SECURITY DIMENSIONS
NO. 32; 2019 (82–105)
DOI 10.5604/01.3001.0014.0988

Intelligence Sources in the Process of Collection of Information by the U.S. Intelligence Community

Mariusz Antoni Kamiński*

ABSTRACT

Every day, U.S. intelligence agencies gather huge amounts of information from a variety of sources. Collection of information is an essential part of the process described as Intelligence Cycle. The purpose of this article is to identify the essence and nature of intelligence sources and to analyze their practical use by the agencies and departments that make up the U.S. Intelligence Community. The author characterizes the main types of intelligence sources – Human Intelligence (HUMINT), Geospatial Intelligence (GEOINT), Signals Intelligence (SIGINT), Measurement and Signature Intelligence (MASINT), and Open Source Intelligence (OSINT) – and indicates which U.S. intelligence agencies are responsible for their use. Moreover, the author presents the problems with the use of intelligence sources that occur in the work of the U.S. Intelligence

* Mariusz Antoni Kamiński, Ph.D., War Studies University, Warsaw, Poland; correspondence address: Akademia Sztuki Wojennej, ul. al. gen. A. Chruściela „Montera" 103, 00-910 Warszawa-Rembertów, Poland; email: m.kaminski@akademia.mil.pl

Community. Research findings indicate that the best results of intelligence work can be achieved with the use of "all-source intelligence" (also referred to as fusion intelligence), which involves using as many sources as possible to prepare a final intelligence product.

ARTICLE INFO

Article history
Received: 3.12.2019 Accepted: 16.12.2019

Keywords
sources and methods of intelligence, collection of information, intelligence cycle, Intelligence Community, HUMINT, GEOINT, SIGINT, MASINT, OSINT

Introduction

There is no general consensus among researchers in the field of intelligence studies on one definition of *intelligence* that would be acceptable to everyone. However, some common elements that characterize the work of intelligence agencies have been identified.

In Lowenthal's definition, "intelligence is the process by which specific types of information important to national security are requested, collected, analyzed, and provided to policymakers; the products of that process; the safeguarding of these processes and this information by counterintelligence activities; the carrying out of operations as requested by lawful authorities".[1]

On the other hand, in Warner's opinion, "intelligence is secret, state activity to understand or influence foreign entities".[2] Also, Warner points out that *intelligence* is, among others, dependent upon confidential sources and methods for full effectiveness; performed by officers of the state for state purposes; and linked to the production and dissemination of information.[3]

Johnson stresses that from the American perspective, the characteristic aspects of *intelligence* are information (knowledge), process (intelligence

[1] M.M. Lowenthal, *Intelligence. From secrets to Policy*, seventh edition, Thousand Oaks 2017, p. 10.

[2] M. Warner, *Wanted: A Definition of "Intelligence". Understanding Our Craft*, „Studies in Intelligence", 2002, no. 46(3), pp. 15–22.

[3] *Ibidem.*

cycle), mission (e.g. counterintelligence and secret operations of intelligence), and organization (U.S. Intelligence Community).[4]

It is clear that in each of these definitions the key role is played by *information*. American intelligence agencies gather huge amounts of information. This knowledge comes from a wide variety of intelligence sources. Over the years, methods of intelligence work have also been developed to acquire information and analyze it.

The purpose of this article is to identify the essence and nature of intelligence sources and to analyze their practical use by the agencies and departments that are a part of the U.S. Intelligence Community. Five classic intelligence sources are analyzed herein: Human Intelligence (HUMINT), Geospatial Intelligence (GEOINT), Signals Intelligence (SIGINT), Measurement and Signature Intelligence (MASINT), and Open Source Intelligence (OSINT). Moreover, for a better understanding of the context of the article, organization of the Intelligence Community organization and activities of the Intelligence Cycle are presented in this article.

In the research process, a critical analysis of literature in the field of Intelligence Studies (mainly by American authors) and source materials (including legal acts, strategies, reports, and other official studies of the entities forming the U.S. Intelligence Community) was performed.

U.S. Intelligence Community

The Intelligence Community is a group of Executive Branch agencies and organizations that work separately and together to engage in intelligence activities that are necessary for the conduct of foreign relations and the protection of the national security of the United States.[5]

The United States Intelligence Community (IC) is composed of seventeen entities which pursue various aspects of the intelligence and counter-intelligence mission. IC is supervised by the Office of the Director of National Intelligence (ODNI) headed by Director of National Intelligence (DNI).[6]

[4] L.K. Johnson, *National Security Intelligence*, [in:] *The Oxford Handbook of National Security Intelligence*, L.K. Johnson (ed.), Oxford 2010, p. 6.

[5] Office of the Director of National Intelligence, *What is Intelligence?*, https://www.dni.gov/index.php/what-we-do/what-is-intelligence (accessed: 30.11.2019).

[6] The Intelligence Community, http://www.intelligence.gov (accessed: 30.11.2019).

DNI oversees and directs the implementation of the National Intelligence Program[7] and acts as the principal advisor to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to national security. The President appoints the DNI with the advice and consent of the Senate.[8]

IC comprises the following:

- two independent agencies: the Central Intelligence Agency and the Office of the Director of National Intelligence;
- eight military units supervised by the Department of Defense: the Defense Intelligence Agency, the National Security Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, and military intelligence units within individual types of the armed forces – the Army (Intelligence and Security Command), Navy (Office of Naval Intelligence), Marine Corps (Marine Corps Intelligence), and Air Force (the Sixteenth Air Force);
- seven civil departments and agencies: "the Department of Energy's Office of Intelligence and Counter-Intelligence, the Department of Homeland Security's Office of Intelligence and Analysis and U.S. Coast Guard Intelligence, the Department of Justice's Federal Bureau of Investigation and the Drug Enforcement Agency's Office of National Security Intelligence, the Department of State's Bureau of Intelligence and Research and the Department of the Treasury's Office of Intelligence and Analysis".[9]

Intelligence Cycle

Over the years of development of intelligence, a systematic process was formed, which consisted of interrelated and repetitive activities of intelligence agencies, referred to as Intelligence Cycle. This is now a typical work form for the Intelligence Community.

[7] National Intelligence Program, http://obamawhitehouse.archives.gov/omb/factsheet_department_intelligence (accessed: 30.09.2019).

[8] Office of the Director of National Intelligence, *What is Intelligence?*, https://www.dni.gov/index.php/what-we-do/what-is-intelligence (accessed: 30.11.2019).

[9] *Idem*, *Members of the IC*, https://www.dni.gov/index.php/what-we-do/members-of-the-ic (accessed: 30.11.2019).

"The Intelligence Cycle is the process of developing raw information into finished intelligence for use by policymakers, military commanders, and other consumers in decision making".[10]

In the intelligence studies literature, as well as among practitioners, there are several versions of the Intelligence Cycle. They differ in the number of steps in the process:

- Minkina lists 4 steps: management/request, acquisition/collection, processing/analysis, dissemination/development, and transfer to the recipient.[11]
- In the official publication *U.S. National Intelligence. An overview 2013*, 6 steps are specified: planning and direction, collection, processing and exploitation, analysis and production, dissemination, and evaluation.[12]
- Lowenthal lists 7 steps: identifying requirements, collection, processing and exploitation, analysis and production, dissemination, consumption, and feedback.[13]

It should be noted that collection plays an important role in each of the above-mentioned Intelligence Cycle concepts. The importance of intelligence collection is best evidenced by the fact that in the publications on this topic it is referred to as the "bedrock of intelligence" or the "very heart of the intelligence".

In the United States, the means of collecting intelligence are sometimes referred to as collection disciplines or INTs.[14] Intelligence is collected using various sources and intelligence methods.

Intelligence sources and methods

According to Goldman, intelligence sources can include persons, images, signals, documents, databases, and communication media capable of providing intelligence through specific means of collection and analysis. Intelligence methods, on the other hand, include strategies and tactics

[10] Intelligence Community Information Sharing Executive, *U.S. National Intelligence: an overview 2013*, 2013, p. 4.

[11] M. Minkina, *Sztuka wywiadu w państwie współczesnym*, Warszawa 2014, p. 170.

[12] Intelligence Community Information Sharing Executive, *U.S. National…, op. cit.*, p. 4.

[13] M.M. Lowenthal, *Intelligence…, op. cit.*, p. 73.

[14] *Ibidem*, p. 91.

of information collection and analysis, as well as operations and technologies used to generate intelligence products.[15]

The standard classification of intelligence sources includes:

- Human Intelligence (HUMINT);
- Geospatial Intelligence (GEOINT);
- Signals Intelligence (SIGINT);
- Measurement and Signature Intelligence (MASINT); and
- Open Source Intelligence (OSINT).

Wirtz points out that the term *intelligence methods* (synonymous with the term *tradecraft*) refers to techniques used by operational officers and analysts in the performance of their duties. *Tradecraft* in operational work may include, but is not limited to, building up a network of undercover agents working in foreign countries, avoidance of detection by counter-intelligence agents, maintenance of secret communication channels, and the very art of recruiting and handling of undercover agents. Analysts' working methods include, among others, elements of methodology used in social sciences, computer analytical tools, teamwork using new information technologies, etc.[16]

The *Intelligence Reform And Terrorism Prevention Act of 2004* indicates that "National Intelligence and the term »intelligence related to national security« refer to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and that involves threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security".[17]

Every country protects its sources and methods of intelligence, as their disclosure could have disastrous consequences for national security. This is also crucial for the success of current and future intelligence operations.

[15] J. Goldman, *Words of Intelligence: An Intelligence Professional's Lexicon for Domestic and Foreign Threats*, second edition, Lanham – Toronto – Plymouth 2011, pp. 237–238.

[16] J.J. Wirtz, *The Sources and Methods of Intelligence Studies* [in:] *The Oxford Handbook of National Security Intelligence*, L.K. Johnson (ed.), Oxford 2010, DOI 10.1093/oxfordhb/9780195375886.003.0004, p. 59.

[17] *Intelligence Reform And Terrorism Prevention Act of 2004*, Public Law 108–458 of December 17, 2004; 118 STAT. 3638, sec. 1012.

In the United States, the term "intelligence sources and methods" is a legal term. Their protection falls within the competence of the Director of National Intelligence, who develops uniform standards and procedures for access to and protection of intelligence, as well as for its consistent implementation in the various agencies and departments.[18] At the same time, each of the entities constituting a part of the Intelligence Community ensures appropriate protection of information obtained in the course of intelligence work.

Human Intelligence (HUMINT)

Human intelligence sources are the oldest form of intelligence collection. Until the time of the technical revolution in the 20th century, they were the main means of intelligence work.

In the official publication of the Intelligence Community entitled *National Intelligence. A consumer's guide*, 2009, the term 'Human Intelligence' is defined as "intelligence derived from information collected and provided by human sources. This intelligence includes overt data collected by personnel in diplomatic and consular posts, as well as otherwise unobtainable information collected via clandestine sources of information, debriefings of foreign nationals and U.S. citizens who travel abroad, official contacts with foreign governments, and direct observation".[19]

This definition clearly distinguishes between information obtained from human sources in an open and covert manner. In the first case, such data is collected by official representatives of the U.S. administration (also called officially covert[20]). On the other hand, information obtained in a covert way is collected by covert intelligence officers (referred to as nonofficial covert, NOC).

In another official publication of the Intelligence Community, entitled *U.S. National Intelligence: an overview 2013*, it is emphasized that HUMINT is the only intelligence source where the persons seeking intelligence talk directly to human information sources, control the topic of the discussion, and guide their actions. It was also pointed out that

[18] *Ibidem*, sec. 102A, (i), (1).

[19] National Intelligence for Policy, Plans, and Requirements, *National Intelligence. A consumer's guide*, 2009, p. 12.

[20] Separation into "official covert" and "nonofficial covert" is also indicated by Lowenthal. See: M.M. Lowenthal, *Intelligence..., op. cit.*, p. 139.

thanks to Human Intelligence it is possible to gain access to information that cannot be obtained in any other way.[21]

As Minkina emphasizes, in the most typical situations it is possible to gain a human source by recruiting a government official (civil or military), who, due to his or her professional position in government structures, has access to important information and, at the same time, for various reasons, agrees to provide this information to an intelligence officer of another state.[22]

In the United States, obtaining information from human sources is primarily the domain of the Central Intelligence Agency. In the structure of the CIA, the Directorate of Operation (DO) is responsible for HUMINT. Of all the agencies subordinate to the Department of Defense, human sources are used mainly by the Defense Intelligence Agency, which has a specialized division called Defense Clandestine Services (DCS). As for other civilian agencies, the FBI and the DIA also use HUMINT.

HUMINT is a much more time-consuming source of information than other technical intelligence sources. On the one hand, there is a need for proper training of intelligence officers and their mastery of methods of working with human sources. On the other hand, acquiring a valuable human intelligence source is an extremely complicated operation that may take years, and the final success depends on many factors.

The use of personal sources (especially secret agents) also requires a great deal of caution and is associated with a huge risk, e.g. people unmasked by counterintelligence agencies may be charged with espionage and face long prison sentences (in some countries even the death penalty). Also, some human sources of intelligence may turn out to be "double agents" who actually work for another intelligence agency and fabricate information to deliberately mislead its recipients.

The 1980s are often referred to as the "golden age of spies". In that period, the competing powers, the U.S. and the U.S.S.R., allocated huge funds for the development of spy networks and for obtaining information about the other side of the conflict using human sources. However, after the end of the Cold War, in the absence of a single powerful enemy of the United States, the process of reduction of the use of HUMINT

[21] Intelligence Community Information Sharing Executive, *U.S. National…*, *op. cit.*, pp. 45–46.

[22] M. Minkina, *Sztuka wywiadu…*, *op. cit*, pp. 178–179.

and of limitation of funds allocated for this purpose began. This has had far-reaching negative consequences. Reports of two congressional committees stated that the reasons for the failure to prevent the terrorist attacks of 11 September 2001 and for the erroneous intelligence assessment that Iraq had weapons of mass destruction (which was the reason for the U.S. invasion of the country) included negligence in the use of *human intelligence*. It was pointed out that, since the break-up of the Soviet Union, American intelligence agencies had lost considerable human sources of intelligence, which caused them to act far below their optimal strength. It was emphasized that in the 1990s there was a significant decline in the number of CIA and DIA staff working in HUMINT and that the Intelligence Community did not adapt to the changing threats; instead, it used old techniques and acted too slowly.[23]

The report of the 9/11 Commission (which led to the reform of the Intelligence Community) contained recommendations to the CIA Director, including restoration of the analytical capacity of the CIA; development of the capacity to extract information from human sources (especially data obtained covertly); ensuring an appropriate operational relationship between HUMINT and SIGNAL sources; greater diversity in the recruitment of persons to work with human sources; and development of better language programs for intelligence personnel with appropriate financial incentives to use them.[24]

Geospatial Intelligence (GEOINT)

The term 'Geospatial Intelligence' is officially defined in the United States Code as[25] the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and

[23] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States*, 2005, http://fas.org/irp/offdocs/wmd_report.pdf (accessed: 30.11.2019), p. 366.

[24] National Commission on Terrorist Attacks, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, http://www.9-11commission.gov/report (accessed: 30.11.2019), p. 415.

[25] The United States Code (USC) is a consolidation and codification by subject matter of the general and permanent laws of the United States. It is prepared by the Office of the Law Revision Counsel of the United States House of Representatives. See: http://uscode.house.gov (accessed: 30.11.2019).

geographically referenced activities on the earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information.[26]

Imagery, in general, means collectively, the representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. Imagery correlation, on the other hand, means the mutual relationship between the different signatures on imagery from different types of sensors in terms of position and the physical characteristics signified.[27] Imagery is most often acquired from the air by means of, among others, satellites, unmanned aerial vehicles, and reconnaissance aircraft. Imagery does not, however, include photographs taken by human sources (HUMINT) by hand.

Imagery Intelligence (IMINT)[28] is a term used in the past to describe the intelligence functions of geospatial sources. In the literature on this subject matter, this term is still used interchangeably with GEOINT. In the opinion of many experts, however, this approach is wrong, as the term IMINT is already obsolete and does not really reflect what GEOINT is today.[29] Currently IMINT is part of GEOINT in the field of image acquisition using, among others, visual photography, radar sensors, infrared sensors, lasers, and electro-optics.[30] Thus, Imagery Intelligence is technical, geographic, and intelligence information derived from the interpretation or analysis of images and additional materials.

Geospatial Intelligence, on the other hand, is a broader concept, also covering Geospatial Information, which is "information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the earth and includes: statistical data and information derived from, among other things, remote sensing, mapping, and surveying technologies; and mapping, charting, geodetic data, and related products".[31] GEOINT also uses the Geographic Information System (GIS) for entering, collecting, processing, and visualizing geographical data to support the decision-making process.

[26] *United States Code*, Title 10, §467, http://uscode.house.gov (accessed: 30.11.2019).

[27] NATO Standardization Agency, *AAP-6(2014)*, 2014, p. 206.

[28] Sometimes the term Photo Intelligence (PHOTOINT) is also used.

[29] This opinion is also expressed by other authors, see C.J. Jensen III, D.H. McElreath, M. Graves, *Introduction to intelligence studies*, New York – London 2018, p. 112.

[30] Intelligence Community Information Sharing Executive, *U.S. National…*, *op. cit.*, p. 74.

[31] *United States Code*, Title 10, §467, http://uscode.house.gov (accessed: 30.11.2019).

It should be emphasized that geospatial information is not only about images, but also about the geolocation of objects or persons. For example, U.S. intelligence services have used geolocation of social media users to map refugees fleeing Syria.[32]

As highlighted in the publication entitled *Geospatial Intelligence in Joint Operations*, GEOINT's full utility stems from the integration and use of three elements: imagery, imagery intelligence (IMINT), and geospatial information. This synergy enables a more comprehensive perspective and a deeper understanding of the operational environment. Geospatial sources include tasks, activities, and events used to collect, manage, analyze, generate, visualize, and deliver imaging, imaging sources (IMINT), and geospatial information necessary to support national security and defense missions, as well as international agreements.[33]

In the United States, within the Intelligence Community, two agencies under the Department of Defense are responsible for collecting geospatial information. The National Geospatial-Intelligence Agency (NGA) plays a leading role in this respect and the other entity is the National Reconnaissance Office (NRO).

A particularly important role is played by the NGA Director, who is also responsible for coordinating all activities related to geospatial sources in the Defense Department as the DoD GEOINT Manager. Additionally, the NGA Director is also an advisor to the Director of National Intelligence (in all matters concerning GEOINT) and, as the GEOINT Functional Manager,[34] performs tasks related to the National System for Geospatial Intelligence (NSG).[35]

Geospatial sources are collected by means of various devices. The first one is satellites, the advantage of which is that by obtaining imagery from space they can provide information on the situation in countries with very difficult access (e.g. North Korea or Iran). As Herman noted, space reconnaissance covers a certain area but, most importantly, in peacetime, it does not violate the international rules of coexistence of states and

[32] M.M. Lowenthal, *Intelligence…, op. cit.*, p. 117.

[33] Joint Publication 2-03, *Geospatial Intelligence in Joint Operations*, 2017, p. VII.

[34] The NGA Director, as the GEOINT Functional Manager, also coordinates issues related to international cooperation on GEOINT, including the Five Eyes (FVEY) initiative which groups intelligence agencies from the United States, the United Kingdom, Australia, Canada, and New Zealand.

[35] Department of Defense, *Directive number 5105.60*, 29 July 2009.

nations.[36] The satellites currently used by the United States to collect geospatial sources provide materials of increasingly high resolution, making the intelligence obtained from these sources more precise. However, the high cost of maintenance of the satellite system (compared to other devices used in GEOINT) remains a problem. In addition, the transmitted images show the current situation only at the time the image is taken (which may change later), so it is essential that the geospatial material is properly analyzed and interpreted.

GEOINT information is also collected by the aviation industry. The NGA commissions Airborne Intelligence Surveillance Reconnaissance (ISR) to conduct air reconnaissance tasks primarily for military aviation. Moreover, the NGA also increasingly uses commercial systems.[37] Usually, reconnaissance planes flying near the border of the country under observation collect geospatial data and, in addition, can intercept messages from the means of communication. However, in times of an armed conflict, the air force carries out reconnaissance flights directly over enemy territory. The evident drawback of this is the possibility of the aircraft being shot down by the enemy and the possible death of the crew (or their becoming prisoners of war).

This risk is not present in the case of Unmanned Aerial Vehicles (UAV), which are also commonly used to acquire geospatial intelligence. In the last two decades, their role has grown rapidly. UAVs have an increasing range, can stay in the air longer, provide data with improved resolution, can approach the object under observation, and transmit data in real time. In addition, unmanned aerial vehicles can be used as a weapon to eliminate enemy targets. There are high hopes concerning the use of microdrones in the future (for the time being they are in the experimental phase), which could revolutionize aerial reconnaissance and intelligence gathering.

Signals Intelligence (SIGINT)

Signals Intelligence is the capture of information from communications, radars, and measurement devices. Traditionally, it is divided into two categories: Communication Intelligence (COMINT) and Electronic Intelligence (ELINT). However, in the United States there is another type

[36] M. Herman, *Potęga wywiadu*, Warszawa 2002, p. 83.

[37] Office of Geospatial Intelligence Management, *Geospatial Intelligence (GEOINT) Basic Doctrine, Publication 1.0*, 2006, p. 19.

of electromagnetic source of intelligence called Foreign Instrumentation Signals Intelligence (FISINT). As Richelson pointed out, even though FISINT is a subcategory of ELINT, a few years ago it was recognized as a source of SIGINT of equal standing with COMINT and ELINT.[38]

Indeed, in the 2013 official publication of the Intelligence Community, the term 'Signals Intelligence' is defined as "intelligence gathered from data transmissions, including COMINT, ELINT, and FISINT. SIGINT includes both raw data and the analysis of that data to produce intelligence".[39]

Communication Intelligence (COMINT) is intelligence derived from electromagnetic communications and communication systems by other than intended recipients or users.[40] COMINT is therefore the result of interception of communications between people, including phone calls, instant messaging, e-mails, and other communication systems.[41] What is also important is Traffic Analysis (also referred to as Geospatial Metadata Analysis), which includes identification of call parties and their detailed location, which devices and methods they use to contact each other, the technical parameters of their transmitters, the way they communicate, the frequency of their calls, etc.

As Goldman emphasizes, COMINT it is the result of the collection and processing (including decryption) of communications transmitted by electromagnetic means from foreign sources. Communication Intelligence does not include monitoring of foreign media or interception of information obtained during counterintelligence activities in the United States.[42]Electronic Intelligence (ELINT), on the other hand, is information originating mainly from interception of electronic signals (usually radar signals), which do not contain elements of interpersonal communication (speech or text). As defined by the Department of Defense, ELINT is "technical and geolocation intelligence derived from foreign

[38] J.T. Richelson, *The U.S. Intelligence Community*, Seventh Edition, New York – London 2018, p. 222.

[39] Intelligence Community Information Sharing Executive, *U.S. National…, op. cit.*, p. 47.

[40] NATO Standardization Agency, *AAP-6, op. cit.*, p. 102.

[41] Locating the interlocutor can be used, for example, to set a target to attack using UAV and to eliminate a person.

[42] J. Goldman, *Words of Intelligence…, op. cit.*, p. 41.

noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources".[43]

Foreign Instrumentation Signals Intelligence (FISINT), on the other hand, is "information derived from the interception of foreign electromagnetic emissions associated with the testing and operational deployment of non-U.S. aerospace, surface, and subsurface systems including, but not limited to, telemetry, beaconry, electronic interrogators, and video data links".[44] FISINT includes, among others, Intelligence Telemetry (TELINT), which concerns, among others, interception of data sent by missiles (or their components) during a test flight in order to estimate their technical characteristics.[45]

In the United States, the National Security Agency (NSA), subordinate to the Department of Defense, is responsible for Signals Intelligence in the field of foreign intelligence. Former NSA director, General Michael Hayden, described SIGINT as a continuous process, a kind of a spy production line where communications signals are collected, processed, analyzed, and reported on 24 hours a day, 7 days a week.[46] In his book *Intelligence. From secrets to Policy*, Lowenthal explains the differences between SIGINT and IMINT and quotes the words of the NSA Director, who allegedly said "IMINT tells you what has happened, SIGINT tells you what will happen".[47]

The National Security Agency points out, however, that Signals Intelligence "involves collecting foreign intelligence from communications and information systems and providing it to customers across the U.S. government, such as senior civilian and military officials. They then use the information to help protect our troops, support our allies, fight terrorism, combat international crime and narcotics, support diplomatic negotiations, and advance many other important national objectives".[48]

[43] Office of the Chairman of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, Washington DC 2019, p. 73.

[44] Intelligence Community Information Sharing Executive, *U.S. National…, op. cit.*, p. 47.

[45] J.T. Richelson, *The U.S. Intelligence…, op. cit.*, pp. 223–224.

[46] M.V. Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*, New York 2016, p. 14.

[47] M.M. Lowenthal, *Intelligence…, op. cit.*, p. 127.

[48] National Security Agency, *Frequently Asked Questions about Signals Intelligence (SIGINT)*, http://www.nsa.gov/about/faqs/sigint-faqs/ (accessed: 30.11.2019).

Signals Intelligence captures information in a variety of ways, including ground equipment, ships, planes, Unmanned Aerial Vehicle (UAV), and satellites. The same platforms are often used to collect GEOINT and SIGINT information, e.g. UAV collecting geospatial sources can simultaneously capture electromagnetic sources.

Information received by SIGINT is often encrypted. Thus, cryptanalysis, which consists in actions taken to convert encrypted text into plain text without the knowledge of the key used during encryption, is becoming immensely important. The NSA has a Central Security Service (CSS), which provides cryptological support, knowledge, and assistance to other cryptological institutions operating in the American military. The director of the NSA is also the head of the CSS. The NSA personnel is located in all the main military headquarters of the U.S. Army and is also located around the world, wherever the American military is present.[49] It should also be stressed that the National Security Agency is responsible for protecting the United States against hostile SIGINT activities.

Measurement and Signature Intelligence (MASINT)

Measurement and Signatures Intelligence (MASINT) is intelligence produced through quantitative and qualitative analysis of the physical attributes of targets and events to characterize and identify those targets and events.[50] According to the NATO dictionary, MASINT is "scientific and technical intelligence derived from the analysis of data obtained from sensing instruments for the purpose of identifying any distinctive features associated with the source, emitter or sender, to facilitate the latter's measurement and identification".[51]

Although Measurement and Signature Intelligence is also a technical intelligence source, the information obtained through MASINT is different from that obtained through GEOINT and SIGINT. Examples of MASINT might be the distinctive radar signatures of specific aircraft systems or the chemical composition of air and water samples.

Richelson points out that MASINT now includes a great many different technical elements, such as:

[49] National Security Agency, *Support to the Military*, http://www.nsa.gov/what-we-do/support-the-military (accessed: 30.11.2019).

[50] Intelligence Community Information Sharing Executive, *U.S. National…*, *op. cit.*, p. 45.

[51] NATO Standardization Agency, *op. cit.*, p. 251.

- radar (line of sight, bistatic, over the horizon);
- radio frequency (wideband electromagnetic pulse, unintentional radiation);
- geophysical data (acoustic, seismic, magnetic);
- nuclear radiation (X-ray, gamma ray, neutron);
- materials (effluents, particulates, debris);
- multispectral, hyperspectral, and ultraspectral imagery;
- biometrics (fingerprints, digital mug shots, speech recognition and voice prints, iris scans, DNA).[52]

It should be noted that there is a discussion among intelligence practitioners and theorists as to whether Measurement and Signature Intelligence should be considered a separate and independent intelligence source or whether it is only a product of SIGINT and GEOINT. However, due to the usefulness of MASINT, especially in the field of proliferation of weapons of mass destruction, most tend to include Measurement and Signature Intelligence in the category of classic intelligence sources.

The fact that there is no separate agency in the United States responsible only for MASINT also has an influence on the discussion as to whether MASINT is a separate intelligence source. Currently, it is the responsibility of the DIA and the NGA. The DIA Director is functional manager for Measurement and Signatures Intelligence. The Defense Intelligence Agency Directorate for MASINT and Technical Collection (DT) is the defense intelligence center for Measurement and Signatures Intelligence (MASINT). It collects and analyzes MASINT, and also develops new MASINT capabilities.[53]

Open Source Intelligence (OSINT)

The last of these classic intelligence sources is Open Source Intelligence (OSINT). This is a very important element in the process of information collection, although in this case information is collected from nonsecretive origins.

The statutory definition of Open Source Intelligence was presented in the *National Defense Authorization Act for Fiscal Year 2006*; in accordance with its provisions, OSINT is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a

[52] J.T. Richelson, *The U.S. Intelligence…, op. cit.*, p. 266.

[53] "Defense Intelligence Agency", http://www.dia.mil (accessed: 30.11.2019).

timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. In addition, this legislation indicates that "the production of open-source intelligence is a valuable intelligence discipline that must be integrated into intelligence tasking, collection, processing, exploitation, and dissemination to ensure that United States policymakers are fully and completely informed".[54]

According to Sands, OSINT can be divided into four main categories: widely available data and information; targeted commercial data; individual experts; and "gray" literature (access to which is possible but restricted only to a specific audience). Of these four categories, information may be collected, among others, from:

- mass media: newspapers, magazines, radio, television;
- public data: information derived from government reports; official data, such as data on budgets and demographics; hearings; legislative debates; press conferences, speeches, and other public sources;
- gray literature: open-source material that usually is available through controlled access for a specific audience. The material in gray literature covers scientific, political, socioeconomic, and military disciplines (for example: research reports, technical reports, unofficial government documents, working papers, discussion papers, preprints, studies, dissertations and theses etc.);
- observation and reporting: information of significance, not otherwise available, that is provided by, for example, amateur airplane spotters, radio monitors, and satellite observers.[55]

Open source information also can include information, which although unclassified, could be considered company proprietary, financially sensitive, legally protected, or personally damaging.[56]

More and more Open Source Intelligence information is also obtained from social media. American intelligence services have used them both during the Arab Spring in Egypt in 2011 and after the Boston Marathon bombing attack in 2013. However, Lowenthal points out that social media are not so important in themselves. More important is their skillful use

[54] *National Defense Authorization. Act for Fiscal Year 2006*, Public Law 109–163 of January 6, 2006; 119 STAT 3412, sec. 931.

[55] Intelligence Community Information Sharing Executive, *U.S. National…*, *op. cit.*, pp. 46–47.

[56] R.A. Best Jr., A. Cumming, *Open Source Intelligence (OSINT): Issues for Congress*, Congressional Research Service, RL34270, 5 December 2007, p. 7.

by intelligence, e.g. in the case of the revolt in the Tahir Square in Egypt, the key question was: Who is the most influential person in the social media there and why?[57]

As Minkina emphasizes, while recognizing the importance of OSINT, intelligence institutions are devoting more and more resources to the possibility of using them for their own purposes. Effective use of their huge quantities and their selection according to the interest and needs requires the use of specialized information technology.[58]

According to various estimates, OSINT accounts for about 80% of all information available to foreign relations intelligence analysts. It is also indicated that it can constitute about 95% of economic information.[59] On the other hand, General Samuel V. Wilson, a former DIA director, says that "ninety percent of intelligence comes from open sources. The other ten percent, the clandestine work, is just the more dramatic. The real intelligence hero is Sherlock Holmes, not James Bond".[60]

In the report prepared by the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction in 2005, it was stated that "clandestine sources, however, constitute only a tiny sliver of the information available on many topics of interest to the Intelligence Community. Other sources, such as traditional media, the Internet, and individuals in academia, nongovernmental organizations, and business, offer vast intelligence possibilities".[61] The Commission therefore recommended setting up an organization responsible for OSINT – the Open Source Directorate (within the CIA). However, President George W. Bush ordered the establishment of such a center in the office of the DNI. Consequently, the former Foreign Broadcast Information Services (FIBIS) was transformed into the Open Sources Center (OSC). However, in 2015 it was changed to the Open Source Enterprise (OSE) and merged with the CIA's new Digital Innovation Directorate. In this

[57] M.M. Lowenthal, *Intelligence…, op. cit.*, p. 153.

[58] M. Minkina, *Sztuka…, op. cit.*, p. 192.

[59] *Ibidem*, p. 192.

[60] R.A. Best Jr., A. Cumming, *Open Source…, op. cit.*, p. 4; A.S. Hulnick, *The Dilemma of Open Sources Intelligence: Is OSINT Really Intelligence?*, [in:] *The Oxford Handbook of Natinal Security Intelligence*, L.K. Johnson(ed.), Oxford 2010, p. 230.

[61] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report…, op. cit.*, p. 395.

way, the responsibility for OSINT was again placed in the domain of the CIA.[62]

At the end of the discussion of Open Source Intelligence, it should be pointed out that sometimes publications on this topic present opinions denying OSINT as a separate branch of intelligence.[63] However, nowadays, most of the opinions definitely indicate that Open Source Intelligence is a prominent intelligence source. Hulnick emphasizes that "OSINT is indeed intelligence. It provides information about our adversaries and enemies they might not want us to have. Properly interpreted, OSINT can be just as enlightening as well-informed secret agent, or an image from an unmanned aircraft zooming in on a terrorist".[64]

Effectiveness of intelligence gathering using intelligence sources

Intelligence work uses a variety of sources, because multi-source information is much more valuable. The U.S. Intelligence Community uses the term 'All-source Intelligence' (synonymous with 'Fusion Intelligence'), which means use of as many sources as possible (HUMINT, GEOINT, SIGINT, MASINT, and OSINT) to prepare the final intelligence product.[65] The *Intelligence Reform And Terrorism Prevention Act of 2004* obliges the Director of National Intelligence to designate a person responsible for ensuring that the intelligence products delivered by the agencies and departments within the *Intelligence Community* are up to date, objective, independent of political actors, and based on all available intelligence sources, and that they apply standards appropriate to analytical intelligence methods (*tradecraft*).[66]

A good example of the use of All-source Intelligence was the joint operation by the United States and Israeli intelligence services called Olympic Games, which was intended to delay Iran's nuclear program. Although cybernetic tools were used for the main attack, many methods

[62] M.M. Lowenthal, *Intelligence…, op. cit.*, p. 151.

[63] See: H. Bean, *The DNI's Open Source Center: An Organizational Communication Perspective*, "International Journal of Intelligence and CounterIntelligence", 2007, no. 20(2), pp. 240–257, DOI 10.1080/08850600600889100.

[64] A.S. Hulnick, *The Dilemma…, op. cit.*, p. 254.

[65] Committee on National Security Systems, *Instruction 4009. Committee on National Security Systems (CNSS) Glossary*, 2015, p. 5.

[66] *Intelligence Reform And Terrorism Prevention Act of 2004, op. cit.*, sec. 1019 (a).

and intelligence sources were also used in the operation. Technical means, such as GEOINT, SIGINT and, MASINT, were used to obtain information about the infrastructure of the Natanz center where Iranians used centrifuges in the uranium enrichment process. In order to infect the Iranian system with the STUXNET virus, it was necessary to use HUMINT, i.e. to use spies who, having physical access to the underground Natanz plant, spread the first variants of the computer worm via an external USB memory stick.

Operation Olympic Games has shown that sharing and using information from various intelligence sources can be very effective in the work of intelligence agencies. However, it should also be noted that in this respect, there is probably a problem that affects intelligence agencies worldwide. The problem is about internal competition between different intelligence agencies in a country and the reluctance to share information with others. This applies in particular to law enforcement and criminal intelligence institutions which aim to investigate, prosecute, and convict offenders. This different nature of work creates certain barriers in cooperation with intelligence institutions due to concerns about the protection of sources (especially in the case of human intelligence sources).[67] However, problems in the exchange of information also concern cooperation between intelligence agencies themselves. This is a widespread phenomenon and also affects the Intelligence Community in the United States. In order to address such situations, the *Intelligence Reform And Terrorism Prevention Act of 2004* provided the Director of National Intelligence with the powers to ensure maximum access to and sharing of intelligence within the Intelligence Community and to establish rules and procedures to resolve conflicts when, on the one hand, there is a need to protect sources and methods of intelligence and, on the other hand, there is a need to exchange intelligence.[68]

The process of sharing intelligence between agencies from different countries is even more complicated. Even in the case of allied countries, it is not so obvious. It should be taken into account that each country has its own interests and objectives and that the provision of certain infor-

[67] More information about cooperation between intelligence services and law enforcement agencies can be found in: F.F. Manget, *Intelligence and Law Enforcement* [in:] *The Oxford Handbook of National Security Intelligence*, L. K. Johnson (ed.), Oxford 2010, pp. 189–211.

[68] *Intelligence Reform And Terrorism Prevention Act of 2004, op. cit.*, sec. 102A, (g), (1), (d).

mation to the agencies of a friendly state does not always have to coincide with these interests. Nevertheless, such cooperation obviously exists and is developing (especially in the field of counteracting and combating terrorism), but it also has its limitations. Good examples of intelligence cooperation include intelligence support in the decision-making process of the North Atlantic Treaty Organization, which is carried out by national intelligence agencies of member states, NATO Headquarters institutions, and integrated military structures. Another example is the cooperation of American, British, Australia, Canadian, and New Zealand's civil intelligence agencies in the framework of the Five Eyes initiative. (FVEY).[69]

Conclusions

Collection of information is a key element of the Intelligence Cycle process and is the basis for effective functioning of intelligence. The agencies and departments within the Intelligence Community acquire information from a wide variety of sources. The classical list of intelligence sources includes technical means (GEOINT, SIGINT, and MASINT), covert sources (HUMINT), and open-source materials (OSINT).

A huge amount of money is spent on technical sources because of the advanced equipment used to acquire the information (satellites, airplanes, UAV, radars, etc.). However, this makes it possible to obtain very clear evidence of the activity of the opponent (satellite images, recordings of conversations, etc.). On the other hand, the use of human sources (especially secret agents) requires a lot of caution and involves a huge risk. However, these actions can be used to obtain information that is not otherwise available. It should also be noted that Open Source Intelligence, which is still somewhat underestimated, provides about 80% of all intelligence information in the United States. Its more efficient use can significantly improve the intelligence work.

It should also be noted that while in the initial historical phase of intelligence development Human Intelligence sources were the main area of activity, the 20th century brought a significant development of technical sources (GEOINT, SIGINT, and MASINT). On the other hand, the development of information society and the advent of the cybernetic era in

[69] More information about Five Eyes can be found in: L. Colucci, *Five Eyes – Foreign Intelligence Services*, [in:] *Homeland Security and Intelligence*, second edition, K. G. Logan (ed.), Santa Barbara – Denver 2018, pp. 97–114.

the 21st century brought about a decisive development of OSINT. Today, it seems most important to maintain an appropriate balance between technical, human, and open sources of intelligence, so as not to neglect any of them. The synergy of sources, i.e. consistent reliance on information from multiple intelligence sources – All-source Intelligence, or Fusion Intelligence – is also of key importance to intelligence work.

The reports of the two committees, the 9/11 Commission and the WMD Commission, and the critical remarks contained in their conclusions on the use of intelligence sources and methods and on internal competition among the agencies and departments forming the Intelligence Community, indicate that there is much room for improvement. On the other hand, it should also be noted that a large part of the commissions' conclusions has been taken into account, which has led to the reform of the Intelligence Community.

References

1. Bean H., *The DNI's Open Source Center: An Organizational Communication Perspective*, "International Journal of Intelligence and CounterIntelligence", 2007, no. 20(2), pp. 240–257, DOI 10.1080/08850600600889100.
2. Best R.A. Jr., Cumming A., *Open Source Intelligence (OSINT): Issues for Congress*, Congressional Research Service, RL34270, 5 December 2007.
3. Colucci L., *Five Eyes – Foreign Intelligence Services*, [in:] *Homeland Security and Intelligence*, second edition, K. G. Logan (ed.), Santa Barbara – Denver 2018, pp. 97–114.
4. The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States*, 2005, http://fas.org/irp/offdocs/wmd_report.pdf (accessed: 30 November 2019).
5. Committee on National Security Systems, *Instruction 4009. Committee on National Security Systems (CNSS) Glossary*, 2015.
6. "Defense Intelligence Agency", http://www.dia.mil (accessed: 30 November 2019).
7. Department of Defense, *Directive number 5105.60*, 29 July 2009.
8. Goldman J., *Words of Intelligence: An Intelligence Professional's Lexicon for Domestic and Foreign Threats*, second edition, Lanham – Toronto – Plymouth 2011.

9. Hayden M.V., *Playing to the Edge: American Intelligence in the Age of Terror*, New York 2016.
10. Herman M., *Potęga wywiadu*, Warszawa 2002.
11. Hulnick A.S., *The Dilemma of Open Sources Intelligence: Is OSINT Really Intelligence?*, [in:] *The Oxford Handbook of Natinal Security Intelligence*, L.K. Johnson(ed.), Oxford 2010.
12. "The Intelligence Community", http://www.intelligence.gov (accessed: 30 November 2019).
13. Intelligence Community Information Sharing Executive, *U.S. National Intelligence: an overview 2013*, 2013.
14. *Intelligence Reform And Terrorism Prevention Act of 2004*, Public Law 108–458 of December 17, 2004; 118 STAT. 3638.
15. Jensen C.J. III, McElreath D.H., Graves M., *Introduction to intelligence studies*, New York – London 2018.
16. Johnson L.K., *National Security Intelligence*, [in:] *The Oxford Handbook of National Security Intelligence*, L.K. Johnson (ed.), Oxford 2010.
17. Joint Publication 2-03, *Geospatial Intelligence in Joint Operations*, 2017.
18. Lowenthal M.M., *Intelligence. From secrets to Policy*, seventh edition, Thousand Oaks 2017.
19. Manget F.F., *Intelligence and Law Enforcement* [in:] *The Oxford Handbook of National Security Intelligence*, L. K. Johnson (ed.), Oxford 2010, pp. 189–211.
20. Minkina M., *Sztuka wywiadu w państwie współczesnym*, Warszawa 2014.
21. National Commission on Terrorist Attacks, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, http://www.9-11commission.gov/report (accessed: 30 November 2019).
22. *National Defense Authorization. Act for Fiscal Year 2006*, Public Law 109–163 of January 6, 2006; 119 STAT 3412.
23. National Intelligence for Policy, Plans, and Requirements, *National Intelligence. A consumer's guide*, 2009.
24. *National Intelligence Program*, http://obamawhitehouse.archives.gov/omb/factsheet_department_intelligence (accessed: 30 November 2019).
25. National Security Agency, *Frequently Asked Questions about Signals Intelligence (SIGINT)*, http://www.nsa.gov/about/faqs/sigint-faqs/ (accessed: 30 November 2019).

26. National Security Agency, *Support to the Military*, http://www.nsa.gov/what-we-do/support-the-military (accessed: 30 November 2019).
27. NATO Standardization Agency, *AAP-6(2014)*, 2014.
28. Office of Geospatial Intelligence Management, *Geospatial Intelligence (GEOINT) Basic Doctrine, Publication 1.0*, 2006.
29. Office of the Chairman of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, Washington DC 2019.
30. Office of the Director of National Intelligence, *Members of the IC*, https://www.dni.gov/index.php/what-we-do/members-of-the-ic (accessed: 30 November 2019).
31. Office of the Director of National Intelligence, *What is Intelligence?*, https://www.dni.gov/index.php/what-we-do/what-is-intelligence (accessed: 30 November 2019).
32. Office of the Director of National Intelligence, *Who we are*, http://www.dni.gov/index.php/who-we-are (accessed: 30 November 2019).
33. Richelson J.T., *The U.S. Intelligence Community*, Seventh Edition, New York – London 2018.
34. *United States Code*, http://uscode.house.gov (accessed: 30 November 2019).
35. Warner M., *Wanted: A Definition of "Intelligence". Understanding Our Craft*, „Studies in Intelligence", 2002, no. 46(3), pp. 15–22.
36. Wirtz J.J., *The Sources and Methods of Intelligence Studies* [in:] *The Oxford Handbook of National Security Intelligence*, L.K. Johnson (ed.), Oxford 2010, DOI 10.1093/oxfordhb/9780195375886.003.0004.

Cite this article as:

M.A. Kamiński, *Intelligence Sources in the Process of Collection of Information by the U.S. Intelligence Community*, "Security Dimensions", 2019, no. 32, pp. 82–105, DOI 10.5604/01.3001.0014.0988.