

Original article

Counteracting imagery (IMINT), optoelectronic (EOIMINT) and radar (SAR) intelligence

Krzysztof Wysocki* , Martyna Niewińska 

Faculty of Military Studies, War Studies University, Warsaw, Poland

email: k.wysocki@akademia.mil.pl; miki723@wp.pl

INFORMATION

Article history:

Submitted: 17 June 2021

Accepted: 28 September 2021

Published: 15 June 2022

ABSTRACT

The development of military technique and technology forces necessary changes in military reconnaissance using advanced methods of contemporary battlefield imaging. This paper addresses the topic of imagery intelligence as an essential source for gaining information about the deployment and quantity of means and forces of a potential enemy. Currently, armies of the world are equipped with modern imagery intelligence systems that make it possible to collect, process and analyse the collected data on enemy's troops and the environment in which the enemy operates. The purpose of the study is to present the proper role of camouflage undertakings that make it possible to counteract imagery, optoelectronic and radar intelligence. The increasing capabilities in this problem area mean that in the near future intelligence tasks will be carried out not only by ground, space or naval systems, but primarily by reconnaissance aircraft and unmanned aerial systems. In accordance with the problem indicated in the topic, the paper brings closer the possibilities of counteracting imagery intelligence from the theoretical and practical perspective. In addition, it presents the latest camouflage solutions employed both in the Polish Armed Forces and other selected armies. At the end of the paper, the authors formulate the most important conclusions that constitute a generalisation of the results of studies presented in different parts of the publication.

KEYWORDS

imaging, optoelectronic, radar intelligence, counteracting intelligence

* Corresponding author



© 2022 by Author(s). This is an open access article under the Creative Commons Attribution International License (CC BY). <http://creativecommons.org/licenses/by/4.0/>

Introduction

Since the beginning of the 21st century, when technological development significantly improved the techniques of capturing and transmitting images, imagery intelligence has undoubtedly been one of the most significant and reliable methods of obtaining information as a captured image also constitutes a proof of a given phenomenon, fact or event.

According to NATO doctrine AJP-2.7 [1], *Imagery Intelligence* (IMINT) is a type of intelligence that involves the acquisition of information with the use of imaging devices and systems. Imagery intelligence complements common operational picture (COP) and recognised

environmental picture (REP). It defines IMINT as an important element of the reconnaissance system that provides detailed and accurate information on the location, physical characteristics of threats, infrastructure and physical environment.

The imagery in question, as indicated by another NATO doctrine, AJP-2.6 [2], is obtained as a result of recording energy from a specific range of the electromagnetic spectrum. Different ranges of the spectrum – such as visible light, near infrared, thermal infrared, and the radio frequency spectrum – have different properties. Sensor orientation is a factor that has a significant impact on the quality, features and characteristics of the obtained images. Imagery sensor orientation has a significant impact on the quality, features and characteristics of the obtained images. Digital and analogue sensors (only with lower accuracy and quality) make it possible to obtain and process data in various ranges of the electromagnetic spectrum, enabling their instant display, collection and sharing.

The primary function of the intelligence in question is to create images of the surface of the Earth. This way, it is possible to control the location of the object as well as the surrounding area, buildings, vehicles and equipment. In addition, it is possible to obtain information on the movement of intelligence targets (objects), for example movements of the enemy army. This type of intelligence enables analysts to establish links between known intelligence targets and new objects, not taken into consideration before the image was captured [3].

For this purpose, we use optical tools, radars and lasers. Nowadays, IMINT mostly relies on satellite systems, reconnaissance aircraft, and unmanned aerial systems (UAS). Intelligence imagery has undoubtedly been one of the most important imaging sources for information retrieval, especially since the beginning of the 21st century, when technological development significantly improved the techniques of capturing and transmitting images.

Compared to other types of intelligence, such as human intelligence and open-source intelligence, IMINT:

- can be considered more accurate and detailed as the obtained data can be georeferenced and are based on physical features of objects/terrain,
- can be considered low-risk as it is controlled from areas outside the reach of the potential enemy,
- can be considered an objective source as the transmitted information (image) is to a greater extent based on facts,
- can be used to determine changes in the condition of an object/terrain over time,
- can be used and analysed in near-real time,
- can be used to determine models of environmental patterns,
- can be used to observe large-surface areas, of even global reach.

With the development of IMINT, the existing procedures are being refined and new technologies are being introduced to counteract imagery intelligence. The article presents the existing methods of counteracting object identification as well as the directions of development in this area, both in the Polish Army and armies of other countries.

1. Characteristics of imagery intelligence

When speaking of counteracting electrooptical imagery intelligence (EO IMINT) and synthetic-aperture radars (SAR), it is necessary to first refer to imagery intelligence itself in order to better understand the specificity of conducting intelligence and the purpose of its application.

The national doctrine – D-2(B) [4] – lists imagery intelligence as one of the methods of the broadly understood military intelligence. It also presents a division of the intelligence in question based on the range of the recorded electromagnetic energy into: electrooptical (EO), thermal and radar imaging as well as the light detection and ranging technology (LiDAR).

To complement the information provided the introduction it should be added that according to the above-mentioned doctrine D-2(B) [4]. Imagery intelligence is one of two types of geospatial intelligence (GEOINT), which is a term used to describe the ability to integrate data from imagery intelligence (IMINT) and secure geospatial intelligence (GEOINFO) data with other intelligence data.

Imagery intelligence also comprises the intelligence potential and the process of obtaining and processing information on the basis of environmental remote sensing method that uses data emitted and/or deflected by objects and the natural background, which then propagate in the atmosphere of the Earth, mainly in the visible band, infrared and, partially, in ultraviolet and radar ranges. According to the provisions of the NO-16-A001 standard [5], imagery intelligence stands for identification of data from image sources and is an intelligence method that consists in the processing of information using devices and imaging systems and images. For this purpose, we use optical tools, radars and lasers.

Imagery intelligence is a type of intelligence that uses techniques of remote retrieval of information about the surrounding reality that make it possible to present the collected data in the form of an image and then record them. Intelligence data come from photographic images, electrooptical, thermal, television and laser devices. The devices can be deployed on land, floating or airborne objects and in space. Information conveyed by means of imaging (an image or a film) is not distorted, objective and can be used to confirm data obtained via other intelligence methods [6].

According to the provisions of the DD-2.6(A) document [7], imagery intelligence information is obtained via satellites, reconnaissance aircraft and unmanned systems as well as television and photographic devices mounted on reconnaissance vehicles. Images can be acquired using military and/or civilian platforms. The platforms will be presented more broadly in the next subsection.

Imagery intelligence is a source of information used to:

- determine and monitor key physical characteristics of the terrain and changes occurring therein,
- gain situational awareness, identify elements of a combat grouping, obtain information on objects,
- conduct battle damage assessment (BDA) and assess the effectiveness of the weapons used,
- support the development of enemy courses of action (ECOAs).

It supports the process of decision making by commanders at all levels of command by:

- delivering a more complete and accurate picture of the current situation, thus reducing operational uncertainty,
- creating an analytical environment supporting the intelligence process by juxtaposing IMINT products with products of other intelligence methods, such as human intelligence, radioelectronic intelligence and open-source intelligence.

Electrooptical (EO) imagery is obtained by recording electromagnetic energy from the visible range or near infrared of the electromagnetic spectrum. The quality of the imaging may be

worse or it may be illegible due to smoke, dust, fog, vapour, clouds, rain, solar reflections, light intensity and the angle of illumination. Optoelectronic sensors are passive devices that record energy deflected from an object. In accordance with the aforementioned doctrine 2.6(A) [7], imaging can be conducted in the visible range or infrared, or as a multispectral, hyperspectral imaging.

Imaging in the visible range is created using sensors that process the visible range of the electromagnetic spectrum (in the wavelength range of 0.4-0.7 μm) and makes it possible to acquire colour or gray scale (panchromatic) images. Near-infrared imaging (in the wavelength range of 0.7-1.4 μm) involves recording deflected energy in the infrared wavelength range. To facilitate the analysis of imaging and identification of different types of objects when reading imaging in infrared, it is possible to use algorithms (pseudocolouring) that present the recorded energy on the imaging in different colours [8]. Infrared sensors are a valuable source of information at night and in situations when the level of illumination is very low, however, their use requires advanced technological tools, knowledge and training. Multi-spectral, hyperspectral imaging is obtained as a result of simultaneous imaging of the same area in different ranges of the electromagnetic spectrum.

Electromagnetic radiation that penetrates the atmosphere and is used in environmental remote sensing is presented in Table 1.

The advantages of optoelectronic imaging include the ability to distinguish anthropogenic objects from the natural environment (due to the use of the visible and infrared bands) and high resistance to jamming interference (due to its passive nature). Significant limitations of optoelectronic imaging include high susceptibility to adverse weather (fog, precipitation, etc.) and lighting conditions as well as its high potential for limiting the effectiveness of systems using one type of optoelectronic imaging by masking and simulating, e.g., using mock-ups of equipment.

Table 1. List of atmospheric windows, that is spectrum ranges in which solar electromagnetic radiation penetrates through the atmosphere to the Earth's surface and thus can be used to investigate objects on the surface of the Earth

Electromagnetic radiation range	Wavelength
Ultraviolet and visible	0.3-0.7 μm
Near infrared	0.7-0.91 μm
	1.00-1.12 μm
	1.19-1.34 μm
Mid-infrared	1.55-1.75 μm
	2.05-2.40 μm
Thermal infrared	3.35-4.16 μm
	4.50-5.0 μm
	8.0-9.2 μm
	10.02-12.4 μm
Microwaves	from 1 cm

Source: [8, p. 282].

Thermal imaging means imaging of infrared radiation in the wavelength range of 7-15 μm , which uses thermal radiation of any object (object) whose temperature is higher than absolute zero. This type of imaging uses the recording of the difference in emitted energy between the object and its surroundings [8]. This type of imaging makes it possible to obtain image information regardless of the time of the day and, as in the case of optoelectronic imaging, it is of passive nature which makes it difficult to jam. However, despite its advanced nature, it has its limitations. It is less useful when the temperature difference between the object and the background is small, or when the emissive power of the object and the background are similar.

In radar imaging, the active sensor is a radar that can acquire intelligence data regardless of the time of day and in almost any weather conditions. It takes advantage of the property which consists in the fact that all materials/substances deflect some of the electromagnetic radiation directed toward them. The distance from the radar antenna to the object can be measured by measuring the time that the radiated electromagnetic wave needs to reach the object and return. There are two types of radar imaging [9]:

- synthetic-aperture radar imaging (SAR). The SAR technique makes it possible to obtain radar images by using relative motion between the transmitting antenna and the receiving antenna (as the radar flies over the observed area, it sends probe signals and receives signal echo). Depending on the length of the radio wavelength (channel) used, the SAR technique makes it possible to penetrate some centers/objects (e.g. layers of vegetation, soil). With the use of additional analysis techniques, such as interferometry (e.g. consistent detection of changes), radar stereoscopy or polarimetry, it is possible to obtain even more intelligence data on the status and activity of a given object from this type of images,
- ground moving target indicator (GMTI). It is a type of imaging that uses the Doppler shift to distinguish stationary objects. Images are created on the basis of an analysis of a series of radar sweeps across an area, depicting the path of motion and making it possible to calculate velocity.

Radar imaging makes it possible to obtain data in adverse weather conditions, such as fog, vapour, clouds of smoke (it is, to a certain extent, limited by heavy precipitation and sand storms). It makes observation possible both during the day and at night [10]. One of its big advantages is the ease of detecting objects made of metal as well as moving objects (objects in motion) with the use of GMTI. It does have certain flaws, though. Weather conditions (space weather) can interfere with radar signals, causing the effect of erroneous feedback data and misdescription of objects. However, due to the fact that synthesised aperture radars are active devices that radiate electromagnetic energy, their most important limitation is the fact that they are relatively easy to detect and jam.

The last technology that will be described is LiDAR light detection and ranging technology (LiDAR). LiDAR technology makes it possible to generate high-resolution digital terrain layout representation products, DEM (digital elevation model) and DSM (digital surface model). When imaging the terrain surface, the LiDAR technology sensors use a laser impulse. LiDAR can be used to identify shoreline, changes in beach size, depth of shallow waterbodies (range of up to 50 m), analyse flood risk, determine water flow, generate DSM for built-up areas. Advantages and disadvantages of LiDAR imaging are the same as those of radar imaging, except for the fact that it is more susceptible to weather conditions [11].

Apart from the division presented above, we should also pay attention to the contemporary possibilities of conducting intelligence with the use of all kinds of night-vision tools [12].

Unlike night-vision goggles that only amplify visible light in passive mode or requiring additional illumination in active mode (infrared, IR), thermal imagers are passive devices and remain independent from external illumination, so they will work places with no light at all (such as caves), where night-vision would require additional, active illumination to generate any image. The same applies to conditions of limited visibility, such as fog, sandstorms or smoke. If a given shielding does not generate heat (as, for example, glass does), a thermal imaging device will provide us with an image of an object whose temperature is higher than the temperature of its surroundings – such as a human body or hot machine elements.

2. Intelligence image data acquisition platforms

Imagery intelligence is conducted with the use of various devices. According to document DD-2.6(A) [7], images can be obtained using military and/or civilian platforms, which include: satellites; manned aircraft and unmanned aerial systems; ships, submarines, and unmanned/autonomous marine systems; land vehicles and unmanned/autonomous ground systems; personal equipment. With the counteraction of imagery intelligence in mind, which is the subject of this paper, the main platforms used for imagery intelligence include reconnaissance satellites, manned aircraft and unmanned aerial systems.

Reconnaissance satellites move above the Earth at different altitudes and orbits, which include: the low Earth orbit (LEO), the medium Earth orbit (MEO), the geostationary orbit (GEO) as well as the highly elliptical orbit (HEO). Reconnaissance satellites in the low orbit are most commonly used for intelligence purposes. They move from pole to pole and pass the equator up to 28 times a day.

Manned aircraft and unmanned aerial systems have many advantages, such as flexibility of use and the possibility of getting close to a target. If damaged, they can be repaired quickly, which is not possible in the case of satellite systems. Today, unmanned aerial systems, which do not require a pilot in the machine, are beginning to play an increasingly important role in intelligence. UAS can be controlled remotely and perform tasks over large distances without risking the lives of the crew. These systems are currently used by most armies, both in strategic intelligence and direct actions at the tactical level. Table 2 presents classification of UAS that includes organisational levels to which devices in individual classes are assigned.

3. Imagery intelligence and how to counteract it – theory

Researchers from the War Studies University conducted a study investigating the range of possibilities of conducting activities associated with imagery intelligence of our troops by a potential enemy and the possibilities of counteracting said intelligence. The study involved military students participating in various forms of professional trainings in the academic year of 2019/2020. The main part of the research group consisted of officers from the Postgraduate Operational-Tactical Studies, Higher Staff Course, Higher Operational-Strategic Course and the improvement course entitled Operational Masking in the Polish Armed Forces). The rest were officers holding positions related directly to military intelligence issues.

Respondents who participated in the survey were directly or indirectly associated with tactical camouflage (as part of combat security), operational camouflage (participation in planning or specific undertakings in this field) and military intelligence, and were among those who participated in the educational process in the field of operational camouflage as part of the curriculum classes in studies and courses conducted at the Academy of Military Arts.

Table 2. UAS classification including organisational levels

Class	Category	Level	Ceiling [m]	Range [km]
Class 1 (under 150 kg)	Micro	Platoon	under 60	5
	Mini	Company	under 305	25
	Small	Battalion/ regimen	under 366	50
Class 11 (150-600 kg)	Tactical	Brigade	under 915	200
Class 111 (over 600 kg)	HALE – high altitude, (ceiling) long endurance	Strategic/ national	under 19,812	unlimited
	MALE – medium altitude (ceiling), long endurance	Operational/ theatre of operations (division/ corps)	under 12,192	unlimited

Source: [13, p. 12].

Analysing the results, the researchers sought to answer the following question: “what possibilities in terms of using platforms designed to obtain images are available to a potential enemy while conducting intelligence of our troops?”. Within the framework of the conducted empirical research, the researchers assessed the capabilities of a potential enemy in terms of conducting imagery intelligence of our armed forces. Respondents’ ratings, which enabled the results to be grouped into an appropriate summary, are illustrated in Figure 1.

The answers of the respondents presented in the chart (sum of percentage values of ranks 3 and 4) are highest for, respectively: manned aircraft – 92%, land vehicles and unmanned/autonomous ground systems – 89%, reconnaissance satellites – 85% each, unmanned aerial systems – 84%, ships, submarines, maritime unmanned/autonomous systems and personal equipment – 80%.

However, if only the “strongly agree” answer is considered, the order changes significantly in favour of aerial reconnaissance: manned aircraft – 56%, reconnaissance satellites – 55%, unmanned aerial systems – 48%, maritime vessels – 43%, other platforms – 39%.

Analysing the above-listed results, we can notice that currently, in time of peace, the armed forces of the Russian Federation have the ability to conduct aerial imagery intelligence, while during an armed conflict, when conducting sea or land operations, they will also use sea and land platforms.

In such event, to hinder said intelligence, it would be necessary to use means of radio-electronic warfare (RF) conduct combat against enemy intelligence devices; increase the potential of forces and means combating imagery intelligence sensor carriers, e.g. counterparts of satellite combat systems at low ceilings; introduce means of active jamming in the range of electromagnetic wave spectra; effectively implement all forms of camouflage, including primarily simulation and concealment at the tactical level and disinformation and protection of critical information in the information environment at higher levels.

In the next question, the respondents were asked to answer the following question: *What do you consider to be essential, in terms of the use of camouflage, including the needs and*

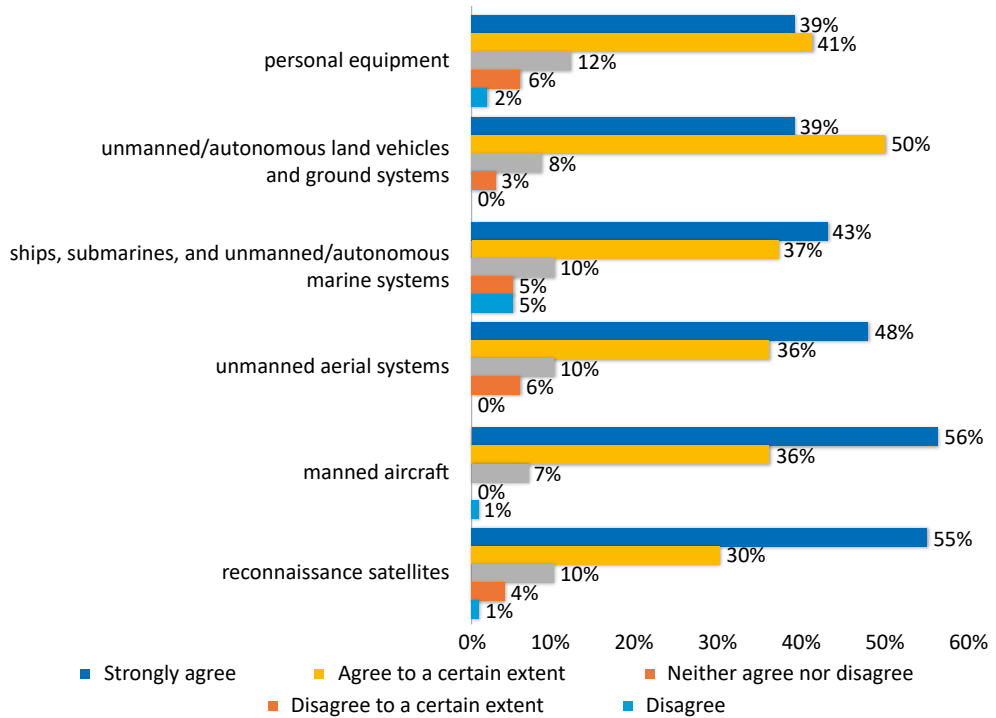


Fig. 1. Distribution of responses regarding the effectiveness of a potential enemy's intelligence platforms used to conduct imagery intelligence of our troops
Source: Authors' own elaboration.

capabilities of military camouflage and military defense infrastructure that you believe will enable hiding military capabilities from enemy intelligence.

The presented opinions of the respondents concern many areas associated with the possibility of applying camouflage for the purposes of protecting the troops and military defense infrastructure.

Based on the most frequently recurring responses, analysing the respondents' answers, the following needs and possibilities in the area of camouflaging troops and military defense infrastructure were distinguished:

- introduction of a large number of mock-ups simulating essential weapons to the equipment of the Polish Armed Forces and adaptation of structures to the possibility of carrying out tasks within the framework of camouflaging (e.g. establishment of camouflage subunits at the brigade and division level, wide application of multi-spectral camouflage nets),
- disinformation coordinated at all three levels (strategic, operational and tactical),
- creation of mock infrastructure facilities,
- creation of mock infrastructure at military airfields, mock command posts as well as mock locations of the troops, away from their actual location, including simulation (creation) of road runways,
- protection of classified information as well as not making everything available to the public on the Internet and via media. Reduction of soldiers' activity in the social

- media, including the possibility of blocking the Internet or introducing a “strict prohibition” on the use of cell phones, or at least blocking “data transfer” (sending photographs, location data) on cell phones,
- adequate awareness of soldiers regarding camouflage – training on military deception (MILDEC) and contemporary methods of conducting disinformation (reducing media coverage of the army, removing of hallmarks, conducting trainings with troops outside training grounds),
 - minimalisation of vehicle markings that reveal affiliation to a given formation,
 - use of civilian electronic networks and devices to mask the operation of electro-technical equipment,
 - planning operations in an unconventional manner so as to avoid creating identifiable indicators of tactics, techniques and procedures (TTP),
 - restricting access to areas immediately adjacent to military facilities; use of “dielectric domes” to shield radar and reconnaissance station antennas (similar to long-range Backbone radars that constitute part of NATO’s missile shield),
 - proper sequence of camouflaging: conducting disinformation, simulating exercises and areas of military and defense infrastructure deployment, concealing actual movements and regions,
 - developing close interconnection between operations conducted in the physical domain and cyberspace, and the ability to achieve camouflage capabilities by means of electronic warfare and cybersecurity assets,
 - use of active jamming means in different electromagnetic wave ranges as well as comprehensive use of the available means of camouflage (camouflage undertakings).

Based on the list of answers provided above, we can conclude that the respondents are aware of the limitations and shortages in the means of camouflage of both the troops and the military defense infrastructure.

In order to present prospective solutions in the area of the research, the respondents were asked to answer another question: *can you indicate the directions and solutions that should be pursued in order to ensure effective protection against enemy imagery intelligence?*

According to the respondents, examples of solutions include:

- developing structures and procedures for establishing camouflage subunits, equipping the troops with adequate means, disseminating camouflage in all types of troops, universality of new-type camouflage nets in systems of various colours,
- modern mock-up modules and developed procedures for their employment and maintenance,
- educating all soldiers on camouflage in various forms of in-service training, as well as planning and organising exercises on the subject at the operational and tactical level,
- making use of conclusions drawn from the experience gained during exercises and contemporary armed conflicts,
- at the tactical level – obtaining equipment for optoelectronic camouflage, full-time equipment and forces for apparent facilities, establishing full-time units responsible for camouflage,
- developing a system that enables the implementation of disinformation tasks,
- using analogue devices, which are less susceptible to jamming,

- developing a smoke screen system for the troops and facilities,
- anti-access weapons in all domains, especially aerial,
- ensuring means of camouflage that provide complete electromagnetic cover,
- with today's advances in technology, ensuring protection against imagery intelligence is extremely difficult, if not impossible. Undoubtedly, we should be striving to develop disinformation, although satellite intelligence prevention – i.e. the ability to use weather and nighttime conditions as well as jamming of satellites – seems to be of the greatest importance,
- developing procedures and implementing solutions that will make it possible to take over and control unmanned objects,
- it is necessary to intensify research and then employ anti-drone systems as well as the SSA (space situational awareness) and SST (space surveillance and tracking) system in the Polish Armed Forces. These programmes are carried out within the framework of the European Space Agency, which Poland has recently joined. In the future, they may make it easier for the Polish Armed Forces to avoid being infiltrated by foreign satellites,
- introducing (becoming capable of) means of active jamming within the range of light waves. Using mock-ups of combat equipment imitating a given object in various ranges of electromagnetic wave (light wave and radar range),
- passive counteraction – introducing new camouflages while simultaneously conducting research on the basis of spectral characteristics obtained using methods of predetection.

As the results presented above show, there is a significant need for changes in the area related to counteracting IMINT. The results also indicate that the possibilities of camouflage with regard to counteracting enemy's imagery intelligence are limited. The Polish Armed Forces have only begun the introduction of some of the presented directions of development.

4. Imagery intelligence and possibilities in terms of counteracting imagery intelligence – practical aspect

In today's combat environment, there are many ways to limit the process of information gathering through IMINT. That said, the procedures and methods aimed at reducing the susceptibility to imagery intelligence which are being developed are not always able to keep up with the modern and quickly implemented recognition systems.

Of course, methods for countering imagery intelligence at the tactical level are constantly being developed; they are aimed primarily at providing the means to reduce the effectiveness of sensors used in imagery intelligence.

The primary method for counteracting IMINT in combat operations is broadly defined military deception, which includes concealing troops and defence infrastructure from enemy intelligence and misleading the enemy as to the actual position of troops and the intent of ongoing operations [14].

An analysis of literature on the subject shows that military deception activities can be carried through the following forms (methods): concealment, simulation and disinformation. In turn, the DD-3.31(A) document [15] defines, on the basis of NATO doctrinal solutions, three forms: disinformation, simulation and concealment as well as protection of critical information in

the information environment [16]. Figure 2 presents the classification of military deception found in literature on the subject.

Considering the mode of action as the criterion for the classification of deception tactics, according to the views of the United States Army, we can distinguish [18]:

- diversion – the act of drawing the attention of an enemy from the point of principal operation of your own forces; the goal is to induce the enemy to concentrate its forces and means at a time and place that is advantageous from the perspective of your own forces,
- feint – an offensive action involving contact with the enemy conducted for the purpose of deceiving the enemy as to the location and time of the actual main offensive action of own forces. A series of such actions can condition the enemy to react ineffectively to a future main attack in the same area,
- demonstration – a show of force similar to a feint but without actual contact with the enemy, in an area where a decision is not sought that is made to deceive the enemy,
- ruse – an action designed to deceive the enemy, usually involving the deliberate exposure of false information to the enemy’s intelligence collection system. A ruse is typically an action based on guile or trickery that contributes to the larger deception plan,
- display – a static portrayal of an activity, force, or equipment intended to deceive the enemy’s visual intelligence collection systems. It involves displaying capabilities, equipment or subunits that do not actually exist.

Ways to counteract intelligence conducted in the visible radiation spectrum include classic methods of deception and concealment as well as disinformation activities. The means commonly used by all armies in the world are camouflage covers for equipment and individual camouflages for soldiers.

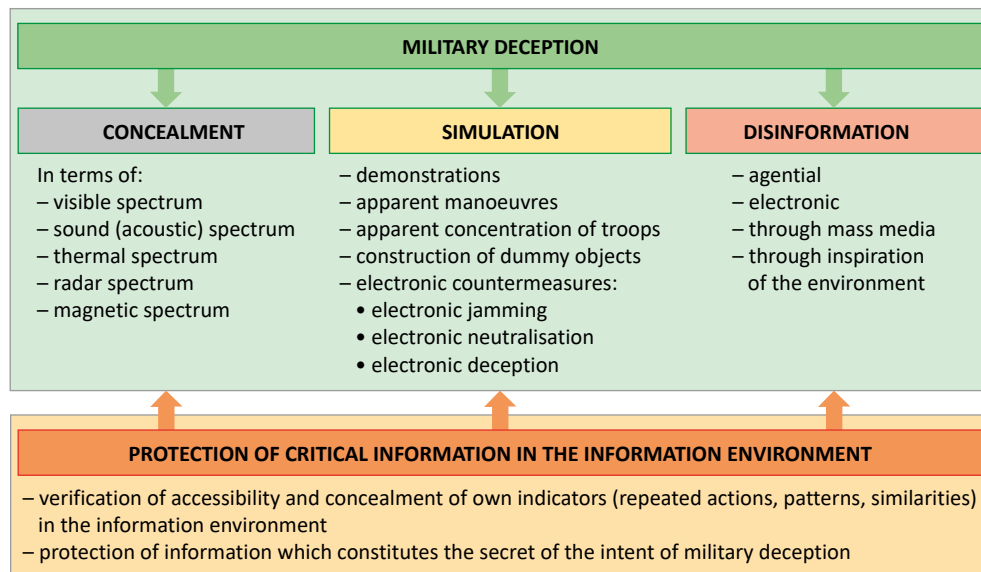


Fig. 2. Classification of military deception found in literature on the subject
 Source: [17, p. 33].

Particular attention should be paid to counteracting intelligence conducted in the infrared radiation spectrum. The methods and means being developed are aimed at hiding the thermal signature from the enemy or reducing it enough to increase the chance that the enemy will ignore it.

The primary methods which can limit the heat signature of a soldier or equipment in both land and air reconnaissance include:

- daytime camouflage – hiding in the shadows of buildings or trees. Using dense forests as a natural means of camouflage,
- nighttime camouflage – hiding, if possible, in structures or under the cover of trees or vegetation. Limiting the use of light to a minimum,
- thermal camouflage – using infrared shielding covers,
- carrying out operations in weather conditions which limit the enemy's ability to use flying objects (especially unmanned flying objects),
- keeping wireless communication to an absolute minimum.

However, due to high capabilities of imagery intelligence systems, actions aimed at deceiving the enemy are much more effective. These actions involve the use of dummy objects, such as mock-ups of weapons and military equipment.

Dummy objects are an important element of camouflage which significantly helps in the attempts to deceive the enemy. The effectiveness (believability) of the system is much higher if dummy objects which simulate basic military equipment are supplemented with general purpose elements (soldiers, people, terrain elements, etc.) and mobile dummy objects which make it possible to carry out apparent subdivision manoeuvres.

Mock-ups fully simulate real vehicles with respect to optical, thermal and radar detection. In addition, their thermal spectrum can be controlled to simulate the increased heat level of various vehicle components due to driving or their cool down during a stop.

The mock-ups should fully simulate individual pieces of combat equipment over a wide range of electromagnetic radiation, i.e. in the visible, radar and thermal spectra. They are typically made of plastic or rubber. These mock-ups should ensure faithful simulation of the equipment and be quick to set up and dismantle.

In Poland, mock-ups are manufactured by LUBAWA S.A. Its military offer includes mock-ups of the ROSOMAK wheeled armoured personnel carrier and the T-72 tank.

One such solution is a pneumatic mock-up of the ROSOMAK wheeled armoured personnel carrier (see Fig. 3), which is designed to simulate a single object or a grouping of military equipment in mixed (mock-ups and actual equipment) and dummy (mock-ups only) areas. The mock-up simulates the equipment over a wide range of the electromagnetic radiation spectrum (see Fig. 4) used in intelligence, i.e. in the scope of optical, thermal, radar and radio detection, to deceive the enemy. The pneumatic dummy ROSOMAK wheeled armoured personnel carrier is made of flexible materials and technical textiles and achieves its target shape by inflation with air until appropriate positive pressure of the pneumatic structure is reached.

The pneumatic mock-up of a T-72 tank (see Fig. 5) is designed to simulate a single object or a grouping of military equipment in mixed (mock-ups and actual equipment) and dummy (mock-ups only) areas. It simulates the equipment over a wide range of the electromagnetic radiation spectrum used in reconnaissance, i.e. in the scope of optical, thermal, radar and radio detection, to deceive the enemy.



Fig. 3. Pneumatic mock-up of a ROSOMAK wheeled armored personnel carrier
Source: Lubawa S.A. information materials.

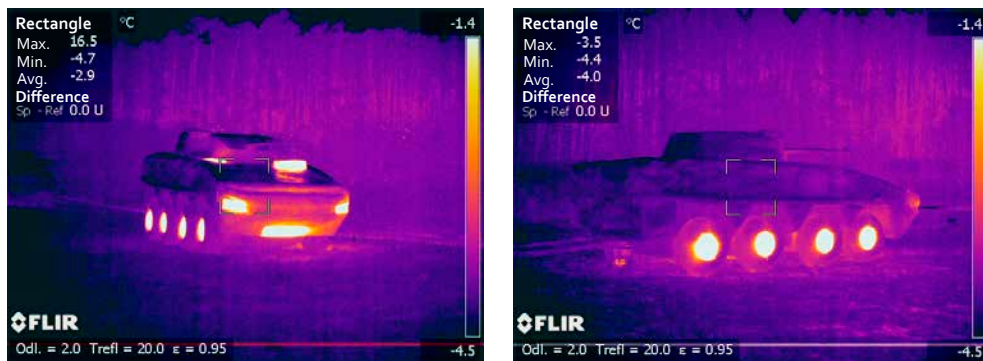


Fig. 4. Visibility of a mock-up ROSOMAK wheeled armored personnel carrier in thermal reconnaissance
Source: Lubawa S.A. information materials.



Fig. 5. A pneumatic T-72 mock-up
Source: Lubawa S.A. information materials.

The pneumatic T-72 tank mock-up is made of flexible materials and technical textiles and achieves its target shape by inflation with air until appropriate positive pressure of the pneumatic structure is reached. The set consists of the following components: a pneumatic frame, an outer cover with camouflage and optionally with features related to radar detection, a thermal system, a radio assembly and stabilising elements.

The mock-up reproduces the shape, together with characteristic elements, of the actual tank. It is also covered with a permanent camouflage made with special camouflage paints used for masking military equipment.

When observed from the ground with unaided eye or with optical and night vision systems, the mock-up is seen as real equipment at the visual recognition distance, while in thermal recognition it is seen as real equipment at a distance of 1000 m (see Fig. 6). The mock-up has a radar signature which enables it to be detected in the field by radar systems.

Camouflage systems for the Russian Armed Forces are manufactured by the Research and Manufacturing Company (NPP) Rusbal seated in Moscow. It primarily manufactures mock-ups of vehicles, aircraft, rocket launchers and anti-aircraft systems (in marching and combat positions) as well as mock-ups of camouflaged military equipment (see Fig. 7).

These Mock-ups are equipped with corner reflectors which imitate radar echoes of actual equipment deployed on the ground as well as radio and thermal emitters which imitate the radio and thermal signatures of equipment powered by internal combustion generators. Each mock-up can be set up within 60 minutes by a team of four people. The life of a mock-up is 5 years or 50 setting up/dismantling cycles. Operating temperature limits are between -20°C and $+50^{\circ}\text{C}$.

An additional element which increases the realism of dummy objects is electronic decoys. Russians have developed a series of radio communications simulators which reproduce the signs of radio communications operations, which is meant to mislead electronic intelligence systems (see Fig. 8). These can also be combined with other mock-ups, creating e.g. fake command posts or apparent areas of troop concentration observable by the entire spectrum of intelligence systems.

No Land Forces vehicle can be given the characteristics of “undetectability” – a running (and therefore heated) drive system will always be a revealing factor, as will the engine exhaust fumes. Actions are thus aimed at limiting the detection range and making it more difficult to

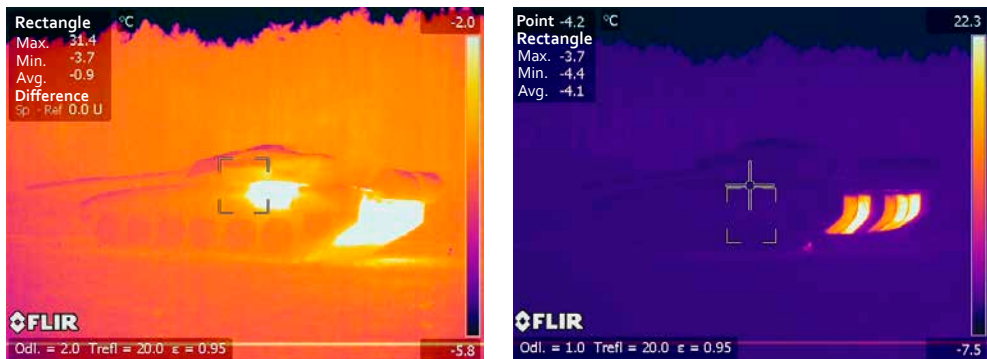


Fig. 6. Visibility of a mock-up T-72 tank in thermal recognition

Source: Lubawa S.A. information materials.



Fig. 7. Mock-ups of an aircraft, a tank, a rocket launcher and a camouflaged anti-aircraft system at the disposal of the camouflage subunits of the Russian Armed Forces
Source: [19].



Fig. 8. Electronic dummy objects combined with 3D mock-ups and corner reflectors allow for a more realistic simulation of command systems at the tactical level
Source: [20].

identify the object. Actions aimed at limiting vehicle detectability can be divided into design solutions and camouflage systems. Certain components are particularly visible in thermal imaging: exhaust fumes, heated engine compartment, drive system elements, a working filtration and ventilation system, working cannon stabilisation systems. One feature of newly designed military vehicles aimed at reducing their thermal detectability is to place the exhaust system low and direct the exhaust fumes at an angle towards the ground, which is meant to promote their dispersion (see Fig. 9). Such solution was ultimately used in the German PUMA infantry fighting vehicle, significantly reducing the thermal spectrum of its exhaust fumes.

While design solutions aimed at reducing detectability have only been implemented in the current decade, multi-spectral camouflage systems are older and date back to the 1980s. The primary element is an appropriate paint coating for military equipment, which not only protects against visual recognition, but also conceals the vehicle in night vision (e.g. the coating of the Leopard 2A5 tank currently used by the Polish Armed Forces).

The Polish Army also uses polyamide covers for vehicles and tanks as well as BERBERYS multi-spectral camouflage nets. The former, unfortunately, no longer provide adequate shielding characteristics due to material of which they are made – polyamide, which means that they have insufficient infrared properties, are not very resistant to weather conditions and quickly become heated in sunlight.

The Polish Armed Forces use two types of multi-spectral camouflage systems for protecting equipment and armaments against optical, thermal and radar detection. These are the BERBERYS camouflage net and the BERBERYS-S winter version, which are systematically supplied to operational forces. Their masking capabilities in terms of protection against optical, thermal and radar detection include the visible and near-infrared spectrum at wavelength range of 0.38×10^{-6} to 1.2×10^{-6} m, the thermal spectrum at wavelength range of 3×10^{-6} to 14×10^{-6} m and the radar spectrum at wavelength range of 3×10^{-3} m to 1.2×10^{-1} m [22] (see Fig. 10).



Fig. 9. A Puma infantry fighting vehicle which utilises a solution involving low placement of the exhaust system and dispersion of the heated exhaust fumes towards the ground

Source: [21].

Figure 11 shows the infrared visibility of a truck concealed using the BERBERYS multi-spectral camouflage.

Equipment and facilities concealed using the BERBERYS multi-spectral camouflage net cannot be recognised with unaided eye in field conditions when observed from the ground or from the air at a distance or height of 1000 m or more and in photographic images taken at a scale of 1:5000 or lower at linear resolution of 20 lines per mm. In terms of temperature difference recognition, the camouflage reduces the effectiveness of thermal recognition by deforming the object’s thermal image, changing the spatial characteristics of radiation and reducing the temperature difference between the camouflaged object and the background to 4°C [22].

Virtually all tracked vehicles and modern combat vehicles have camouflage (smoke) grenade launchers. In the most advanced solutions, they are bundled into an active vehicle protection system (AVePS). Smoke screen systems implemented in Israel, South Korea and Germany have additional radar or infrared-ultraviolet detectors which enable detection of passively-guided anti-tank missiles.

The latest solutions used by the Russian Federation show that this way of “dealing” with enemy observation is becoming increasingly effective and necessary on the modern battlefield. During recent exercises, Russian troops tested an automated command system, which includes a camouflage control subsystem. Its purpose is to conceal airfields, facilities and areas of unit concentration using smoke screens. This automated control system combines electronic warfare equipment with special machines for creating smoke clouds. The system first detects how enemy intelligence is tracking troops: via aircraft, drones or satellites. It then gives the command to perform protective action appropriate to the detected threat, which provides effective cover against terrestrial, aerial and spatial reconnaissance as well as targeting by precision weapons of all kinds. Smoke screen deployment systems, depending on the situation, make it possible to cover a given area in smoke. Intelligence capabilities of unmanned aerial systems will be disrupted by a conventional smoke screen (see Fig. 12).

If the enemy is found to conduct radar reconnaissance, reflective dipoles which reflect radar signals are scattered in the air. That way, instead of silhouettes of helicopters or tanks, the enemy sees “snow” on its radar screens. In addition, special chemical fillers (substances),

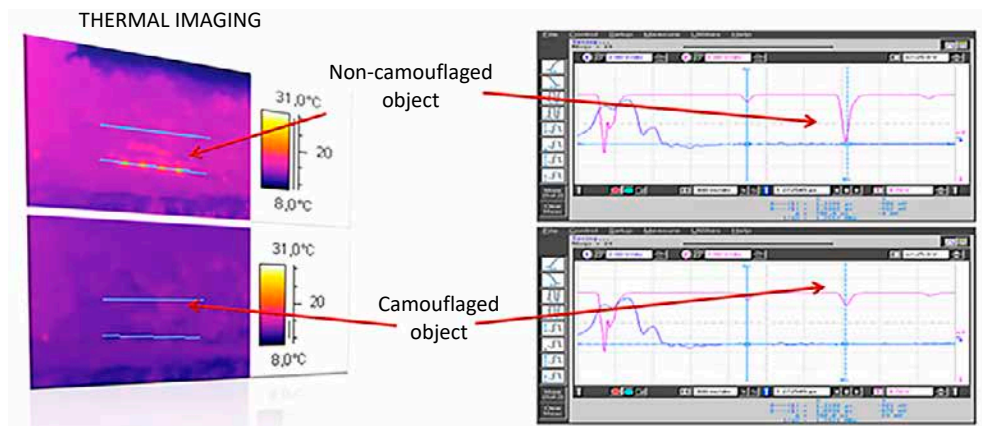


Fig. 10. Reduction in thermal signature of a combat vehicle achieved through the use of the BERBERYS multi-spectral camouflage
 Source: Lubawa S.A. information materials.

most likely containing carbon particles, which make it impossible to observe troops and equipment using thermal imaging cameras, can also be used. Finally, there are also aerosols, which, together with smoke, prevent the effective use of state-of-the-art weapons, including manoeuvring missiles with laser-guided warheads [23].

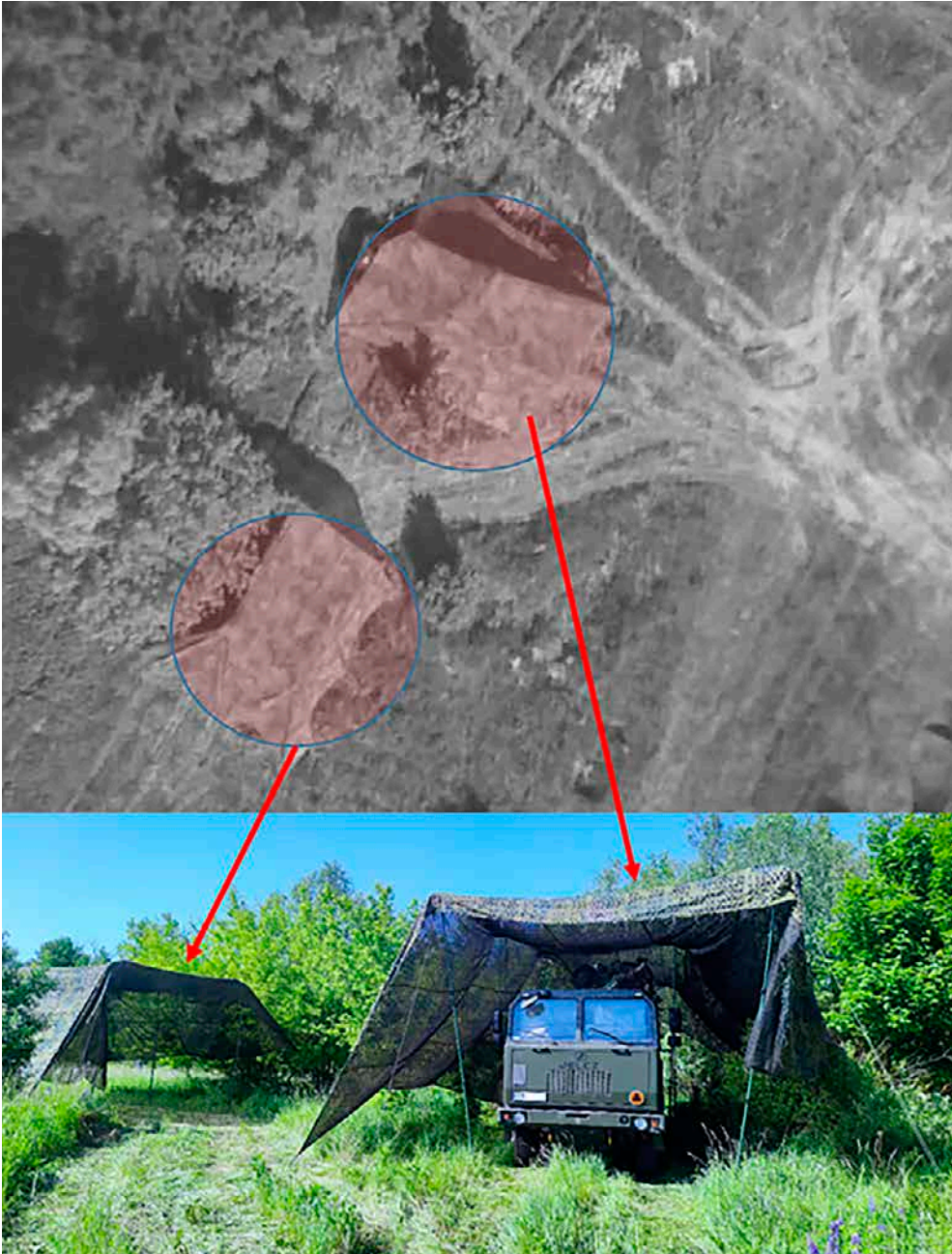


Fig. 11. Infrared visibility of a truck under the BERBERYS multi-spectral camouflage net
Source: Authors' own elaboration.



Fig. 12. One of the components of an automated control system, designed for deploying a smoke screen
Source: [24].

Conclusions

One of the advantages of IMINT is that it enables ongoing analysis of received information, as the obtained material is an up-to-date evidence of the occurrence of a given fact or event, acquired directly and not subject to falsification. This can speed up the decision-making process and prevent the consequences of late responses to the situation.

A breakthrough of sorts in the field of imagery intelligence is the use of unmanned systems which nullify the risk of loss of life, e.g. of a crew of a traditional reconnaissance aircraft. This has increased the flexibility of use and reduced the cost of IMINT, which is high for satellite systems.

Imagery intelligence systems which provide real-time information to a potential enemy, coupled with the capabilities of its firepower, both in terms of speed of fire response and the ability to perform precision strikes, make the issue of counteracting imagery intelligence one of the key elements of the military survival system. To increase the effectiveness of protection of troops and facilities of the Polish Armed Forces, it is necessary to strive towards using military and technological means of preventing IMINT.

The constantly increasing capabilities of imagery intelligence systems will force changes in the scope of passive camouflage of equipment and soldiers. This means moving away from traditional camouflage nets and individual camouflage, such as face painting or camouflaging via hand-held means. Their ever-decreasing effectiveness will force the proliferation of multi-spectral camouflage techniques which hinder detection by modern sensors.

As the development of camouflaging systems is reactive in nature, i.e. the development of new camouflaging techniques is a response to new intelligence systems, it is always “a step behind”. For this reason, deception and diversion tactics constitute a very important part of military protection system operations, as they partially offset this unfavourable state of affairs.

In the Polish Armed Forces, deception tactics using mock-ups of equipment seem underestimated. The high effectiveness of such tactics was demonstrated e.g. by the war in Kosovo (NATO Operation "Allied Force"), where Serbian forces deployed en masse fake vehicle columns and artillery positions using decommissioned equipment, which largely contributed to the fact that Serbian losses due to bombing, despite numerous reports on detection and destruction of Serbian forces and installations, were in reality minimal [25].

The constantly increasing imaging capabilities make it impossible to completely protect troops against detection on the modern battlefield. Detection can, however, be limited. But this cannot be done by relying e.g. solely on passive systems. Increasing the ability to prevent the detection of troops, facilities and infrastructure by an enemy conducting imagery intelligence requires creation of a coherent system based on actively fighting platforms which carry imaging equipment, equipping subunits with modern passive camouflage means and using deception and diversion tactics extensively. Although it entails high costs and poses a significant technological challenge, protection against imagery intelligence is a necessary condition for the army to be able to fight and survive on the modern and future battlefield.

Acknowledgement

No acknowledgement and potential founding was reported by the authors.

Conflict of interests

All authors declared no conflict of interests.

Author contributions


All authors contributed to the interpretation of results and writing of the paper. All authors read and approved the final manuscript.

Ethical statement

The research complies with all national and international ethical requirements.

ORCID

Krzysztof Wysocki  <https://orcid.org/0000-0002-0527-6976>

Martyna Niewińska  <https://orcid.org/0000-0001-6921-4320>

References

1. *Allied Joint Doctrine for Joint Intelligence, Surveillance, and Reconnaissance. AJP-2.7*. North Atlantic Treaty Organization, Allied Joint Publication; 2014.
2. *Allied Joint Doctrine For Imagery Intelligence. AJP-2.6*. North Atlantic Treaty Organization, Allied Joint Publication; 2018.
3. Sabała J. *Rozpoznanie obrazowe w systemie wywiadu strategicznego*, [online]. Portal infosecurity24.pl. Available at: <https://www.infosecurity24.pl/rozpoznanie-obrazowe-w-systemie-wywiadu-strategicznego> [Accessed: 10 May 2021].
4. *Doktryna Rozpoznanie Wojskowe D-2*. Warszawa: Sztab Generalny Wojska Polskiego; 2013.
5. *NO-16-A001. Lotnicze rozpoznanie obrazowe i aparatura rozpoznawcza – Terminologia*. Warszawa: Wojskowe Centrum Normalizacji, Jakości i Kodyfikacji; 2017.
6. Roślan G. *Wybrane problemy automatyzacji w kontekście powietrznego rozpoznania obrazowego*. *Zeszyty Naukowe Akademii Obrony Narodowej*. 2010;4(81):148-66.

7. *Doktryna Rozpoznanie Obrazowe DD-2.6(A)*. Bydgoszcz: Centrum Doktryn i Szkolenia Sił Zbrojnych; 2019.
8. Zawila-Niedźwiecki T. *Teledetekcja i fotogrametria obszarów leśnych*. In: Okła K (commissioning editor). *Geomatyka w Lasach Państwowych. Część I. Podstawy*. Warszawa: Centrum Informacyjne Lasów Państwowych; 2010, p. 277-98.
9. Baumgartner SV, Krieger G. *Multi-Channel SAR for Ground Moving Target Indication*. In: *Academic Press Library in Signal Processing. Vol. 2. Communications and Radar Signal Processing Academic Press Library in Signal Processing*. Elsevier; 2013, p. 911-86. DOI: 10.1016/B978-0-12-396500-4.00018-1.
10. Królikowski J. *Od GMES do Sentineli*, [online]. Portal geoforum.pl. Available at: <https://geoforum.pl/teledetekcja/sentinel> [Accessed: 16 May 2021].
11. Reutebuch SE, Andersen HE, McGaughey RJ. *Light Detection and Ranging (LIDAR): An Emerging Tool for Multiple Resource Inventory*. *Journal of Forestry*. 2005;103(6):286-92. DOI: 10.1093/jof/103.6.286.
12. Gryga M. *Izraelskie wojska specjalne*. *Przegląd Wojsk Lądowych*. 2021;3:140-50.
13. Przekwas A, Jaroszuk R. *Bezzałogowe statki powietrzne w rozpoznaniu wojskowym*. *Przegląd Wojsk Lądowych*. 2009;7:9-15.
14. *Instrukcja maskowania w Siłach Powietrznych*. Warszawa: Dowództwo Sił Powietrznych; 2013.
15. *Maskowanie operacyjne DD-3.31(A)*. Bydgoszcz: Centrum Doktryn i Szkolenia Sił Zbrojnych; 2018.
16. *Allied Joint Doctrine for Operations Security and Deception AJP-3.10.2. Edition A Version 2*. Allied Joint Publication; 2020.
17. Wysocki K, Dąbrowska I, Idziek M. *Maskowanie wojsk i obiektów na przykładzie doświadczeń wybranych państw*. Warszawa: Wydawnictwo Akademii Sztuki Wojennej; 2020.
18. *Military Deception. JP 3-13.4*. Joint Publication. Joint Forces Staff College. January 2012.
19. [online]. Available at: <https://www.rusbal.ru/o-maskirovke/> [Accessed: 22 May 2021].
20. [online]. Available at: <https://www.rusbal.ru/imitacia> [Accessed: 22 May 2021].
21. [online]. Available at: <https://www.monch.com/mpg/news/land/1826-puma2.html> [Accessed: 15 June 2021].
22. *Wielozakresowe pokrycie maskujące BERBERYS*, [online]. Available at: <https://www.lubawa.com.pl/pl/kamuflaz-i-pozoracja/kamuflaz-statyczny/wielozakresowe-pokrycie-maskujace-berberys> [Accessed: 16 June 2021].
23. Ramm A, Stepovoy B. *Dym v Otechestvo: armiyu spryachut ot shpionov v aerazol'nykh oblakakh*, [online]. Available at: <https://iz.ru/976360/aleksei-ramm-bogdan-stepovoi/dym-v-otechestvo-armiiu-spriachut-ot-shpionov-v-aerazolnykh-oblakakh> [Accessed: 17 June 2021].
24. [online]. Available at: <https://vpk.name/file/img/dym-v-otechestvo-armiyu-spryachut-ot-shpionov-v-aerazolnykh-oblakah-wo0jgrzx-1583790061.jpg> [Accessed: 17 June 2021].
25. *Report to Congress: Kosovo/Operation Allied Force After-Action Report*. Washington: Department of Defense; 2000.

Biographical note

Krzysztof Wysocki – Colonel, PhD, Associate Professor at the War Studies University. Areas of professional and research interest of the Author are mainly related to theory and practice of military engineering, including issues concerning the principles of organisation of engineering operations, operational tactics of military engineers, command of military engineering units and subunits and the unique nature of performance of engineering tasks in various environmental conditions. The Officer's interests also include areas related to issues concerning planning, directing and organising military deception at the operational and tactical levels. He has also authored and co-authored numerous publications whose substantive value has been repeatedly acknowledged both at his alma mater and outside the University, in military

units. Academic achievements of Krzysztof Wysocki, Doctor Habilitatus, include over 30 publications, comprising both independent and joint studies in the field of military engineering and information technology in Polish and in English, e.g.: K. Wysocki, I. Dąbrowska, M. Idziek, *Maskowanie wojsk i obiektów na przykładzie doświadczeń wybranych państw (Camouflaging of Troops and Structures on the Example of Selected countries)*, Akademia Sztuki Wojennej: Warszawa, 2021; K. Wysocki, *Planowanie działań inżynierskich z wykorzystaniem technologii informatycznych (Planning of Engineering Operations with the Use of Information Technology)*, Akademia Sztuki Wojennej: Warszawa, 2019; K. Wysocki, *Inżynierska ocena środowiska na potrzeby kierowania działaniami inżynierskimi (Engineering Assessment of the Environment for the Purposes of Directing Engineering Operations)*, Akademia Sztuki Wojennej: Warszawa, 2018; S. Kowalkowski, W. Kawka, K. Wysocki (eds.), *Lądowy wymiar pokonywania przeszkód wodnych przez wojska lądowe w działaniach taktycznych (The Land Dimension of Overcoming Water Obstacles by Ground Troops in Tactical Operations)*, Akademia Sztuki Wojennej: Warszawa, 2018; K. Wysocki, M. Depczyński, P. Szymczak, *Współczesne wojska Inżynierskie Federacji Rosyjskiej (Contemporary Engineering Forces of the Russian Federation)*, Akademia Sztuki Wojennej: Warszawa, 2017; K. Wysocki, W. Więcek, M. Ochalski, *Modern Approach to Tactical Activities*, Akademia Obrony Narodowej: Warszawa, 2017; K. Wysocki, W. Więcek, M. Ochalski, *Land Forces in Contemporary Operations*, Akademia Obrony Narodowej: Warszawa, 2015; K. Wysocki, *Wybrane narzędzia informatyczne wspomagające planowanie działań inżynierskich (Selected IT Tools which Support the Planning of Engineering Operations)*, Akademia Obrony Narodowej: Warszawa, 2014; W. Kawka, K. Wysocki, *Inżynierskie dokumenty dowodzenia (Engineering Command Documents)*, Akademia Obrony Narodowej: Warszawa, 2014; W. Kawka, K. Wysocki, *Ocena inżynierska potencjału wykonawczego Sił Zbrojnych Rzeczypospolitej Polskiej (Engineering Evaluation of the Performance Capacity of the Polish Armed Forces)*, Akademia Obrony Narodowej: Warszawa, 2011.

Martyna Niewińska – MSE, graduate of a Master's degree course in Defence Studies at the Faculty of Military Studies of the War Studies University. Areas of professional and research interest of the Author are mainly related to military intelligence, especially the issues of intelligence operations and the operation of intelligence forces and means. Her research addresses selected issues in the field of air imagery intelligence. She authored the publication titled *Współczesne uwarunkowania prowadzenia rozpoznania obrazowego (Contemporary Considerations for Conducting Imagery Intelligence)*, which was published in the *Przegląd Sił Zbrojnych (Armed Forces Review)* No. 3/2020 in 2020. She won 2nd place in the Dean of the Faculty of Military Studies competition for the best thesis in the 2019/2020 academic year.

Przeciwdziałanie rozpoznaniu obrazowemu (IMINT), optoelektronicznemu (EOIMINT) i radarowemu (SAR)

STRESZCZENIE

Rozwój techniki i technologii militarnej wymusza konieczne zmiany w prowadzeniu taktyki rozpoznania wojskowego z użyciem zaawansowanych środków zobrazowania współczesnego pola walki. W niniejszym artykule poruszono tematykę rozpoznania obrazowego jako kluczowego źródła zdobywania informacji o rozmieszczeniu oraz ilości posiadanych sił i środków potencjalnego przeciwnika. Obecnie armie świata wyposażone są w nowoczesne systemy rozpoznania obrazowego pozwalające na realizację gromadzenia, przetwarzania i analizowania zgromadzonych danych o wojskach własnych przeciwnika i środowisku, w jakim prowadzi działania. Przeznaczeniem opracowania jest przedstawienie właściwej roli przedsięwzięć z zakresu maskowania, umożliwiających przeciwdziałanie rozpoznaniu obrazowemu, optoelektronicznemu

oraz radarowemu. Zwiększające się możliwości w przedmiotowym obszarze problemowym powodują, że w najbliższej przyszłości spectrum zadań rozpoznawczych realizowane będzie już nie tylko przez systemy naziemne, kosmiczne czy też morskie, ale przede wszystkim przez samoloty rozpoznawcze oraz bezałogowe systemy powietrzne. Zgodnie z zaproponowaną w temacie problematyką przybliżono możliwości przeciwdziałania rozpoznaniu obrazowemu w aspekcie teoretycznym i praktycznym. Ponadto zaprezentowano najnowsze rozwiązania z obszaru maskowania zarówno w Siłach Zbrojnych Rzeczypospolitej Polskiej, jak i w innych wybranych armiach świata. Na końcu artykułu podane są najważniejsze wnioski, stanowiące uogólnienie wyników badań zawartych w poszczególnych częściach publikacji.

SŁOWA KLUCZOWE rozpoznanie obrazowe, optoelektroniczne, radarowe, przeciwdziałanie rozpoznaniu

How to cite this paper

Wysocki K, Niewińska M. *Counteracting imagery (IMINT), optoelectronic (EOIMINT) and radar (SAR) intelligence*. Scientific Journal of the Military University of Land Forces. 2022;54;2(204): 222-44. DOI: 10.5604/01.3001.0015.8975.



This work is licensed under the Creative Commons Attribution International License (CC BY).
<http://creativecommons.org/licenses/by/4.0/>