OPEN SOURCE INTELLIGENCE (OSINT) AS AN ELEMENT OF MILITARY RECON

Agata ZIÓŁKOWSKA, MSc
info@aziolkowska.pl
Faculty of National Security
War Studies University, Warsaw, Poland

Abstract

One of the most basic functions of the state is to ensure the security to it and its citizens. Significant elements are: perseverance, political independence, territorial integrity and maintenance proper level of life quality. Today's intelligence, which is part of the structures of security organs, belongs to the elite part of the special forces performing strategic goals. Therefore, acquiring the information by OSINT is important not only for the institution itself but also for citizens. OSINT is one of the means by which security is provided to the internal and external states. Open source information is one of the agents of economic, political, military, etc. Books, periodicals, statistical yearbooks, social networking sites and daily newspapers belong to the basic, verified sources. In globalized world, OSINT has particular importance because, due to the obtained information, the state can take defensive action. In this article, the author pointed out the use of OSINT in the military diagnosis.

Keywords: Open Source Intelligence, Military Recon, government, special services

> "That, what we call an intelligence, is simply a disguised way of organising information about the surroundings by specialised institutions created for that purpose by the state."
>
> P. Wroński
> [*Czas nielegałów*, 2016]

Introduction

Due to the importance of the security of the country, each state owns and maintains designated intelligence services to collect and analyse information. All actions are secret and support the decisions of the state authorities. For security reasons, the ways in which actions, structures and effects are carried out limited in their public availability. In the 21st century, the Information Society is increasingly deepening its knowledge in the field of intelligence, with the consequence of breaking the limits and consciousness about the activities of the state, including special services. Computerisation and technological development changes the state's security considerations and the evolution of security instruments (i.e., *responsible entities for identifying threats and counteracting them*). Intelligence is carried out by functional, operational and informational divisions, which perform a specific role at various stages of the information cycle, including military reconnaissance. Military identification, despite its specificity and character, is coincident with strategic intelligence, where the difference between them can be seen in the names and extended methods of collection and analysis of the information. As a secret tool for information gathering, it uses open source intelligence (OSINT), which does not disclose to the entity performing the verification and verification activities. OSINT is currently called an extra-informal form of collecting information i.e. on a military theme. In the past, during the Cold War, the importance of basic sources of information, such as books, magazines and the daily press, according to British intelligence, emphasised that "studying Soviet and daily newspapers and technical journals is very valuable as a source of intelligence and should be used at every opportunity" (Więckiewicz 1974, p. 18). With the evolution and development of technology, the Internet is currently the primary source of OSINT (especially appreciated by the Federal Security Service of the Russian Federation -FSB).

Indication of the subject and purpose of the analysis of the available literature led to identification of the research problem in the form of a question: Does the use of Open Source Intelligence belong to the tools used for military reconnaissance?

The English-language nomenclature popularised the concept of Open Source Intelligence (OSINT), which includes two structured ways of acquiring and then analysing information. In this article, the open source formulation is identical to the terms "White Intelligence" and "Open Source Intelligence - OSINT". The first formulation is used by government agencies responsible for state security, while the second is also in the private sector. In this article, the author discusses and pays special attention to the definitions of intelligence, successively referring to OSINT as a form of military intelligence, because the inseparable association of intelligence with secrecy is one of the fundamental elements that distinguishes it from freedom of expression and demerging views.

Historical traces of intelligence come from ancient Persia, Greece and Rome. The premise is that the oldest denunciation was formally written about 4,000 years ago, and was reported by the station commander to his master for mysterious light signals (Faligot and Kauffer 2006, pp. 24-26). It is difficult to determine whether and to what extent the obtained data came from public sources in the past, but the message was sent to the recipient through a full conspiracy, which used various forms and methods of concealment, for example sewing them in the sandals of a messenger who did not even know what his mission was. Spartans even used encrypted messages with a device called a squid (*it was a device consisting of a smooth roll and a shaft*), which could be read on the stem of the apparently written text (Korzeniewski and Pepłoński 2005, p.15).

Intelligence and military recon

The definition of the term "intelligence" is explained according to the subjected matters and fields of study. The intelligence was defined as the knowledge that the state must have in order to ensure that the interests of the state will not be affected and the taken actions will not be doomed. This means that acquiring knowledge requires a functional organisation consisting of people and specific structures, who and which receive information products, which are made up of

knowledge bases, information about current events and phenomena, and very valuable predictions and intelligence assessments (Minkina 2014, p. 27). The meaning of the term "intelligence", which refers both to the form of intelligence and recognition, is very important. That's why the term military reconnaissance is interchangeable with the term "military intelligence" in this article.

Intelligence is an important factor in decision-making in foreign and internal policy, defence, international security, and often in the economy. Nowadays, it is very important to use properly open source information (OSINT). Much available data, after proper processing, verification and analysis, could become useful material in intelligence agencies. Therefore, public information is included in the form of military reconnaissance. Such information searches are also used by international institutions, i.e. the NATO Alliance and the European Union, which have appropriate intelligence departments (Dictionary of the NATO).

The term "military reconnaissance" of the Armed Forces in Poland is usually related to the acquisition, computation and use of information by their commanders. It has a documentary and observation character. In war intelligence methods (*consisting of fighting with groupings of fighters*), the boundary between tactical actions and strategic is flushed, while the goal of acquiring information is the same. The designation "intelligence information" is understood to be relevant for political and security policy purposes and for the prevention of threats. Military matters, such as military capabilities and plans for operations, have great importance. For operational activities, publicly available and published information is crucial, i.e. about diplomatic activity and political plans that can be acquired through tools such as OSINT. This category also includes information on internal, economic, social, scientific and technical policies as well as demographic issues. Despite its openness, it is in the secret services' scope, because after proper processing and analysis, it becomes valuable information (Dictionary of NATO). At the data gathering stage in military reconnaissance, available sources of information may be collected by several people or by a group of specialists acting as linkers between the users and the forces assigned to them.

However, it is essential to have analytical skills that enable the user to process the data in relevant reconnaissance information. Once the data collection plan is completed, it is analysed in such a way that the compilation of all data is forwarded to the commander in order to promptly determine the scope of future activities (Modrzejewski 2013, pp. 141-142).

OSINT

The term "white intelligence" or "open source of information" is becoming more and more common. White intelligence mainly consists of acquiring information from public sources i.e. publicly available. The formulation of this term ("white intelligence") is a Polish concept, as it usually uses the American acronym OSINT (Open Source INTelligence), which is literally translated as "open source" (Minkina 2014, p. 41).

Through "white intelligence", we can understand that intelligence activities are conducted on the basis of open and widely available sources i.e. analysis of journalism or media coverage. Often this is referred to as legal, in accordance with the Vienna Convention on Diplomatic Relations, but it is worth pointing out that in intelligence activities, even the analysis of information from open sources is not and should not be public. This is a very common method used in intelligence agencies, which mainly consists in studying and analysing officially published materials. This method, also referred to as the non-subjective, apparent or public, is based on monitoring: daily news, political, business and technical press; reports on the actions and intentions of the government or the ruling party; radio and television broadcasting; geoinformation and many other open public databases (Larecki 2007, pp. 749-750).

Open Source Intelligence's (OSINT) blatant information, is also defined as the result of performing information acquisition activities. Information is searched, compared in content, and the most relevant for the recipient identified. OSINT is also defined as information analysis from a legal, blatant source. It is distinguished by a friendly and secure form of information and public access for every citizen (Mroziewicz 2007, p. 334). As the source information, it includes data and its sequence from one or more sources (Liedel 2004, pp. 48-50).

Of course, the main advantage of the open source intelligence is the speed of information acquisition, including quantity, quality and transparency, variety, ease of use and low cost of analysis. This is the result of the information technology revolution and the development of the Internet. With surveillance tools, such as mobile devices and broadband connections, tracking and analysing of entities is available from anywhere in the world. Sometimes, investigative journalists report

more information than intelligence services. That is why monitoring information with OSINT is very important for the activities of the special services (Leetaru 2010, p. 18).

Metadata as a white intelligence (OSINT)

The tasks of military reconnaissance in which OSINT serves as a solution concern the broadly understood collection of information which allow a given object to be identified, in particular to acquire geospatial data used in map creation. Image recognition uses Open Source Intelligence. Information intelligence conducted with the use of Open Source Intelligence is aimed at providing information relevant for determining the strategic directions of the activity of other countries.

On the grounds of information obtained from open sources, political decisions are made as well as threats in the external environment are monitored. Image recognition (Imagery Intelligence - IMINT) involves obtaining information using imaging tools and photos. Not only optical tools, radar, reconnaissance aircraft and lasers are used for this task, but also public programmes for every Internet user. Depicture diagnosis is undoubtedly one of the most important and the most reliable disciplines of obtaining information (Minkina 2011, p. 186).

Thanks to programmes containing databases, researchers can i.a. develop geographical protection by visualising the area. Military reconnaissance focuses on information including: terrain, hydrographic networks, transport networks, land cover and the type of land. All this data is needed to develop a military strategy that often determines the success or failure of security systems. Imaging diagnosis is constantly strengthening its position among other intelligence disciplines. Unfortunately, this technology, despite the obvious advantages of facilitating intelligence work and accelerating the decision-making process, also has technical limits which hinder its effects (Clark 2013, p. 195). Because of the programmes, providing maps and their analysis, you get data on: routes and determining the passability of an area, visibility analysis, recognition of targets, and, thanks to shaded military bases on the map, you can also determine their location. An extremely useful source of information in the context of military reconnaissance are websites that contain maps with current positions of troops.

They accept both the form of websites and applications integrated with social networking sites.

Geoinformation as the field of geography deals with the collection, processing, transmission, acquisition, interpretation and analysis of geospatial data. Due to the fact that this data is largely free of charge, the use of geoinformation studies may be one of the most important for OSINT techniques. The basic geoinformation tool is the Geographic Information System (GIS). It is an information system used to enter, collect, process and visualise geographical data, including that which supports the decision-making process. GIS consists of geographical databases, software and hardware. The group of GIS applications are i.a. land and building registry. Another group of GIS applications includes statistical data analysis. These systems can be a helpful tool for data processing on the technical infrastructure of the area, i.e. water, gas, energy or communication lines (Liedel and Serafin 2011, pp. 69-71).

In addition to the advanced tools provided by GIS, there are also many portals which provide maps and satellite images. In Polish cyberspace, the largest and most useful of these is undoubtedly the *Geoportal* (Geoportal.gov.pl). It allows access to many geographical databases, including agriculture, forestry, construction, state administration, activity of private entities, current and accurate spatial information, including geographical environment data, and objects and phenomena in the entire geographic space (*geportal*). Other useful services that give access to maps and satellite images are, among others, maps.google.pl, bing.com/maps and targeo.pl. *Targeo* is extremely useful for locating buildings quickly. Google Street is a useful service, especially for *ad hoc* operational planning. The program provides photos of streets made from the car's perspective and the database contains most of the metropolises and cities in the world (OSGeo).

The big advantage of IMINT is that it covers a wide range of technical devices and methods of obtaining information, using photography and optics. Image data, especially from satellite systems, allows observation of large areas, including those that cannot be reached by other intelligence disciplines. The information obtained through white intelligence includes: information about the potential opponent and terrain, the ability to operate in the group over areas of interest, the recognition of large areas of interest and the high accuracy of the location of objects and their display.

OSINT in military intelligence

Many institutions have for a long time appreciated the usefulness and value of information obtained from open sources, despite the fact that in the past, information from human sources (HUMINT, agents) or technical means (IMINT, SIGINT) was considered as the most valuable. Nowadays, the view has changed radically and it is appreciated that information is acquired in an open way, so that agents are not at risk of losing their health or life.

Moreover, the data set and analytical look may result in the addition of information value. Nowadays, most of the information is available online so you can easily reach it. You cannot, however, bypass open sources with limited availability. Some portals and databases belong to these. Intelligence agencies are devoting more and more resources to obtaining information from the public. Unlimited access to content and a powerful amount of data requires appropriate selection in terms of topics and needs. Therefore, this type of operation uses specialised information technology. Searching for information using OSINT requires different forms of activity, for example: intelligence services review journals and publications from different disciplines, and intelligence officers participate in scientific conferences and debates, where views on specific topics are exchanged. Proponents of obtaining information from open sources point out the unlimited possibilities of rapid and violent change in the direction of intelligence, where in comparison to human intelligence, there is no risk of personal disclosure. Thanks to the conspiratorial nature, OSINT is an effective instrument for fighting terrorism and is probably the most effective way of obtaining information about an attack (Minkina 2014, pp. 191-195).

From the point of view of the intelligence services, the primary advantage that cannot be overestimated is the negligible risk of counterfeiting, so that there are no consequences for this intelligence activity. Accordingly, this method was and is most often used by Western intelligence services (Mercado 2017). Another advantage is the ability to use a wide distribution of reports, which were developed using open source intelligence. Due to the fact that the procedures for the protection of classified information are omitted, there is the possibility of exchanging data between allied services, thus increasing the efficiency of intelligence work (Minas 2010, pp. 34-35).

In Poland, special services do not exist as in other countries. It has separate specialist analytical teams which deal exclusively with open source intelligence. The obtained information is often verified by compiling it in secret databases or gained information by operational teams (Dupont 2008, p. 26). However, it also has specialists responsible for the analysis of information derived from OSINT. The organisational model in Poland's intelligence services is not homogenous. In individual departments, the structures responsible for obtaining information from open sources are: Foreign Intelligence Agency - Bureau of Information and Analyses (Zarządzenie Nr 74 Prezesa Rady Ministrów z dnia 26 czerwca 2002 r. *w sprawie nadania statutu Agencji Wywiadu* (M.P. 2011 nr 26 poz. 433), 3 § ust. 1), Internal Security Agency - Office of Records and Analysis (Office E) (Zarządzenie Nr 73 Prezesa Rady Ministrów z dnia 26 czerwca 2002 r. *w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego* (M.P. 2002 nr 26 poz. 432), 3 § ust. 1), Central Anti-Corruption Bureau - Analysis Department (Zarządzenie Prezesa Rady Ministrów z dnia 6 października 2010 r. *w sprawie nadania statutu Centralnemu Biuru Antykorupcyjnemu* (M.P. z 2010 r. Nr 76, poz. 953), § 3 ust. 1). In the case of military special services, i.e. Counterintelligence Service Military (SKW), tasks are currently carried out by individual boards i.e. Operational, Economic Protection of Interests of Armed Forces and Protection of Armed Forces. According to SKW executives, the implementation of Open Source Intelligence activities has made it time-consuming to implement analytical and informational activities (Hoc 2012, p. 313).

Information war in military recognition

Due to easier access (via the Internet and mobile telephony) to the majority of information, texts and images (practically from anywhere in the world), intelligence faces new challenges and its functionality is influenced by conditions and phenomena created in civilisation processes, i.e. development information technology, transparency of the modern world and non-state actors. Commercial media, which communicates messages globally with the use of satellite platforms, has moved some away from mainstream information. On the other hand, democratic states publish a large amount of information about their politics and about the activities undertaken. Important information officially published for

the military sector is information about general supplies and stock of weapons, which are designed to reduce the probable outbreak of an unexpected war. Often, such information is not necessarily true and needs to be analysed for geopolitical reasons. By means of these measures, trust and the misperception of reality and the uncertainty of citizens are reduced (Mearsheimer 1994/1995).

Global access to a large amount of information found in public sources brings with it specific consequences and problems for intelligence. Access to official forecasts and analytical reports, state publications and non-governmental organisations does not mean that military intelligence has the necessary information. Wide access to information poses the most problems for analytical divisions, because the amount of information hinders its correct assessment (Lord 2007, p. 186). Military operations are notable for their highly mobile activities. Adequate acquisition, processing and transmission of information has become a challenge that significantly affects the process of command. The right decision depends on what information the commander has. Erroneous decisions are often made due to underestimating or missing information. However, those prepared in a methodically correct manner and based on reliable information are most often effective (Penc 2000, p.158).

Military reconnaissance is currently perceived through the prism "information war" as a context for the information preparation of the battlefield. The task of military reconnaissance also includes conducting information fights. The essence of this informational preparation is to maximise the effects of data acquisition and to transform them in the process of analysing the information. Disinformation projects are used to disrupt and circulate information in command systems. They exert pressure on the psyche of soldiers and commanders and mask their own forces and resources. Therefore, the "credibility" of all these undertakings should be maximised, because such actions can be introduced by an opponent in error and provide an advantage. Information fight is treated not only as an electronic fight with psychological activities but also as a theoretical development of the problem of military reconnaissance with possessed forces and means operating in information spaces (Ciborowski 2000).

Conclusions

The intelligence of the armed forces is mainly driven by the information needs of the staff and the armed forces, the commanders and the defence ministry. It involves recognising air, sea and land forces, as well as potential warfare, cyberspace and space. Interest mainly concerns the defence potential of any opponent, strategies, possibilities of using the armed forces, doctrines and administration of the defence system. For military intelligence, the social support of the armed forces and their actions is important. This information can be obtained from Open Source Information (OSINT).

Mankind has learned not only the acquisition of information over the years, but also the means of intelligence and the identification of channels for secret information. Through publicly available sources without infringing on the law, all the world's services have accessed them in recognisable ways. Often, official publications, exhibitions, advertising conferences, and ordinary people have provided missing information that complements the acquired knowledge through intelligence.

The OSINT functions properly at all levels of intelligence activities in almost every subjected area, so there are many actors that use it not only for military issues, but also in the private sector. Effective information retrieval using Open Source Intelligence has found its application at strategic, operational and tactical levels. In the age of technological development, the use of "white intelligence"/ OSINT offers many new opportunities for special services. Although the source of intelligence in Polish services is practised to a lesser degree than in the West, its potential is being increasingly recognised.

References

Ciborowski, L., 2000. *Planowanie, organizowanie i prowadzenie walki informacyjnej na szczeblach taktycznych wojsk lądowych.* Warsaw.

Clark, R.M., 2013. *Intelligence Collection.* Sage, Los Angeles.

Dupont, A., 2008. Intelligence for the Twenty-First Century. In W.K. Wark (ed.), *Twenty-First Century Intelligence.* Routledge, London.

Geoportal.gov.pl [online] Available from: http:/www.geoportal.gov.pl [Accessed 26 Mar 2018].

Faligot, R. and Kauffer, R., 2006. *Służby specjalne. Historia wywiadu i kontrwywiadu na świecie.* Iskry, Warsaw.

Hoc, S., 2012. Analiza informacji kontrwywiadowczej. In J. Konieczny (ed.), *Analiza informacji w służbach policyjnych i specjalnych.* Wydawnictwo C. H. Beck, Warsaw.

Korzeniewski, L. and Pepłoński, A., 2005. *Wywiad gospodarczy. Historia i współczesność*. Kraków.

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

Leetaru, K., 2010. The Scope of FBIS and BBC Open-Source Media Coverage, Studies. *Intelligence* 54 (1).

Liedel, K. and Serafin, T., 2011. *Otwarte źródła informacji w działalności wywiadowczej*. Dyfin, Warsaw.

Liedel K. and Piasecka P., Współpraca międzynarodowa w zwalczaniu terroryzmu, „Adam", Warszawa 2004

Lord, K.M., 2007. National Intelligence in the Age of Transparency. In L.K. Johnson (ed.), Strategic Intelligence, vol. 1: *Understanding the Hidden Side of Government.* Westport.

Mearsheimer, J., 1994/1995. *The False Promise of International Institutions*. International Security, Winter.

Mercado, S.C., 2017. *Sailing the Sea of OSINT in the Information Age: A Venerable Source in a New Era* [online] Available from: https://www.cia.gov/library/center-for-study-of-intelligence/csipublications/csistudies/vol48no3/article05.html [Accessed 8 Oct 2017].

Minas, H., 2010. *Can the Open Source Intelligence Emerge as an Indispensable Discipline for the Intelligence Community in the 21st Centrury?* RIEAS: Research Paper, no. 139.

Minkina, M., 2014. *Sztuka wywiadu w państwie współczesnym.* Rytm, Warsaw.

Minkina, M., 2011. *Wywiad w państwie współczesnym. Rozprawa habilitacyjna*. Zeszyty Naukowe AON, dodatek.

Modrzejewski, Z., 2013. *Rozpoznawcze wsparcie operacji informacyjnych*. Zeszyty naukowe AON 90 (1).

Mroziewicz, K., 2007. *Czas pluskiew*. Sensacje XX wieku, Warsaw.

OSGeo [online] Available from: http://www.osgeo.org [Accessed 26 Mar 2018].

Penc, J., 2000. *Menedżer w uczącej się organizacji*. Wydawnictwo: Menadżer, Łódź.

Więckiewicz, Z., 1974. *Niektóre formy i metody działalności wywiadowczej. Publikacje i międzynarodowy ruch osobowy*. Warsaw, MSW.

Zarządzenie Nr 73 Prezesa Rady Ministrów z dnia 26 czerwca 2002 r. w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego (M.P. 2002 nr 26 poz.432).

Zarządzenie Nr 74 Prezesa Rady Ministrów z dnia 26 czerwca 2002 r. w sprawie nadania statutu Agencji Wywiadu (M.P. 2011 nr 26 poz. 433).

Zarządzenie Prezesa Rady Ministrów z dnia 6 października 2010 r. w sprawie nadania statutu Centralnemu Biuru Antykorupcyjnemu (M.P. z 2010 r. Nr 76, poz. 953).