Received: 7. 3. 2018 Accepted: 5. 4. 2018 Published on-line: 15. 6. 2018
Available from: www.obranaastrategie.cz doi: 10.3849/1802-7199.18.2018.01.113-130

INFORMAČNÍ OPERACE Z POLSKÉ PERSPEKTIVY

INFORMATION OPERATIONS FROM THE POLISH POINT OF VIEW

Zbigniew Modrzejewski[a]

Abstrakt

Informační operace stále nejsou dokonale pochopeny. Pro mnohé představují jednoduše počítačové bitvy nebo psychologický boj. Hlavním cílem je popsat základní aspekty informačních operací v polském doktrinálním dokumentu, součástí je též prezentace klíčových definic a vysvětlení, jak je informační prostředí vnímáno. Autor rovněž popisuje klíčové schopnosti a techniky, které jsou informačních operací součástí.

Abstract

Information operations are still not understood very well. For many people, Info Ops are simply computer warfare or psychological operations.
The main purpose of the article is to describe the fundamental aspects of information operations in the Polish doctrinal document. The content of the paper includes presentation of key definitions and explanation of how the information environment should be perceived. The author made also an attempt to describe key capabilities and techniques integrated and coordinated through information operations.

Klíčová slova

Informační operace; informační aktivity; informační prostředí; psychologické operace.

Keywords

Information Operations; Information Activities; Information Environment; Psychological Operations.

[a] Department of Information Activities, Faculty of Military Studies, War Studies University. Warsaw, Poland. E-mail: z.modrzejewski@akademia.mil.pl, ResearcherID: E-8527-2018

INTRODUCTION

The rapidly changing nature of information, its flow, processing, dissemination, impact and, in particular, its military employment has influence on development of information operations (Info Ops).

The ratification of the *Allied Joint Publication* (AJP)-3.10(A), *Allied Joint Doctrine for Information Operations* by Poland, as a member of NATO, determined the necessity to implement the regulations contained in it in the Polish Armed Forces. The implementation of the provisions of the above doctrinal document enables functioning of the Polish Armed Forces in accordance with standards that are obligatory in NATO. Doctrinal document *Operacje Informacyjne DD-3.10(A)*[1] is the national equivalent of the allied AJP-3.10(A) which has been ratified without reservation. This document was introduced in Polish Armed Forces on 2 October 2017. I would like to emphasize that this is the first doctrinal document dedicated to information operations in the Polish Army. The purpose of this document is to provide guidance and direction for integrating Info Ops planning, conduct and assessment of operations. DD-3.10(A) mainly focuses on the operational level, but can be used as a reference at all levels. This document presents the basic principles of conducting information operations in the national and allied systems. It also applies in the coalition dimension.

INFO OPS DEFINITIONS

In NATO publication Info Ops are defined as:

> *"A staff function to analyse, plan, assess and integrate information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and NAC*[2] *approved audiences*[3] *in support of Alliance mission objectives".*[4]

Polish definition of Info Ops is more complex:

> *"Information operations (Info Ops) are projects coordinated by the staff cell consisting in analysing the information environment, planning, integrating and assessing information activities in order to obtain the expected effects on the will to act, understand the situation and possessed by the opponent (potential opponent) and other approved objects of influence to support the achievement*

[1] *Operacje informacyjne DD-3.10(A)*. Bydgoszcz: Centrum Doktryn i Szkolenia Sił Zbrojnych, 2017.
[2] NAC - North Atlantic Council.
[3] NAC approved audiences are those identified in top-level political guidance on Alliance information activities. These may include adversaries, potential adversaries, decision-makers, cultural groups, elements of the international community and others who may be engaged by Alliance information activities. *Allied Joint Publication AJP-3.10, Edition A, Version 1, Allied Joint Doctrine for Information Operations*, NATO Standardization Agency, 7 December 2015, p. 1-5.
[4] *Allied Joint Publication AJP-3.10,* ref. 3, p. 1-5

of the assumed objectives of the operation, as well as the strategic communication objectives".[5]

According to the definitions presented above, Info Ops have an advisory and coordination function for military information activities. Commanders at operational and tactical level ensure through the Info Ops function that all military information activities (IA) are properly coordinated as well as integrated into the operational planning process.

In the Polish doctrine, the information activities are defined as:

"Actions designed to affect an object of influence, information and information systems using appropriate abilities and tools. They can be performed by any actor and include precautionary measures limiting the impact on their own information and information systems."[6]

For comparison, in the allied doctrine, we can read that information activities are: "*actions designed to affect information or information systems. Information activities can be performed by any actor and include protection measures*."[7]

Both definitions are very similar and contain an offensive aspect (impact on information and information systems of the enemy) and defensive (protect own resources and information systems).

INFORMATION ENVIRONMENT

Contemporary military operations are conducted in a complex environment in which information plays a key role. The *information environmen*t (IE) is a part of the operational environment. In fact, any activity that occurs in the information environment simultaneously occurs in and affects one or more of the operational environment domains. Operational environment includes physical areas and factors of the air, land, space, maritime, and cyberspace domains, and the information environment, which includes cyberspace.

When we observe the latest conflicts and global engagements we can see the nature of the information environment especially that this environment runs the gamut from the least to the most technologically advanced in any given area of operations. Information operations create effects in and through the information environment. These effects are intended to influence, disrupt, corrupt or usurp enemy or adversary decision making and everything that enables it, while enabling and protecting friendly decision making.

The development of information operations, their shape and character are very rapid, hence, it is important for the issues under consideration to understand the information environment clearly.

[5] Department of Information Activities, ref. 1, p. 15
[6] Ibid.
[7] *Allied Joint Publication AJP-3.10,* ref. 3, p. 1-5

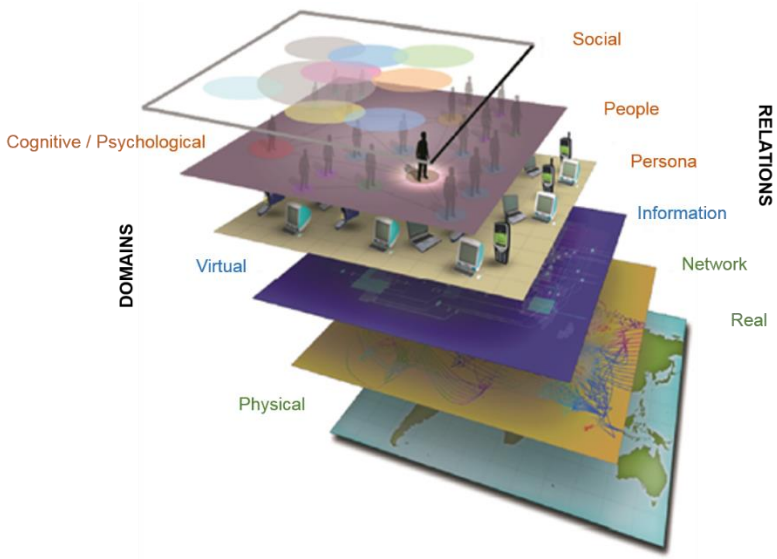
The *NATO Military Policy for Information Operations* (MC 0422/5) defines information environment as follows:

> *"The information environment (IE) comprises the information itself, the individuals, organizations, and systems that receive, process and convey the information, and the cognitive, virtual, and physical space in which this occurs."*[8]

Another definition of this term can be found in the Polish document, according to which: "*the information environment is a space in which information is produced, acquired, processed and transmitted from senders to designated recipients*."[9]

The information environment consists of two main facets – the domains and the relationships between them.

Figure 1. The Information Environment



Source: Allied Joint Publication AJP-3.10(A), op. cit., p. 1-2.

The first facet comprises the input into three domains: physical, virtual and cognitive/psychological.

Physical domain is the space where physical activities occur and individuals, nations, states, cultures and societies interact. Within the physical dimension of the information environment there is the connective infrastructure that supports the transmission, reception, and storage of information. Physical domain involves physical platforms and communications networks that connect them as well as a number of elements which

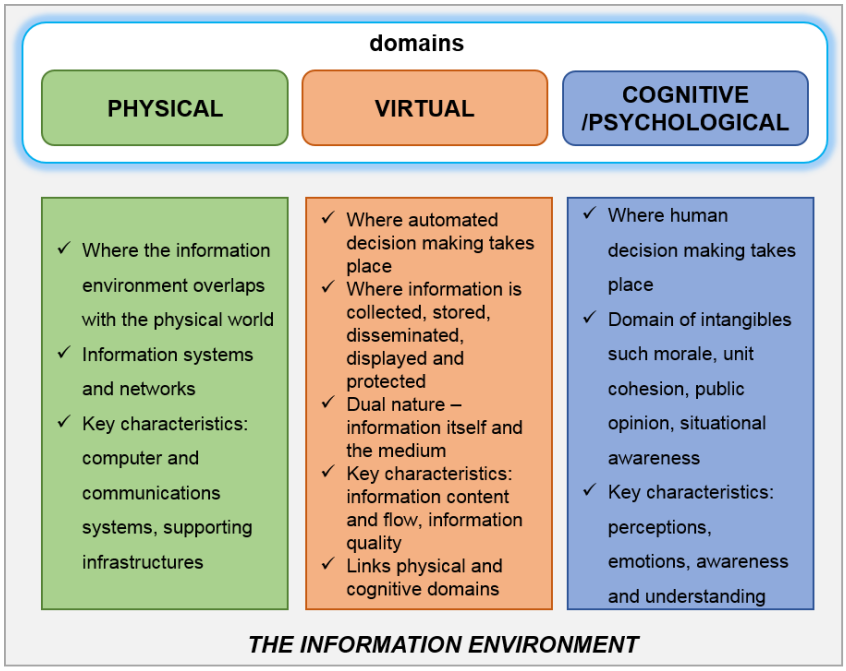
[8] *Military Decision on MC 0422/5. NATO Military Policy for Information Operations,* North Atlantic Military Committee, 11 February 2015, p. 2.
[9] Department of Information Activities, ref. 1, p. 18

include people, infrastructure, publications, computers, tablets, smartphones and other communication items. Also, within this dimension there are tangible actions or events that transmit a message in and of themselves, such as patrols, aerial reconnaissance, and civil affairs projects.

Communication is facilitated in the virtual domain by intangible activities and technical tools. Within the virtual domain there is the content or data itself. The virtual domain refers to the content and flow of information, such as text or images, data that staffs can collect, process, store, disseminate, and display. This domain provides the necessary link between the physical and cognitive dimensions.

The cognitive/psychological domain is the most important as it consists of cognition and emotions, which affect an individual's decision-making. Within the cognitive domain there are the minds of those who are affected by and act upon information. These minds range from friendly commanders and leaders, to foreign audiences affecting or being affected by operations, to enemy, threat or adversarial decision makers. This domain focuses on the societal, cultural, religious, and historical contexts that influence the perceptions of those producing the information and of the targets and audiences receiving the information. In this domain, decision makers and target audiences are the most prone to influence and perception management. Decisions are made in this domain.

Figure 2. The Information Environment Domains



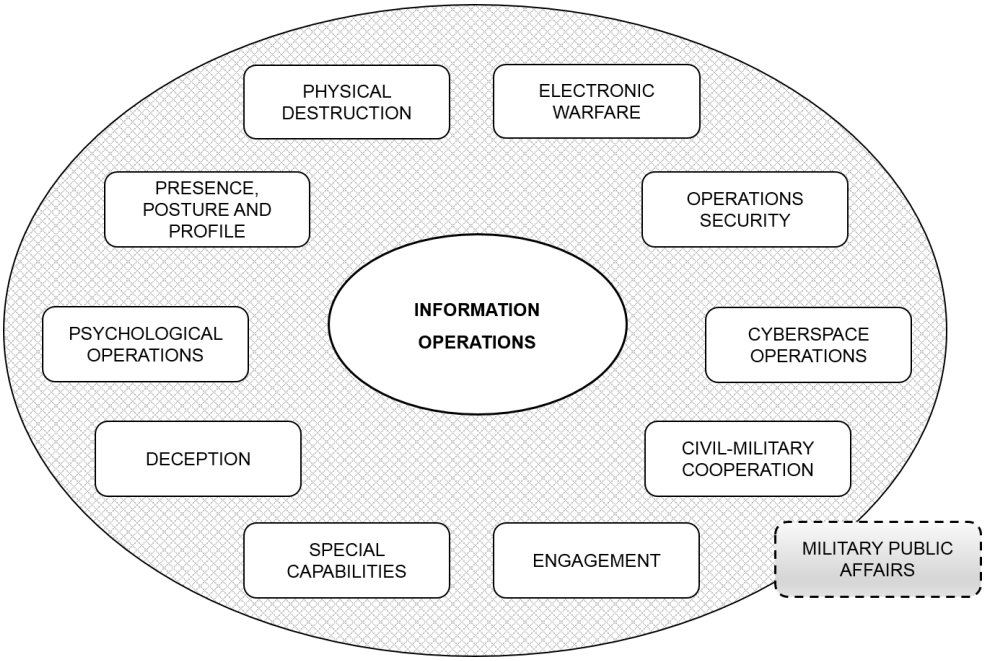
Source: Author.

The second facet concerns the interrelationships between six elements or layers of the information environment. These are:

- real world and its events;
- network connectivity that delivers information;
- information itself;
- persona that inhabit the environment and who develop the messages in it;
- people (individuals, actors and social groups) that interpret and exploit the environment.

KEY CAPABILITIES AND TECHNIQUES INTEGRATED THROUGH INFO OPS

Figure 3. Capabilities and Techniques of Info Ops



Source: Author.

The nature of the information environment is global, overarching and multi-facetted, and does not belong to anyone. There are no boundaries that limit the worldwide flow of information. The information environment has increased in complexity. Due to the widespread availability of the Internet, wireless communications and information, the information environment has become an even more important consideration to military planning and operations, because the military increasingly relies on these technologies.

Understanding the information environment is the most essential prerequisite for dealing with crisis/conflict. Understanding the IE includes underlying causes, actors, dynamics and drivers. Inadequate analysis of the IE is perhaps the most common error. Commanders and their staffs must understand the information environment, in all its complexity,

and the potential impacts it would have on current and planned military operations. The assessment of the Information environment contributes to the development of mission objectives and appropriate messaging.

To sum up, Army employs Info Ops to create effects in and through the Information Environment that provide commanders a decisive advantage over adversaries, threats, and enemies in order to defeat the opponent's will.

In the Polish doctrine, Info Ops are composed of ten capabilities and techniques and one related activity.

The above list of capabilities and techniques forms the basis of most Info Ops activities. I would like to emphasize that it is not exhaustive and is limited only by the availability of the capabilities and techniques and the constraints of policy and law.

Psychological Operations (PSYOPS)

Psychological operations are a key capability required for the conduct of military information activities against opponents or towards a local population.

The *Allied Administrative Publication* (AAP)-06 defines psychological operations as: "*planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives.*"[10]

Since January 2018, a new doctrine of psychological operations has been implemented in the Polish Army. According to this document:

> *"Psychological operations are one of the elements of the strategic communication. They constitute a planned process of transferring prepared content using various methods and means of communication directed to selected and approved objects of influence (audiences) in order to influence the expected change in perception, attitudes and behaviours, being designed to achieve the intended political and military objectives."*[11]

Psychological Operations (PSYOPS) are military activities which are aimed at influencing the perceptions, attitudes and behaviours of target populations. The essence of PSYOPS consists in the fact they are of a long-term nature.

PSYOPS activities are coordinated through Info Ops as part of the overall information strategy. PSYOPS represent one of the key capabilities that allows the force to communicate its themes and messages to approved audiences.

In support of Info Ops, PSYOPS seek to affect perceptions, attitudes and behaviour; they can affect a broad range of audiences from populations to decision-makers at all levels.

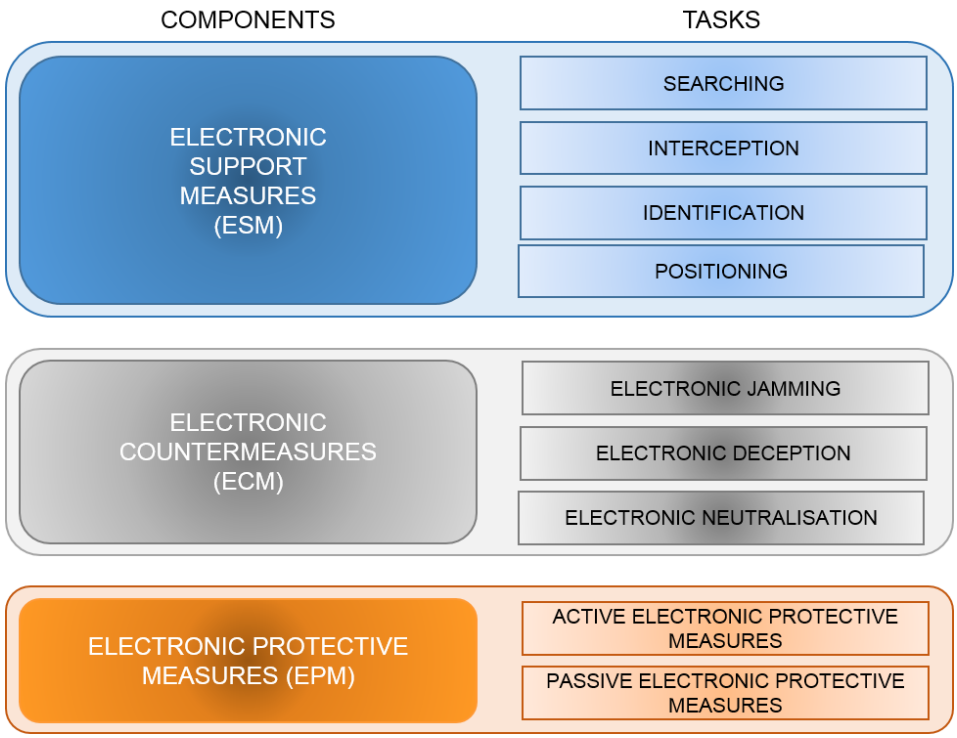
[10] *AAP-06 (2015) - NATO Glossary of Terms and Definitions*, NATO Standardization Office, 17 November 2015, p. 2-P-10

[11] *Operacje psychologiczne DD-3.10.1(B)*, Bydgoszcz: Centrum Doktryn i Szkolenia Sił Zbrojnych, 2017, p. 13

Electronic Warfare (EW)

Military operations are executed in an environment complicated by increasingly complex demands on the electromagnetic (EM) spectrum. According to the Polish Electronic Warfare Doctrine, electronic warfare (EW) consists of military activities that use EM energy to provide situational awareness and achieve offensive and defensive effects.[12] Electronic warfare is a military action to exploit the electromagnetic spectrum which encompasses the interception and identification of electromagnetic (EM) emissions, the employment of EM energy, including directed energy, to reduce or prevent hostile use of the EM spectrum and actions to ensure its effective use by own or friendly forces.[13] EW contributes to the success of information operations by using offensive and defensive tactics and techniques. Electronic warfare supports all types of military activities across the spectrum of the conflict. The main goal of the EW is to prevent the opponent from gaining an advantage in the EM environment. It also supports the conduct of friendly information activities, such as deception and PSYOPS. EW comprises three sub-components presented in the charts below.

Figure 4. Overview of Electronic Warfare



Source: Author.

[12] *Walka radioelektroniczna DD-3.6(B)*. Bydgoszcz: Centrum Doktryn i Szkolenia Sił Zbrojnych, 2015, p. 20
[13] Ibid.

Electronic support measures (ESM) is the first division of EW involving actions taken to search for, intercept and identify electromagnetic (EM) emissions and locate their sources for the purpose of immediate threat recognition. ESM is an integral part of intelligence collection.

Moreover, electronic support measures are an integral part of the INTEL collection. They provide the commander with a greater degree of situational awareness to aid timely and informed decision-making.[14]

Electronic countermeasures (ECM) is the second division of EW involving actions taken to prevent or reduce the adversary's effective use of the EM spectrum, through the use of EM energy. They combine non-destructive actions to degrade or neutralise, such as EM jamming and deception, along with the destructive capabilities of DE weapons to neutralise adversary devices.

Electronic protective measures (EPM) protect personnel, facilities, equipment, and, along with spectrum management, counter hostile information capabilities and protect friendly use of the electromagnetic spectrum.

The sub-components of electronic warfare described above can be used together or separately.

To sum up, electronic warfare is essential for protecting friendly operations and denying adversary operations within the electromagnetic spectrum throughout the operational environment.

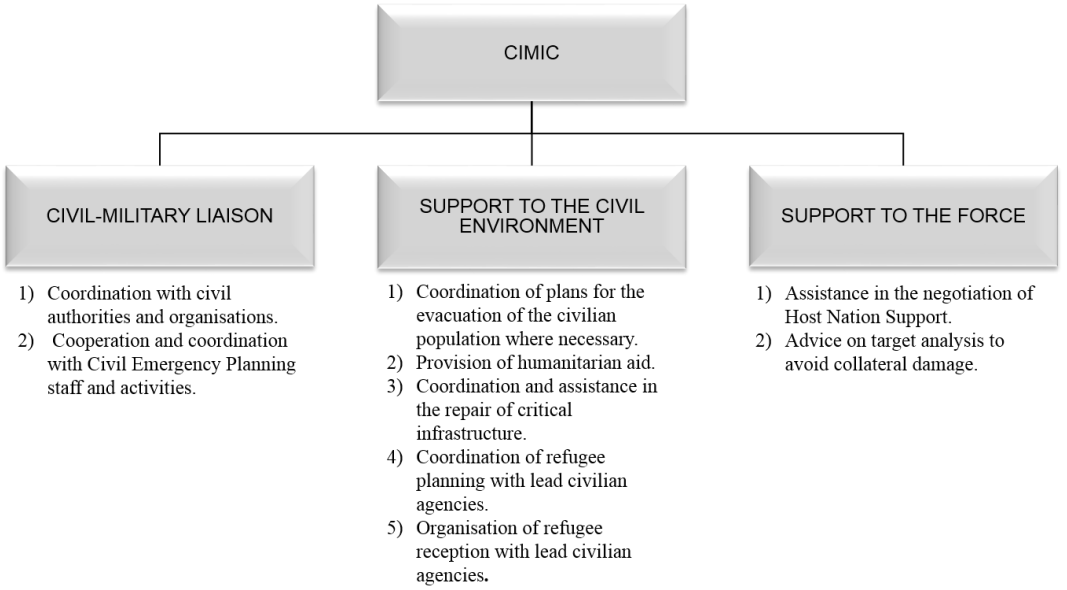
Civil-Military Cooperation (CIMIC)

Civil-military cooperation is another area that can directly affect and be affected by Info Ops. After reviewing the allied and national doctrinal documents it can be concluded that civil-military cooperation is coordination and cooperation, in support of the mission, between the commander and civil actors, including national population and local authorities, as well as international, national and non-governmental organizations (such as the International Red Cross and Red Crescent Movement) and agencies.[15]

[14] *Allied Joint Publication AJP-3.10,* ref. 3, p. 1-11

[15] Compare with: *Doktryna współpracy cywilno-wojskowej Sił Zbrojnych RP DD/9,* Warszawa: Sztab Generalny WP, 2004, p. 8 and *Allied Joint Publication AJP-3.4.9, Edition A, Version 1, Allied Joint Doctrine for Civil-Military Cooperation*, NATO Standardization Agency, 8 February 2013, p. 2-1

Figure 5. CIMIC Core Functions



Source: Author.

CIMIC activities establish, maintain, influence, or exploit relations between military forces, governmental and non-governmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operations area in order to achieve mission objectives. It supports and assists Info Ops by enhancing the relationship between the overall force and the civilian populace. CIMIC is an integral part of modern operation and is intended for all types of operations.

According to the Polish doctrine, CIMIC facilitates cooperation and coordinates activities between a military force and all parts of the civilian environment within the operations area by:[16]

- liaising with civil actors;
- providing assessments and knowledge on political, economic, environment and humanitarian factors when planning and conducting military operations;
- building an effective relationship between the military and civilian authorities, organizations, agencies and populations within the operation area;
- as part of civilian support, it can also coordinate military activities in relief operations.

The conduct of appropriate and timely "Hearts and Minds" tasks can add considerable credibility to an Info Ops message. However, care must be taken to avoid giving the perception that non-military parties are being exploited by the military, CIMIC must therefore remain based on an atmosphere of mutual understanding and trust.

[16] *Operacje informacyjne DD-3.10(A)*, ref. 1, p. 26

Engagement

Traditionally, engagement has focussed only on the key leader, but recent operations (see for instance: Iraq, Afghanistan) have emphasized that engagement at all levels and all times can have an impact on behaviour, attitudes and perceptions of the target audience.

According to the Polish doctrine, key leader engagements (KLE) are:

> *"Engagements between military commanders and their representatives and key decision-makers representing individual participants of the activities that have defined goals (such as a change in policy or supporting the objectives of the operation)."*[17]

Key Leader Engagement is a significant part of the influencing piece in any campaign, but specifically in a non-kinetic operation.

> *"KLE is not a new phenomenon. Military commanders and diplomats have been meeting with important local officials for decades in different countries and mission areas. However, the meaning of KLE is not universally understood nor documented within doctrines. Some argue that KLE is engagement conducted only by high ranking officials while others believe that KLE can be conducted by anyone on any level."*[18]

Therefore, the engagement has been divided into two categories:[19]

- key leader engagement (KLE); and
- soldier level engagement (SLE).

KLE means the relationship between Polish military commanders and their representatives and the key decision-makers (local politicians, military and police leaders, religious, tribal and cultural leaders), of approved audiences that have defined goals, such as a change in policy or supporting the operation objectives. These engagements can be used to shape and influence foreign leaders at the strategic, operational and tactical levels, and may also be directed toward specific groups, such as local politicians, military and police commanders, religious and tribal leaders, academic leaders, and cultural leaders, e.g., to solidify trust and confidence in the Polish forces. All key actors and their inter-relationships should be identified. Their personalities, leadership styles, ambitions, motivation, objectives (short and long term), current stance, dependencies, psychological profile and personal history must be fully understood. The complex, adaptive relationships and dependencies that exist between actors and social groups must be recognised.

KLE may be applicable to a wide range of operations such as stability operations, counterinsurgency operations, non-combatant evacuation operations, security cooperation activities, and humanitarian operations. Info Ops staff supports these

[17] Ibid., pp. 31-32

[18] LINDOFF, Jenny - GRANASEN, Magdalena, *Challenge in Utilising Key Leader Engagement in Civil-Military Operations* [online]. Stockholm: Swedish Defence Research Agency, 2011 [Cited 2018-02-01]. Available from: https://goo.gl/ixEnpF

[19] *Operacje informacyjne DD-3.10(A),* ref.1, pp. 30-31

engagements by identifying and maintaining a database of all key actors within the operations area and moreover coordinate the commander's key leader engagement plan.

In the Polish doctrine, the term SLE is not defined, but it can be assumed that it means that military personnel interact with the civil environment representatives (local and regional population) on a daily basis.[20] To exploit this opportunity best, all soldiers as well as civilian personnel of the armed forces should be trained on how to engage with local population and given a simple narrative that they can construct their engagement around.

To sum up, the leader and soldier engagement means interpersonal interactions of leaders and soldiers with audiences in area of operations.

Presence, Posture and Profile

Presence, posture and profile are interrelated terms that define and describe a unit's visual, aural, and oral presentation to others. Presence, posture and profile are an active means by which units can shape sentiments through physical, visual and audible actions.

Presence. The presence or threat of deploying a force will have an impact on perceptions. Deploying even limited capabilities to the right place at the right time adds substantial credibility to messages delivered through other channels and provides a major contribution to deterrence.

We should deploy even limited capability to the right place at the right time. Real or perceived presence of friendly forces (FF) can provide a major deterrence to mission threatening behaviour.

Posture. The posture and conduct of force elements can be scrutinised by global audiences and make a considerable difference to the perceptions of all actors. Therefore, force posture must be deliberately considered and feature in prevailing cultural and threat factors.

Posture can demonstrate commitment and intent, can demonstrate strength, must be considered for risk to or enhancement of force protection and will be interpreted by the enemy, friendly forces and by the populace.

Profile. It addresses the degree of presence, both in terms of quantity and quality. The term expresses our specific interactions with the individuals and groups in the area of operations (for example: *How regularly do we patrol?* or *Do we talk to civilians?*). During the stability-focused operations, unit's profile may be both minimized and optimized through partnership efforts with local national security forces. However, during the conduct of offensive or defensive-focused operations, a unit tends to optimize its profile in terms of all assets or effects it can bring to bear. The commander plays an especially important part. His public profile can impact upon perceptions and may create opportunities to get messages across.

Deception

The definition contained in the Polish doctrine coincides with the NATO Glossary of Terms and Definitions and presents deception as: "*Those measures designed to mislead*

[20] *Operacje informacyjne DD-3.10(A),* ref.1, p. 31

the enemy by manipulation, distortion, or falsification of evidence to induce him to react in manner prejudicial to his interests."[21]

The aim of deception is to mislead the adversary and thus persuade him to adopt a course of action that is to his disadvantage. It is often most effective when it aims to reinforce existing preconceptions and perceptions.

According to the author, the specific purposes of deception may include:

- causing surprise,
- ensuring the safety of activities,
- allowing the commander's freedom of movement,
- misleading the enemy,
- minimizing one's own losses and limiting the time of operation and the level of used forces and resources.[22]

Whilst *operations security* (OPSEC) denies information to an adversary, reducing his capacity to make effective decisions, deception fills the void with information tailored for his consumption leading to definite but incorrect decision-making. Therefore, *military deception* (MILDEC) can be characterized as actions executed to mislead the adversary decision makers deliberately, creating conditions that will contribute to the accomplishment of the friendly mission.

To employ the art of deception effectively, the deceiver must know and understand the mind of the enemy. Good intelligence becomes the cornerstone of a successful military deception operation. To understand the value added that intelligence brings to the deception planning process, it is important to understand the difference between information and intelligence.[23]

According to the *NATO Glossary Terms and Definitions,* information should be understood as: "*unprocessed data of every description which may be used in the production of intelligence.*"[24]

While intelligence is:

> *"The product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of actors, in order to identify threats and offer opportunities for exploitation by decision-makers."*[25]

[21] Ibid., p. 29; AAP-06 (2015); *Operacje psychologiczne DD-3.10.1(B)*, ref. 10, p. 2-D-2
[22] MODRZEJEWSKI, Zbigniew, *Operacje informacyjne*, Warszawa: Wydawnictwo Akademii Obrony Narodowej, 2015, p. 78, ISBN-978-83-7523-381-0.
[23] JOHNSON, Mark - MEYERAAN, Jessica, *Military Deception: Hiding the Real - Showing the Fake*. [online]. Joint and Combined Warfighting School 2003, p. 4. [Cited 2018-02-05]. Available from: https://goo.gl/QneePT
[24] *Operacje psychologiczne DD-3.10.1(B)*, ref. 10, p. 2-I-4
[25] Ibid., p. 2-I-6

Cyberspace Operations

Cyberspace does not have a standard, objective definition. According to the Polish language dictionary cyberspace is: "*a vital space in which communication between computers connected via the Internet is carried out.*"[26]

In an American joint doctrine we can find an explanation that:

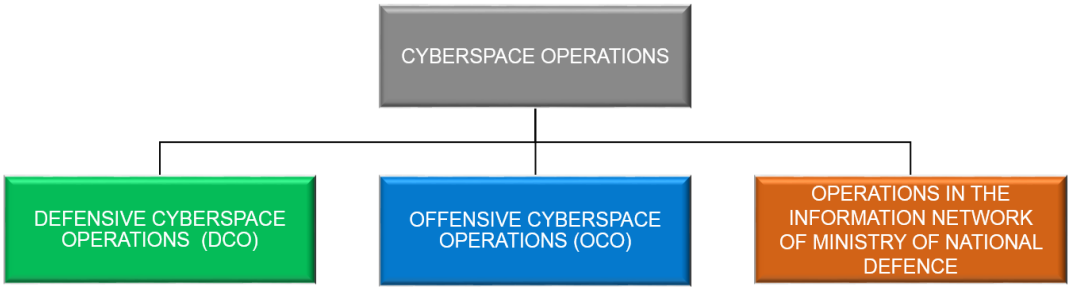
> *"Cyberspace consist of many different and often overlapping networks, as well as the nodes (any device or logical location with an internet protocol [IP] address or other analogous identifier) on those networks, and the system data (such as routing tables) that support them."*[27]

In this document the term *cyberspace operations* means: "*the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.*"[28]

Nowadays, cyberspace operations play an increasingly important role. Cyberspace operations are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.

The Polish doctrinal document does not contain a definition of cyberspace operations. According to this document cyberspace operations are divided into three groups shown in the figure below.

Figure 6. Cyberspace Operations



Source: Author.

Comparing Polish doctrinal document with the allied one, different terminology is clearly visible, because in the NATO document there is no cyberspace operation.

The doctrine *AJP-3.10* from 2009 defined *Computer Network Operations* (CNO), further differentiating between *Computer Network Attack* (CNA), *Computer Network*

[26] *Słownik języka polskiego,* PWN [online]. [Cited: 2018-06-04]. Available from: https://goo.gl/p9g2KW

[27] *Joint Publication JP 3-12(R) Cyberspace operations,* Joint Chiefs of Staff, 5 February 2013, p. I-2.

[28] Ibid., p. II-1

Exploitation (CNE) and *Computer Network Defence* (CND),[29] but in the docrine *AJP-3.10(A)* from 2014, only the following are mentioned: *Computer Network Attack* and *Computer Network Exploitation*.[30]

This difference is due to the fact that those who wrote the Polish doctrine probably took into account the new NATO's doctrine: *Allied Joint Doctrine for Cyberspace Operations AJP-3.20(A)* where such a division would be accepted. It should be added that cyber operations are yet to be defined in AAP-06 and doctrines.

Operations Security (OPSEC)

Operations security (OPSEC) is the process which gives a military operation or exercise appropriate security. It focuses on preventing our adversaries from access to information and actions that may compromise the operation.

OPSEC identifies and protects critical information and subsequently analyses friendly actions connected with military operations and other activities to:

- "*Identify those actions that can be observed by adversary intelligence systems;*
- *determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries;*
- *select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.*"[31]

Operations security denies the enemy the knowledge of dispositions, capabilities or intensions of friendly forces using both active and passive means. OPSEC protects critical information described as *essential elements of friendly information* (EEFI). EEFI allow the commander to determine how he must protect from successful gathering of information by the enemy. Commanders at all levels are responsible for ensuring that their units, activities or installations plan, integrate, and implement OPSEC measures to protect their command's sensitive and/or critical information in every phase of all operations, exercises or activities. The command implements the OPSEC measures selected in the assessment of risk action or, in the case of planned future operations and activities, includes the measures in specific OPSEC plans.

Special Capabilities

According to both allied at Polish doctrinal documents:

> *"Special capabilities refer to highly classified compartmentalized national capabilities that can be generic or mission specific. Where such capabilities exist,*

[29] *Allied Joint Publication AJP-3.10*, ref. 3; NATO Standardization Agency, November 2009, p. 1-11

[30] Ibid., p. 1-12

[31] *Operations Security (OPSEC)*, Washington: Headquarters Department of the Army, DC 19 April 2007, p. 67

national organizations will hold a nominated officer able to brief the commander where appropriate."[32]

Special capabilities appeared for the first time in the AJP-3.10(A) from 2014 and were not in the earlier versions of the doctrine of information operations. Both the allied and Polish doctrines contain no more information about special capabilities. According to the author of the article this is a result of the fact that such operations will be carried out by special forces and special agencies and will be top secret.

For example, special operations are conducted across the full range of military operations to achieve, among others (political, military), also psychological objectives. Moreover, special operations force precision physical destruction operations against targets where precision-guided munitions cannot guarantee first strike success or when the contents of a facility must be destroyed without damages to that facility.[33]

Physical Destruction

The use of force sends a strong message and consequently the direct application of force through physical destruction of adversary assets will have a significant impact on perceptions. Carefully applied force can play a major role in coercion and deterrence and in reducing the adversary's ability to exercise command.

Physical destruction has two main aspects for creating effects in the information environment.

Firstly, by attacking C2 systems physical destruction affects the decision-making process by disrupting the ability to exercise command and control. This may result in a loss of understanding of the operational situation by the adversary.

Secondly, using force sends a strong message and consequently has a significant psychological impact, especially on the enemy troop's morale.

However, undue collateral damage and unnecessary casualties will have an adverse effect on public support. Whilst physical destruction will almost invariably be required, the commander must consider and balance the potential negative impact that it may cause with the expected benefits.

Military Public Affairs (MPA)

In the Polish doctrinal document, the military public affairs are defined as:

"A tool in which planning and implementation of cooperation with the media, internal communications, and community relations to promote the Polish Armed Forces aims and objectives to audiences in order to enhance awareness and understanding of military aspects of the Polish Armed Forces."[34]

[32] *Allied Joint Publication AJP-3.10*. ref. 3, p. 1-14; *Operacje informacyjne DD-3.10(A)*, ref. 1, p. 30

[33] See *Allied Joint Doctine for Special Operations AJP-3.5*, NATO Standardization Agency, January 2009, p. LEX-5 and p. 2-2.

[34] *Operacje informacyjne DD-3.10(A)*, ref. 1, p. 33.

MPA is a separate, but related function to Info Ops. Both directly support military objectives, counter adversary disinformation and deter adversary actions.

However, it should be remembered that MPA and Info Ops may have different audiences, scope of activity and intention. It is therefore necessary to coordinate the activities constantly and ensure cooperation between these areas at all levels, which is carried out through strategic communication and various coordination projects. Cooperation and coordination between MPA and Info Ops ensure coherence of the information transmission, support the overall effectiveness and credibility of operations, especially during *consequence management* (CM). MPA is a command responsibility at all levels. Practitioners are directly responsible to their respective commanders for the conduct of the *military public affairs* (MPA) activities, and responsive to guidance from the MPA function at higher headquarters.

CONCLUSION

In fact, the increased attention to information operations both in Poland and in other NATO nations is due to the awareness that we are living in an information-dominated environment. The information environment has changed the nature of warfare. Conflicts seem to have no identifiable boundaries and this is why we should think of it as of a global battlespace.

The close coordination by Info Ops staff of all available military capabilities and techniques will contribute to the achievement of the overall objective. A large element of Info Ops is non-lethal and recent operations (especially in Afghanistan and Iraq) have shown its significance by increasing the commander's choice of means, whose effects can be created or generated at all stages of a crisis to support achievement of objectives.

Information operations seek to create specific effects at a specific time and place. They are conducted at all levels of war, across all phases of an operation and across the conflict spectrum. Units conduct Info Ops across the full range of military operations, from operations in garrison, through deployment, to combat operations, and continuing through redeployment upon mission completion.

Therefore, Info Ops integrate all aspects of information to support and enhance the elements of combat power, with the goal of dominating the battlespace at the right time, at the right place, and with the right weapons or resources.

To point out, when the commander understands the importance of the information environment, the Info Ops staff is more likely to gain the support and guidance needed to develop an effective information operation.

The subject of these considerations was the Polish point of view on information operations. The author of the article presented fundamental aspects of information operations through the Polish doctrinal documents.

In conclusion, the doctrinal document *Operacje Informacyjne DD-3.10(A)* is the national equivalent of the *Allied Joint Publication AJP-3.10(A)* from 2014, which has been ratified by Poland without reservation, therefore we can observe that the Polish doctrine is very similar to the allied doctrine. The Polish information operations doctrine is intended primarily for use by the Polish forces.

Table 1. Information Activities Summary

ACTIVITY	PRIMARY OBJECTIVE	PRIMARY TARGET
PSYOPS	Influence and shape perceptions Counter propaganda	Military forces Population
EW	Degrade, disrupt,, deny, exploit, and protect use of EM spectrum	Reconnaissance, Intelligence, Surveillance and Target Acquisition (RISTA) Command and Control (C2) Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR)
CIMIC	Gain local acceptance and support	Foreign civil authorities/organisations Population (NGOs) Private voluntary organisations (PVOs)
OPSEC	Deny critical information	Enemy collectors and sensors (RISTA)
ENGAGEMENT	Influence on behaviour, attitudes and perceptions	Key leaders Population
DECEPTION	Mislead	Enemy decision-makers
PHYSICAL DESTRUCTION	Degrade, disrupt, deny, and destroy Info infrastructure and Info Ops-related capabilities	C2 systems, links, and nodes Defensive and offensive Info Ops systems
MPA	Counter misinformation Keep people informed	Society Friendly forces Foreign decision-makers

The capabilities discussed in this article do not constitute a comprehensive list of all possible capabilities that can contribute to Info Ops. This means that individual capability ownership will be highly diversified. The ability to access these capabilities will be directly related to how well the commanders understand and appreciate the importance of Info Ops.