DOI: 10.53477/ 1842-9904-22-17

INFORMATION OPERATIONS – COMPARATIVE DOCTRINAL ANALYSIS

*Cosmina-Andreea NECULCEA**
*Florian RĂPAN, PhD***

The aim of this article is to identify differences in doctrinal projection at the level of the North Atlantic Alliance. The article has been designed as a comparative study of the doctrinal projections specific to information operations (InfoOps), mainly with regard to the doctrines and operations manuals of the United States of America, as the originator of most of these documents, NATO doctrines and domestic doctrines. On an initial examination of the three doctrinal projections, it can be observed that there are differences in the InfoOps approach, both in terms of surface elements, recognized by identifiable markers, and differences in perspective, which allow and encourage interpretation. There is therefore a need to clarify the nature of InfoOps and its correct understanding from a conceptual and practical point of view, and to achieve coherence between the doctrines for information operations of NATO member states and the allied doctrine.

Keywords: *information operations (InfoOps); doctrines; comparative analysis; differences; doctrinal interoperability.*

*
* *

In writing the article, we started from identifying the differences in doctrinal projection in the American, Romanian and NATO doctrinal apparatuses, with the intention of contributing to a higher degree of interoperability for joint actions and exercises in the field of information operations. To this end, we have resorted to a content analysis of the information operations doctrines and, subsequently, to a

**** LT Cosmina-Andreea NECULCEA is Assistant Lecturer at "Henri Coandă" Air Force Academy, Braşov and a PhD Student at "Carol I" National Defence University, Bucharest, Romania, E-mail: saghincosmina@yahoo.com***
***** Maj. Gen (Ret) Florian RĂPAN, PhD, is a Professor at the "Dimitrie Cantemir" Christian University, Bucharest, Romania, E-mail: rapan_florian@yahoo.com***

comparison of them from three perspectives: the definition of the concept and key areas, the identification of the operating principles and of functional structure and the surface and in depth differences in the application of each of the key areas of information operations within the American, the Romanian and NATO doctrines.

Introduction

Over time, the nature of conflicts has changed, and one of the determining factors of warfare and the one that led to the shaping of concepts was *technology*. In the past, differences between the technological capabilities of adversaries constituted the main differentiating element and, together with the level of asymmetry regarding the number of belligerents involved in the conflict, were essential for gaining superiority. Nowadays, the extensive flow of information, the decrease in the number of soldiers involved in operations (decrease in the battlefield deployment density), as well as the influence of technology, have made the achievement of information superiority, which can only be interpreted in classic operations, the main objective. In addition to the five operational domains, land, air, maritime, space and cyber, the human mind can be considered a new domain of operations (even if it has not become an independent domain, the cognitive domain is being recognized in the Western armies as well; in Chinese doctrine it is enacted as such). For example, the US Information Operations Doctrine, JP 3-13/ Information Operations, emphasizes the importance of human influence and gives the cognitive dimension the status of the most important dimension of the information environment.

At the Alliance level, AJP-3.10/ Allied Joint Doctrine for Information Operations, published in 2015, emphasizes the influence of global trends on the human factor and global power dynamics, creating instability and increasing the probability of conflict. The importance and complexity of the information environment, as well as the changing nature of global security, has led NATO to continuously develop and adapt its concepts and doctrines to meet new challenges.

In the Romanian doctrinal projection, InfoOps[1] support Joint Operations, being considered the most appropriate response to contemporary threats.

1. InfoOps Definitions in NATO, US and Romanian Doctrinal Projections

The rapid changes that have taken place in the information environment, the experiences on the battlefield as well as the lessons learned from recent conflicts have determined the member states of the Alliance to focus more and more on the

[1] For the coherence of the current article and the assurance of its conceptual unity, we will preserve the abbreviation InfoOps, as it appears within the Romanian doctrines.

concept of *information operations* and the awareness of their importance. Concern over InfoOps policies and doctrines both at the level of the Alliance and at the level of other nations began in the 1990s, when many military operations were assigned InfoOps objectives.

The US, as the originator of most Alliance doctrinal documents, first addressed the operational context of InfoOps in the US Field Manual FM 100-6/ Information Operations, which outlined the continuing expansion of the media and assessed that "this new era, the so-called Information Age, offers unique opportunities as well as some formidable challenges". (Headquarters, Departament of the Army 1996, iv). In 1998, the first doctrine for information operations in a joint context, JP 3-13/ Joint Doctrine for Information Operations, emerged and information operations received a definition very similar to what is understood today by operations in cyberspace. Information warfare was also described as "information operations conducted during time of crisis or conflict (including war) to achieve or promote specific objectives against an adversary or adversaries". (Joint Chiefs of Staff 1998, I-1) The emergence of a new doctrine, in 2006, led to the abandonment of the use of the term *information warfare* in favour of the term *information operations* and introduced the concept of *information environment*.

According to the 2006 doctrine, the main objective of InfoOps was "to achieve and maintain information superiority for the US and allies" (Joint Chiefs of Staff 2006, ix), in order to "enhance commanders' freedom of action and enable them to make decisions and maintain the initiative while remaining inside the adversary's decision cycle" (Joint Chiefs of Staff 2006, 1-5). The current doctrine projects information superiority only in relation to information assurance/IA[2]. In both doctrines, the information environment is described as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act upon information" (Joint Chiefs of Staff 2014, ix) and includes three dimensions: physical, informational and cognitive, which constantly interact with individuals, organizations and systems.

The InfoOps approach from the US perspective is slightly different from NATO or Romanian because it does not offer a definition, but rather considers the information operations to be "the integrated employment, during military operations, of information-related capabilities/ IRCs in concert with other lines of operation to influence, disrupt, corrupt, or impede decision-making of adversaries and potential adversaries while protecting our own" (Joint Chiefs of Staff 2014, ix). Information capabilities are "tools, techniques, and activities that affect any of the three dimensions of the information environment" (Joint Chiefs of Staff 2014, x)

[2] "Information assurance is necessary to gain and maintain information superiority", (JP 3-13/2014, p. II-9). Here, information superiority represents "The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same".

and are available to the commander to affect the three dimensions of the information environment.

In Alliance operations, InfoOps played a special role, a role that was analyzed and reflected both in theoretical works and in doctrines and manuals, implying direct effects on the battlefield. For NATO, a common understanding of information operations seemed to be crucial to meet the challenges. In this context, AJP-3.10/ Allied Joint Doctrine For Information Operations, published in 2009, defined information operations as follows: "Info Ops is a military function to provide advice and coordination of military information activities in order to create desired effects on the will, understanding and capability of adversaries, potential adversaries, and other NAC approved parties in support of Alliance mission objectives". (NATO Standardization Agency 2009, 1-3)

In order to define influencing operations, the above description was completed by another expression, information activities, defined as "...actions designed to affect information and or information systems. They can be performed by any actor and include protective measures." (NATO Standardization Agency 2009, 1-3). Six years later, a new allied doctrine AJP-3.10/2015 appears, which no makes substantial changes to the definitions in the previous doctrine.

At the national level, the concept of information operations was implemented in the Romanian Army in 2006, with the emergence of the Doctrine of Information Operations, which aimed to create a general framework for planning, conducting and evaluating the effects of information operations, at the operative and tactical level. Later, in 2011, a new doctrine appeared, the Doctrine for Information Operations of the Romanian Army (General Defence Staff 2011)*,* which aimed to align with the 2009 NATO document. The emergence of new types of threats, such as the hybrid one, led modern armies, and implicitly the Romanian Army, to formulate new responses. Therefore, in 2017, a new doctrine emerges, which is still in force today, the Information Operations Doctrine, which emphasizes the role and importance of information operations in the contemporary operating environment. The definition of information operations is very similar to the allied doctrine: "a general staff function, intended for the analysis, planning, evaluation and integration of all information activities in order to obtain the desired effects on the will, understanding, perception and capabilities of adversaries, potential adversaries and of the target audiences approved by the Supreme Council of National Defence, in support of the fulfillment of military objectives". (General Defense Staff 2017, 13)

Considering the comparative analysis of InfoOps definitions from a diachronic perspective, we can assert that InfoOps remains a complex subject, which needs a clear and concise understanding. For example, while the definition of InfoOps in the American doctrine limits InfoOps coordination and synchronization only during military operations, the definitions of the other two projections analyzed do not specify this. In the American conception, InfoOps relies on other information capabilities to create effects at a specific time, in and through the information environment, giving the commander the ability to gain an operational advantage. While these IRCs create their own effects, InfoOps represents the aggregation of these effects, an action seen as essential to achieving objectives.

While NATO and Romanian doctrines mention, in a general way, that the purpose of InfoOps is to create the desired effects, the American definition is much more specific, the purpose of InfoOps being to influence, disrupt, corrupt, usurp the decision-making of adversaries and potential adversaries. Taking into account the three dimensions of the information environment, the cognitive effects manifested by behavior modification are the most important for achieving decisive results, but take time to manifest, compared to effects in the physical and informational dimensions, which can be immediate.

The continuous evolution of the information domain makes it more necessary than ever the need to constantly update these definitions to guarantee a clear vision of what the complexity of InfoOps means. At the same time, different definitions in the three doctrinal projections will lead to different interpretations, and these interpretations can lead to strategic failures.

2. InfoOps Principles in the NATO, US and Romanian Doctrinal Projections

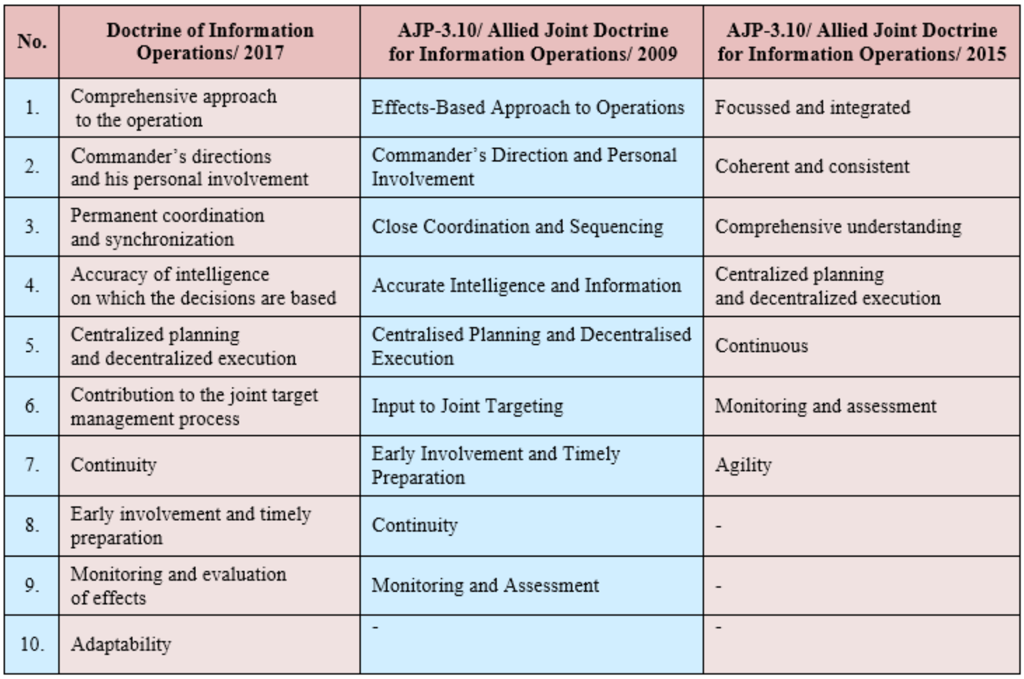
Underpinning the planning and conduct of information operations is a set of principles that have the role of directing activities with an impact on the information environment in support of the full range of military operations, as well as integration into the target selection process.

The Information Operations Doctrine presents a number of ten principles that constitute the foundation of planning and conduct of information operations, principles that are largely taken from the 2009 NATO doctrine, with some modifications or additions.

A first difference identified is that the allied doctrine includes a set of nine principles, while at national level the initial set of nine principles has been completed with the tenth, adaptability. It is also observed that the principles are not listed identically, with principles 7 and 8 changing places.

Moreover, the 2015Allied Doctrine for Information Operations stands out with a different set of principles, compared to the previous doctrine, as can be observed in the Table no. 1:

Table no. 1: InfoOps Principles based on Romanian and NATO doctrines



No.	Doctrine of Information Operations/ 2017	AJP-3.10/ Allied Joint Doctrine for Information Operations/ 2009	AJP-3.10/ Allied Joint Doctrine for Information Operations/ 2015
1.	Comprehensive approach to the operation	Effects-Based Approach to Operations	Focussed and integrated
2.	Commander's directions and his personal involvement	Commander's Direction and Personal Involvement	Coherent and consistent
3.	Permanent coordination and synchronization	Close Coordination and Sequencing	Comprehensive understanding
4.	Accuracy of intelligence on which the decisions are based	Accurate Intelligence and Information	Centralized planning and decentralized execution
5.	Centralized planning and decentralized execution	Centralised Planning and Decentralised Execution	Continuous
6.	Contribution to the joint target management process	Input to Joint Targeting	Monitoring and assessment
7.	Continuity	Early Involvement and Timely Preparation	Agility
8.	Early involvement and timely preparation	Continuity	-
9.	Monitoring and evaluation of effects	Monitoring and Assessment	-
10.	Adaptability	-	-

One of the durable components of the doctrine is represented by the principles, because they stand for the basis of the management of military operations and must be applied on a large scale, regardless of the operational context. One could argue that once we find different principles in doctrines, this can also be understood as a simple conceptual gap. This analysis of differences in the projection of information operations principles are identifiable markers or surface elements in comparative doctrinal analysis.

3. Key Domains Coordinated within InfoOps According to NATO, US and Romanian Doctrinal Projections

Falling under the same category of surface elements, the key domains differ to a greater extent between the conceptual apparatuses analyzed. The first difference concerns precisely the naming/framing of the list of activities under the InfoOps umbrella. The Romanian doctrine of information operations projects a series of 12 key domains**:** Psychological Operations (PSYOPS), Troop Presence, Profile and Posture (PPP), Operations Security (OPSEC), Information Security (INFOSEC), Military Deception (MILDEC), Electronic Warfare (EW), Physical Destruction, Key

Leader Engagement (KLE), Military Engagement, Cyberspace Operations, Cyber Defence and Civil-Military Cooperation (CIMIC), subordinated and coordinated within InfoOps, and can be considered "InfoOps activities only when they are directly aimed at the understanding and perception, will and capabilities or means of the adversary, the potential opponent or other approved entities". (General Defence Staff 2017, 22)

NATO Doctrine, AJP-3.10/2015 includes key InfoOps domains in a distinct category, entitled Capabilities and Techniques Integrated Through Information Operations. Although the list is not exhaustive, the capabilities and techniques listed represent the basis of most InfoOps activities. The current doctrine has also completed the list of capabilities in the previous doctrine with three other capabilities, such as Special capabilities, Military Public Affairs and Cultural understanding and engagement and excluded Information Security/INFOSEC. (NATO Standardization Office 2015, 1-10)

In the US, JP 3-13/ Information Operations doctrine of 2014, lists a more numerous series of capabilities that contribute to InfoOps, which fall under Relationship and Integration**,** as follows: Strategic Communication, Interagency Joint Coordination Group, Public Affairs, Civil-Military Operations, Cyberspace Operations, Information Assurance, Space Operations, Military Information Support Operations/MISO (in previous editions of the doctrines, Psychological Operations, Intelligence, Military Deception, Operations Security, Special Technical Operations, Joint Electromagnetic Spectrum Operations, Key Leader Engagement (Joint Chiefs of Staff 2014, II-5).

The second difference stems from differences in terminology. This includes both surface elements, directly identifiable markers in terms of the name alone, but also aspects of depth or differences of perspective in terms of the philosophy and physiognomy of the key domains involved. Regarding the psychological operations, with the acronym PSYOPS, used by most NATO states, in 2011, there was a terminological change at the US level, replacing the acronym PSYOP with MISO (Military Information Support Operations). However, this change did not produce considerable effects. According to Lieutenant Colonel Robert Bockholt, spokesperson for the US Special Operations Command, "PSYOP forces conduct MISO", and "Psychological operations refer to the name of units, while MISO refers to the function that the military personnel in PSYOP units perform". (Myers 2017)

Furthermore, compared to mass media operations and information and public relations activities, PSYOPS have control over the content and the means of disseminating information and, implicitly, involve a focus on influencing activity through them, i. e. on achieving certain expected effects of the transmitted contents. For example, the Russian InfoOps approach to information security aims not only to guarantee the technical integrity of information, but also to produce the intended cognitive effect. Russia also focuses on influencing the perceptions of the target audience, whereas the Western countries are rather constrained by the objectivity of information. (Joan Prats i Amorós 2019, 16) These examples allow the understanding of the issue as a result of the difference in perspective to a greater extent than as a result of the simple difference in surface, i. e. naming.

Two key domains that encompass the offensive and defensive aspects of InfoOps in cyberspace are *cyberspace operations* and *cyberdefence*. The term cyber is also used in the American doctrinal projection, under the name *cyberspace operation*s, while at NATO level, the 2009 doctrine remained at the wording of *computer network operations* (attack, exploitation and defence), and the 2015 doctrine is limited only to *computer network attack* and *computer network exploitation.*

Through electronic warfare/EW, armies try to dominate the electromagnetic spectrum through the three types of EW actions: electronic protection, electronic attack and electronic support. The US equivalent of EW consists of joint electromagnetic spectrum operations/JEMSO which involves both electronic warfare actions and joint management operations of the electromagnetic spectrum. (Joint Chiefs of Staff 2014, II-12)

While Alliance doctrine, AJP-3.10/2015 and Romanian doctrine use the term Civil-Military Cooperation/CIMIC, the US uses the term Civil-military operations/CMO and does not accept the idea that this action dimension, civil-military cooperation, is considered a capacity.

Regarding key leader engagement/KLE, this capability appears in all three doctrinal projections analyzed, and in the NATO and Romanian projections, it also appears at the military level. In carrying out the mission, every military interacts with the local population, which imposes the need for one's training regarding the mode of interaction as well as the messages to be disseminated. The link between *strategic communications/*StratCom and KLE is that engaging StratCom requires "a robust Key Leader Engagement programme" (Gage 2014, 54). This concept benefits from rather poor documentation and there are no established standards for what a successfully completed KLE would mean.

Another important aspect of information activities is presence, posture and profile/PPP. The deployed unit(s) must be aware of the public image they are displaying, regardless of the deployment area or the assigned mission. In the American projection, this capacity is not included in the list, but we find aspects related to it in the attempts to define StratCom, a capacity that does not only mean "verbal communication, it is presence, posture and profile of our activities, particularly our readiness to support our words with actions thus showing our strength from the political level down until very tactical". (TŪTINS 2015)

In the Romanian doctrine, PPP ranks second in the set of key domains coordinated within InfoOps. The perception and attitude of the target audience can be influenced by the presence, attitude and behavior of the troops and their leaders. The PPP description also emphasizes the need to synchronize these aspects with media operations, given the role of commanders in conveying messages, as well as the protection requirements of forces deployed in the field. Allied doctrine places PPP within the set of capabilities and techniques integrated through information operations, highlighting at the same time the individual effect that this capability can create, because "the mere presence of a force can have a significant impact on perceptions", but also on the information environment. (NATO Standardization Office 2015, 1-12)

Even if the OPSEC concept emerged relatively late, the semantic content is very old, being a means of protection whose challenge "is not the release of classified information, but rather pieces of a puzzle that provide adversaries with a picture of the overall operation" (Dominique 2009, 17). All three doctrinal projections analyzed emphasize the importance of OPSEC in preventing the accidental leakage of information, as well as the role of this capacity in the protection of one's own information. OPSEC requires constant attention, and this capability must be integrated into all aspects of military operations from the very planning stage. In addition, OPSEC proves very important when it comes to deception. The two areas prove to be essential in achieving surprise as well as obtaining and maintaining initiative. Although OPSEC and MILDEC are distinct and discrete processes, the two domains support each other. This is highlighted in all three projections analyzed, each of which clearly highlights this relationship in the text of the doctrine. The link between the two domains stems precisely from their purpose, namely affecting the opponent's decision-making process. Although history provides many examples of deception, military success does not depend entirely on deception. Rather, it serves as a force multiplier. The recent changes in the socio-political landscape have not only increased the importance of deception, but also require Western countries to step up their game of deception. For example, the Russian military sees deception as a distinct activity, outlined by the term Maskirovka (Vowel 2016) – a much more complex form of enemy deception.

The only kinetic lever, as Călin Hentea mentioned, is the physical destruction, a leverage used "not only to eliminate or annihilate some points or command networks or adverse communications, but also to achieve a certain psychological impact on the targeted population or leaders". (Hentea 2008, 303)

The definition of IA/Information Assurance captures the role of this capability in achieving and maintaining information superiority, as well as the interdependence between IA and cyber operations. Also, many features of IA are attributed to Information security/ INFOSEC. With the recognition of space and cyberspace as two new operational domains, the physiognomy of warfare has also changed. Space can be used for both peaceful and aggressive purposes, and the potential for conflict in space has never been more apparent.

Regarding the connection of space operations with information operations, perceived as a joint function, the American doctrine states that the two support each other. Outer space supports the flow of information, it also supports the decision-making process, but it can also deliver information to the information environment. On the other side, information can generate effects that support the achievement of information superiority, defined as "the degree of control in space of one force over any others that permits the conduct of its operations at a given time and place without prohibitive interference from terrestrial and space-based threats". (Joint Chiefs of Staff 2020, I-4)

Conclusions

An essential prerequisite for achieving the objectives entrusted to us is the ability of armies to train and operate together in an integrated and coordinated manner. This helps to guarantee operational efficiency that can only be achieved through a controlled approach to interoperability. In this context, doctrines represent the basic pillar that includes both the concepts (what?) and all the rules of engagement and aspects that characterize military action (how?). In other words, doctrines describe the methods, organization as well as the set of procedures that make it possible to carry out actions in a joint framework. Therefore, comparing different InfoOps approaches is an essential process in the effort to ensure doctrinal coherence.

The nature of InfoOps must be continually clarified so that information operations are conceptually and practically well understood and to be consistent with the evolution and trends of the modern battlefield. There is also a need to achieve coherence between NATO and allied doctrines for information operations. For example, as long as the degree of doctrinal correspondence between NATO and Romanian doctrines in the field of information operations is quite high, interoperability can be achieved seamlessly. Instead, the Romanian presence in information operations under American command would create problems regarding, for example, the integration of INTEL within this function. We can say that interoperability at the operational and tactical level also depends on this issue, on the doctrinal differences, both at the surface level (principles and key areas) and at the depth level, as a way of application and subordination in relation to the joint command. Regarding the three doctrinal projections, there are significant differences, both in the umbrella term "information operations" and in the key areas. Therefore, we emphasize the need to revise the related terminologies in order to be able to keep up with the characteristics of the contemporary operating environment, or to complete the doctrinal apparatus with documents necessary to obtain a high degree of interoperability in joint Romanian-American exercises. It is not necessary to change the terminology used, as it is compatible with NATO terminology, but only to identify these forms of coordination in order to obtain a higher coefficient of doctrinal interoperability, respectively to introduce other concepts necessary for understanding the functionality and dynamics of the battlefield into the Romanian doctrinal apparatus, such as that of Effects-Based Approach to Operations, a proposal found as early as 2016 in the study Information Warfare (Lesenciuc 2016, 47-51). Last but not least, an update of the Romanian Army Doctrine would allow an easier adaptation to the realities of the battlefield.

BIBLIOGRAPHY:

Dominique, Michael. 2009. "Information Operations: The Military's role in gaining information superiority." https://duckduckgo.com/?q=dominique+michael+information+operations+the+military+role+in+gaining+site%3Aapps.dtic.mil&t=newext&atb=v344-1&ia=web

Gage, Daniel. 2014. "The continuing evolution of Strategic." *The Three Swords Magazine*, 54. https://www.jwc.nato.int/images/stories/threeswords/NOV_STRATCOM_evolution.pdf

General Defence Staff. 2006. *Doctrina Operațiilor Informaționale.* (*Information Operations Doctrine).*

—. 2017. *Doctrina Operațiilor Informaționale.* Ediția a 2-a. (*Information Operations Doctrine)*

—. 2011. *Doctrina pentru Operații Informaționale a Armatei României.* (*Doctrine for Information Operations of the Romanian Army*).

Headquarters, Departament of the Army. 1996. "FM 100-6 Information Operations." https://www.hsdl.org/?view&did=437397

Hentea, Călin. 2008. "Noi dimensiuni ale războiului contemporan." *Revista Română de Sociologie*, 289-306. https://www.revistadesociologie.ro/pdf-uri/nr.3-4-2008/Art%206-Hentea.pdf (*New dimensions of contemporary warfare)*

Joint Chiefs of Staff. 1998. *Joint Pub 3-13 Joint Doctrine for Information Operations.* https://www.c4i.org/jp3_13.pdf

—.2006. *Joint Publication 3-13 Information Operations.* https://www.globalsecurity.org/intell/library/policy/dod/joint/jp3_13_2006.pdf

—. 2014. *Joint Publication 3-13 Information Operations.* https://irp.fas.org/doddir/dod/jp3_13.pdf

—. 2020. *Joint Publication 3-14 Space Operations.* https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14Ch1.pdf

Lesenciuc, Adrian. 2016. *Războiul Informațional.* Brașov: Editura Academiei Forțelor Aeriene "Henri Coandă". (*Information Warfare*)

Myers, Meghan. 2017. "The Army's psychological operations community is getting its name back." https://www.armytimes.com/news/your-army/2017/11/06/the-armys-psychological-operations-community-is-getting-its-name-back/

NATO Standardization Agency. 2009. *AJP-3.10 Allied Joint Doctrine for Information Operations.*

NATO Standardization Office. 2015. *AJP-3.10 Allied Joint Doctrine for Information Operations.* Edition A, Version 1.

Prats i Amorós Joan, Guillaume-Barry Augustin. 2019. "Not Only Blood. The Need to Integrate Psychological Operations in the West's Military Culture." *Opinion Paper IEEE 81/2019*, 16. https://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEE81_2019JOAPRA_Psyops_ENG.pdf

TŪTINS, Māris. 2015. "Strategic Communication and Protecting Environment in Military Training Areas." http://putniadazos.lv/sites/default/files/kcfinder/files/2015-05-05_StratCom_environment.pdf

Vowel, JB. 2016. "Maskirovka: From Russia, With Deception." *Real Clear Defense.* https://www.realcleardefense.com/articles/2016/10/31/maskirovka_from_russia_with_deception_110282.html