (Ed.), Warszawa 2012.

Dobrowolski G., Filipkowski W., Kisiel-Dorohnicki M., Rakoczy W., *Wsparcie informatyczne dla analizy otwartych źródeł informacji w Internecie w walce z terroryzmem. Zarys problemu*, [in:] *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu,* Paprzycki L., Rau Z. (Ed.), Warszawa 2009.

Gannon J.C., *Strategic use of open source information: A corporate strategy that leverages the best practices*, "Vital Speeches of the Day" 2000, vol. 67/5.

Górka M., *Otwarte źródła informacji – nowa czy klasyczna formuła wywiadu*, [in:] *Służby wywiadowcze jako element polskiej polityki bezpieczeństwa. Historia i współczesność*, M. Górka (Ed.), Toruń 2016.

Górka M., *Wybrane działania polityki bezpieczeństwa w zakresie informacji wywiadowczych na początku XXI wieku*, „Świat Idei i Polityki" 2019, vol. 18.

Goryca T., *Identyfikacja i ocena zagrożeń dla bezpieczeństwa VIP*, [in:] *Różnorakie perspektywy bezpieczeństwa*, M. Banasik, A. Rogozińska (Ed.), Warszawa 2019.

Goryca T., *Planning of VIP protection in the aspect of the continuity of the State Protection Service operation*, [in:] *Dimensions of regional and global security,* M. Górnikiewicz, I. Mucha (Ed.), Toruń 2019.

Goryca T., *Risk and threats in protective measures of the units responsible for security of executive states bodies*, "Security Forum" 2022, 6 (1).

Goryca T., *Theory and practical aspects of state authorities protection organization*, "Security Forum" 2021, 5(2).

Grabowski M., Zając A., *Dane, informacja, wiedza – próba definicji*, "Scientific Journals" 2009, No. 798.

Jarczewska-Walendziak K., *Wykorzystywanie otwartych źródeł informacji przez służby śledcze,* „Toruńskie Studia Bibliologiczne" 2017, no. 1 (18).

Kaczyński J., *Taktyka działań ochronnych*, Gdańsk 2009.

Larecki J., *Wielki leksykon służb specjalnych świata: organizacje wywiadu, kontrwywiadu i policji politycznych świata, terminologia profesjonalna i żargon operacyjny,* Warszawa 2007.

Liedel K., Serafin T., *Otwarte źródła informacji w działalności wywiadowczej*, Warszawa 2011.

Minkina M., *Gry wywiadów. Sztuka wywiadu w państwie współczesnym,* Warszawa 2014.

NATO Open Source Intelligence Handbook, Norfolk November 2001.

Nauki o bezpieczeństwie. Wybrane problemy badań, Czupryński A., Wiśniewski B., Zboina J. (Ed.), Józefów 2017.

Omilianowicz R., *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej*, [in:] *Wywiad i kontrwywiad w świecie*, W. Wróblewski (Ed.), Szczecin 2009.

Pączkowski T., *Biały wywiad*, Katowice 2020.

Saramak B., *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy,* Warszawa 2015.

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

Sienkiewicz B., *Historia pewnego złudzenia*, „Przegląd Bezpieczeństwa Wewnętrznego" 2021, April 6.

Tylutki K., *Informacja masowego rażenia – OSINT w działalności wywiadowczej*, „Homeland Security Review" 2018, No. 10 (19).

Tzu S., Pin S., Sztuka *Wojny*, *3rd edition*, Gliwice 2013.

Wiśniewski B., Zwęgliński T., Socha R., *The Theory of Commanding*, "Вісник Львівського Державного Університету Безпеки Житттєдіяльності" 2016, No 14/2016.

Zarządzanie kryzysowe. Teoria, praktyka, konteksty, badania, eds. J. Stawnicka, B. Wiśniewski, R. Socha, WSPol., Szczytno 2011.

Ziółkowska A., *Open source intelligence (OSINT) as an element of military recon*, "Security Defence Quartely" 2018, vol. 19(2).

About Author

Tomasz Goryca, doctor of social sciences. In his scientific work he deals with national security problems, system improvement safety and protection of persons performing managerial functions in the state.