THE BASIC PROPERTIES OF THE INFORMATION DIMENSION OF THE SECURITY ENVIRONMENT[*]

Milan Miljković[**]
Dragan Jevtić[***]
Slobodan Stojičević[****]

Достављен: 01. 01. 2022. *Језик рада:* Енглески
Кориговано: 15. 02. и 07. 03. 2022. *Тип рада:* Прегледни рад
Прихваћен: 06. 04. 2022. *DOI број:* 10.5937/vojdelo2202018M

The information dimension of modern security environment is characterized by complexity, abundance of non-structured information and numerous conflicts fought via information warfare, which further complicates the analysis of this dimension. Modern information technology has enabled all the participants within a conflict, mainly non-state actors, to influence the global information dimension, thus influencing the security environment. Taking into account that the domestic military theory thus far has not presented comprehensive classification and analysis of the information dimension of security environment, the aim of this paper is to present, analyze and synthesize current views on the theoretical-doctrinal approaches regarding this issue.

Comparative analysis and synthesis of the presented doctrinal approaches to the analysis of the information dimension, points out that such analysis cannot be comprehensive and functional in military context, unless it does not also encompass the methods for analysis of threats and possible opponent actions in the information dimension, besides the analysis of elements, areas, levels, actors and their ability of action in the information dimension.

[*] The paper was prepared as a part of the scientific project "Neutrality and Strategic Deterrence", in the School of National Defense "Vojvoda Radomir Putnik", University of Defense in Belgrade, in the part of the project that consider the theoretical and practical bases of deterrence in the information dimension of conflict.

[**] School of National Defense, University of Defence in Belgrade, Belgrade, Republic of Serbia, milanmiljkovic04011@gmail.com

[***] Military Academy, University of Defence in Belgrade, Belgrade, Republic of Serbia.

[****] Institute for National Strategy, Novi Sad, Republic of Serbia.

It can be concluded that only comprehensive analysis of structure and actors of the information dimension can provide military forces with the information about the possibility of its shaping, i.e. the possibility to act through this dimension and thus affect the potential opponents and contribute to achieving both military goals and national security goals.

Key words: *the information dimension, analysis, PMESII and ASCOPE method, the pattern of information action of the opponent*

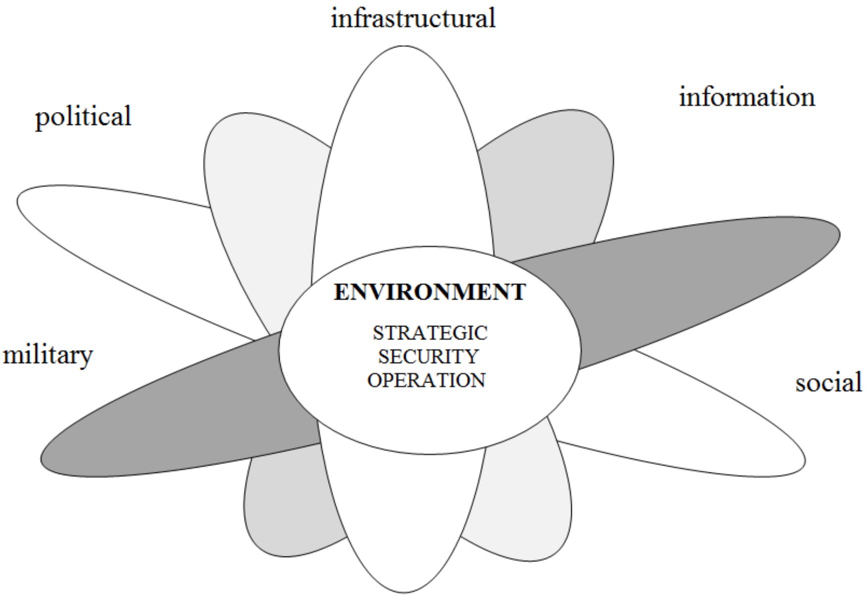
Introduction

For a country and its national security system, security environment is an area in which the leadership of a country and the components of security system cooperate or come into conflict with other countries or actors, for the purpose of improving the state of national security. The analysis of security environment is carried out for the purpose of observing the state and trends of internal and external factors of the environment and their influence on the security of a country. The individual, cumulative and hybrid influences of military, political, economic, information, social, technological and other factors, which influence the state security in different ways, are observed.[1] Each aforementioned factor creates specific dimension of security environment. The current phase of development and security of modern society is characterized by an increasing role of information sphere, which is a set of information, information structure, the subjects that collect, form, expand and use the information, as well as systems for regulating current social relationships.[2] The information sphere is considered as the information dimension of security environment, which, as the systemic factor in the society, actively influences the state of political, economic, defensive and other security components of nation states. In contemporary age, the defense of every country crucially depends on the protection of national interests within the information dimension of security environment, and within the course of future technological development this dependence will be on the increase.[3]

[1] Дејан Стојковић, „Израда стратегијских докумената Републике Србије у области безбедности и одбране”, *Војно дело*, 6/2018, p. 180.

[2] *Доктрина информационной безопасности Российской Федерации* (утверждена Указом Президента РФ № 646 от 5 декабря 2016 г., https://Совет Безопасности Российской Федерации, Доктрина информационной безопасности Российской Федерации (scrf.gov.ru)

[3] *Доктрина информационной безопасности Российсой Федерации*, утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895, https://Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 09.09.2000 N Пр-1895) (утратила силу) | ГАРАНТ (garant.ru)



Picture 1 – *Types of environment and factors of (dimensions) environment*[4]

The information dimension is heterogeneous global environment in which people and automated systems observe, orient themselves, make decisions and act upon data, information and knowledge. Functioning as a channel influencing the decision making in conflicts, the information dimension is a key component of security environment. It is characterized by omnipresence of different media, hyper-connection of actors, so that nowadays the information dimension enables unprecedented communication and information exchange.[5] Modern military forces must be aware of the information dimension through the continuous process of its monitoring and analysis, as well as the possibility to affect potential opponents by acting through this dimension.

Basic characteristics of the information dimension of security environment

The information dimension is defined as a set of individuals, organizations, or systems for collecting, processing or distribution of information. The information dimension permeates and overpasses the borders of land, sea, air, space and cyber

[4] The picture was adapted in accordance with the scheme of operation environment from *Доктрине Војске Србије*, Медија центар „Одбрана", Београд, 2010, p.101

[5] US Department of Defense Strategy for Operations in the Information environment, June 2016, DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf (defense.gov)

space.[6] Certain characteristics of the information dimension, such as the abundance of information, non-structured information, problematic information value and low competence of the information users, make understanding and evaluation of security environment more difficult.[7]

The ones who make decisions in modern conflicts are faced with a phenomenon of "abundance of information" which is the cause of growing issues concerning creating correct intelligence warnings, and frequent omissions of intelligence services, so that the main problem leading to intelligence omissions is not the lack of information, but the "flood of information".[8] By information overwhelming, the entropy effect is achieved in the very process of informing, i.e. "information blindness" is achieved.[9]

In addition, the modern information dimension has led to the transformation of modern conflicts whose characteristics further complicate proper understanding of security environment. One of the basic types of modern conflicts is information warfare which is used with the aim of taking action against hostile information and information systems, as well as the opponent's source of information, but also changing the way of thinking of the opposing side.[10] The primary aim of information warfare is the decision-making process of the opposing leadership. Along with the technological development of information environment, different ways of influencing the opponent and waging information war are developed.[11]

The analysis and understanding of the information dimension is a prerequisite for its shaping for the purpose of adapting the future conditions for conducting military activities. In accordance with that, the provisions regarding the analysis of elements, areas, levels and actors and capabilities in the information dimension are presented in the military doctrinal documents of the USA, the NATO and the Russian Federation. The aforementioned approaches and methods of its analysis shall be presented in the text below.

[6] Милан Миљковић, Драган Јевтић, „Сукоби у информационом простору из угла савремене војне мисли у Руској Федерацији – искуства за безбедност Републике Србије", *Национални интерес*, Београд, no. 2021/2, p. 108.

[7] Tomasz Kacała, „Military Leadership in the Context of Challenges and Threats Existing in Information Environment", *Journal of Corporate Responsibility and Leadership*, https://www.researchgate.net/publication/ 297751621, 08/12/2021.

[8] Milan Miljkovic, Vangel Milkovski, „Challenges facing information environment in contemporary conflicts", *Archibald Reiss Days 2020*, Belgrade, 18-19 November 2020, Thematic conference proceedingsof international significance, University of Criminal Investigation and Police Studies Belgrade, 2020/http://eskup.kpu.edu.rs/ dar/article/view/230/117,08/11.2021.

[9] Милан Миљковић, „Изазови у раду обавештајних служби у информатичком добу", *Безбедност* 3/2020, p. 148.

[10] Милан Миљковић, Драган Јевтић, „Сукоби у информационом простору из угла савремене војне мисли у Руској Федерацији – искуства за безбедност Републике Србије", *Национални интерес*, Београд, no. 2021/2, p. 107.

[11] Нежданов Игорь Юрьевич, *Технологии информационных войн в интернете*, https://studylib.ru/doc/2333221 Технологии информационных войн в интернете (studylib.ru), 25/12/2021.

The analysis of the elements and areas of the information dimension

As stated previously, the information dimension is defined as a set of information, information infrastructure, subjects who collect, create, expand and use the information, as well as the systems for regulating social relationships.[12] The aforementioned provisions from The Information Security Doctrine of the Russian Federation 2016, present the attitudes about basic elements of information dimension. Similar attitudes are mentioned in the American military theory which defines the information dimension as a set of individuals, organizations and systems which collect, process, expand and react to information.[13] Essentially, the information dimension comprises tangible physical elements (communication systems and others) and intangible elements (the information).

In accordance with the aforementioned classification, the elements of the information dimension have been analyzed by the American RAND Corporation[14] in the document “Redefining information military warfare in wireless world” in which it is stated that the information dimension consists of two partially intersecting components: social networks and cyber space.[15] It has been estimated that the people’s social relationships via social networks are growing everyday both in terms of relevance and influence, thus influencing the evolution of contemporary conflict.

The aforementioned theoretical and doctrinal terms present the attitudes about the basic elements of the information dimension, and its classification into three subsets of its elements has been carried out, which is sufficient for the initial structural analysis of this dimension.

The question of further classification and analysis of the information dimension shall be continued by explaining the theoretical-doctrinal approach which is accepted both in the eastern and western military territory, as well as in our doctrinal theory, and that is the approach which classifies and analyses the main areas of the information dimension.[16] The military-doctrinal theory of the USA and the NATO, as well as our doctrinal documents, state that the information dimension consists of three areas: physical, information and

[12] Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ № 646 от 5 декабря 2016 г., https://Совет Безопасности Российской Федерации, Доктрина информационной безопасности Российской Федерации (scrf.gov.ru)

[13] US Department of Defense Strategy for Operations in the Information environment, June 2016, DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf (defense.gov)

[14] The American RAND Corporation is an American non-profit that carries out research and analyses for the US armed forces.

[15] Isaac R. Porche III, „Emerging Cyber Threats and Implications”. *RAND Corporation* Santa Monica, CA, 2016. https://www.rand.org/pubs/testimonies/CT453.html, accessed on 07.03.2022.

[16] Compare: AJP-3.10, NATO, Allied Joint Doctrine for Information Operations, 2015. стр. I-2; US Department of Defense Strategy for Operations in the Information environment, June 2016, DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf (defense.gov); *Доктрина Војске Србије*, Медија центар „Одбрана”, Београд, 2010, стр.101.

cognitive.[17] The American military theory states that, within the information dimension, conflict participants may expect challenges through three interrelated areas: 1) *physical area*, which consists of command and communication systems, as well as the accompanying infrastructure enabling the individuals and organizations to create the effect regarding the information, 2) *information area* consisting of the information content itself including the way which they are collected, processed, stored, distributed and protected, and 3) *cognitive area* comprising beliefs and perceptions of those who transfer, receive and react to the information or act upon them.

Table 1 – *The analysis of elements and areas of the information dimension*

AREAS	THE ELEMENTS OF ANALYSIS OF THE INFORMATION DIMENSION
Physical	– Physical world and its contents, especially the one enabling and supporting the exchange of ideas, information and messages. – The information system and physical networks. – The communication systems and networks. – People and human networks. – Personal devices, manual gadgets and graphic user interface for social media. – Mobile phones, personal digital assistants and graphic user of social networks.
Information	– The information content. – The quality and quantity of information. – The flow of information. – Collected, processed, stored, distributed, presented and protected information. – The social media application software.
Cognitive	– The influence of information on a person's will. – Contextual information and person's decision making. – Immaterial role such as morals, values, world view, situation awareness, perception and public opinions, beliefs, emotions and system of values. – Mental calculations as a stimuli response like the liking for something within the social community.

According to the NATO Allied Joint Doctrine for Information Operations, the physical area is an area of real world in which the interaction between the individuals, nations, cultures and civilizations is conducted and it also includes people, printed media, transmitters, information and communication systems. The information area is data centric and it is a link between physical and cognitive area. The NATO Doctrine has termed the cognitive area, which is human centric, as psychological domain which comprises perceptions, understanding, belief, emotions and system of values. These elements are influenced by different factors such as personal and cultural beliefs, norms, motivations, feelings, experiences, morals, education, mental health, identity and ideologies.[18]

[17] *Доктрина Војске Србије*, Медија центар „Одбрана", Београд, 2010, p.101.

[18] AJP-3.10, NATO, Allied Joint Doctrine for Information Operations, 2015. p. I-2

The western military theory estimates that the cognitive area is the most significant component of the information dimension, because the effects within the physical and the information area are eventually registered as the influence on human cognitive area which makes this area central object of analysis and the target while conducting activities in the information dimension.[19]

The abovementioned doctrinal attitudes have contributed to different classification of the information dimension into three areas, explaining their function and interrelation, and stressing out the significance of the cognitive area. The Table 1 provides a more detailed insight into the doctrinal presentation of the analysis elements of the information dimension area, thus providing basis for more in-depth structural analysis of this dimension.

The analysis of the levels of the information dimension

According to the American doctrinal views, structurally speaking, the information dimension of security environment has its global, national and military context, i.e. level.[20]

The high rate of development and application of the Internet and the electronic media at the turn of the Millennium, has lead to the formation of the global information structure and space. Along with the land, sea, air and space, this information dimension was actively used by the military forces of the developed countries to carry out a wide spectrum of military tasks.[21] The global information infrastructure can be defined as global connecting of communication networks, computers and data bases which make the large amount of information accessible for users. It does not imply only physical objects used for storage, processing and presenting the information. The personnel who make the decisions and handle the transmitted information is a crucial component of the global information infrastructure.[22] While analyzing the global context, the starting point is understanding the connection between a specific information dimension and the global one, and the relation between the actors of a specific security environment and the global media, foreign governments and international political bodies, especially those that could have a negative impact on the activities of security

[19] US Department of Defense Strategy for Operations in the Information environment, June 2016, DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf (defense.gov)

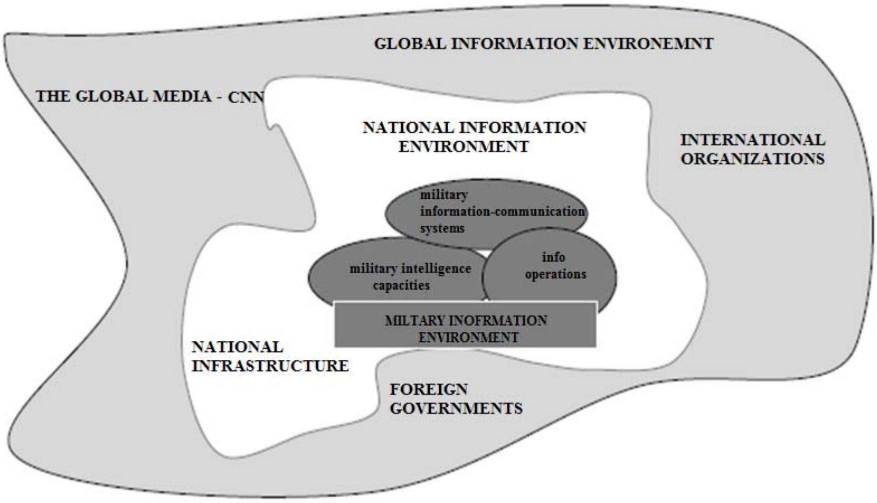
[20] Compare: *Planner's Handbook for Operational Design*, Joint Staff, J-7, Joint and Coalition Warfighting Suffolk, Virginia, 7 October 2011, p A-14; *Information Operations, FM 100-6*, Headquarters, Department of the Army, pp. 1-2, *Information Operations, Joint Publication 3-13*, 20 November 2014, p. GL-3

[21] Концептуальные взгляды на деятельность вооруженных сил Российской Федерации в информационном пространстве, Министерство обороны Российской Федерации, 2011 г. http://pircenter.org/media/content/files/9/13480921870.pdfp. 3

[22] Compare: Global Information Infrastructure, https://itlaw.fandom.com/wiki Global Information Infrastructure, The IT Law, Fandom; *Joint Doctrine for Information Operations (Joint Pub. 3-13),*U.S. Joint Chiefs of Staff, Oct. 9, 1998, at I-13 and I-14.

forces. The special emphasis is placed on the opponent's ability to break the potential information blockade established by security forces, as well as the international support for the opponent's communication and information system.

The national information infrastructure can be defined as the national interconnection of communication networks, computers and data bases which provides the users with large amount of information at their disposal.[23] The country's personnel who make the decisions and handle the transmitted information is a critical component of the national information infrastructure.[24] The national information infrastructure is, by its nature and purpose, similar to the global, but in terms of scope it only refers to the national information environment including the whole government and civilian information infrastructure.[25] The part of the analysis regarding the opponent's national information system, technical and other capabilities of national communication organizations are observed, as well as national radio, television and the Internet infrastructure. The ability to influence the global and regional dimension is also analyzed, as well as the proprietary properties of the national and regional media, whether they are and up to what percentage, the owners of the Internet servers, rooters and provider services.


GLOBAL INFORMATION ENVIRONEMNT
THE GLOBAL MEDIA - CNN
NATIONAL INFORMATION ENVIRONMENT
INTERNATIONAL ORGANIZATIONS
military information-communication systems
military intelligence capacities
info operations
MILTARY INOFRMATION ENVIRONMENT
NATIONAL INFRASTRUCTURE
FOREIGN GOVERNMENTS

Picture 2 – *The Levels (contexts) of the information dimension*

[23] National information infrastructure, US DoD Definition, https://www.militaryfactory.com/dictionary/military-terms-defined.ph,term_id3588 national information infrastructure (US DoD Definition) (militaryfactory.com)

[24] *National Information Infrastructure (NII),*https://itlaw.fandom.com/ National Information Infrastructure, The IT Law, Fandom, *Joint Doctrine for Information Operations (Joint Pub. 3-13),* U.S. Joint Chiefs of Staff, Oct. 9, 1998, at GL-7 and GL-8

[25] *Ibid,* I-14

The military information structure is a network of communication networks, computers, software, data bases, applications, but also facilities and people and other possibilities that satisfy the needs for information of military forces and defense forces in peace, crisis situation and during war.[26] While analyzing military-communication infrastructure and dimensions, the properties of the opponent's defense information system, its location, hardware and software standards of its telecommunication systems and capability of the defense information system to conduct information warfare and operations, as well as capability to collect relevant intelligence information. Regarding this capability, it is separately analyzed whether the opponent has developed the doctrinal-normative aspects of information warfare, whether organizations and groups for information operation have been established, as well as whether there are sufficient human and material resources for such operation.

Moreover, the American doctrinal theory points out that modern military forces are facing the problem of expansion of global information environment, as well as the expansion of national and military information infrastructure. In relation to that, it is stated that traditional borders between countries, between military and political domains, as well as military and civilian domains, are becoming more and more blurred in the information age. Due to the cross-border nature and architecture of global information networks where the information flow more or less freely across state borders, where national information infrastructures are becoming inseparable parts of global information infrastructure, the political borders, as well as the borders between military and civilian sphere are becoming porous. The battlefield expansion to virtual space and to human perception has led to greater involvement of civilian forces in modern conflicts. According to the future warfare scenario, typical military conflict is not the final goal, because the information dimension allows much lower expenses and better conditions for initiating conflicts covertly.[27]

The attitudes towards the classification and analysis of the levels of the information dimension into global, national and military, even though they are partly directed towards the analysis of technical characteristics of infrastructure, provide new quality by emphasizing the crucial significance of interconnectivity of these levels, especially the connections to global level, taking into account its significance and influence on the public opinion towards the conflicts, as well as the importance of people as a critical element of the analysis. The additional quality is provided by attitudes towards the need for the analysis of capabilities within the military level, for conducting information warfare and the influence on the global information dimension, focusing on the existence of the doctrinal-normative theory, organizations and groups, human and material resources for information operation.

[26] Compare: *Capstone Requirements Document: Global Information Grid 70* (GIG), JROCM 134-01, U.S. Joint Forces Command, Aug. 30, 2001, *U.S. DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*. U.S. Department of Defense, DoD Instruction 5200.40, Dec. 30, 1997.

[27] Myriam Dunn, *Information Age Conflicts A Study of the Information Revolution and a Changing Operating Environment*, Zurich, November 2002, P 38-39, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/ZB_64.pdf/ Information Age Conflicts (ethz.ch)

The analysis of capabilities of the information dimension actors

Theorists state that the information dimension actors can be divided into several groups based on their interests and activities. They are *individuals* who are given an unprecedented opportunity, by the new technologies, to become directly involved in public communications. Then, *the media* use both traditional and new channels for mass communication. Also, *private companies* that collect and maintain information by offering or selling the access to information. Then, *public and local institutions*. Next, *businesses* use communication channels for marketing and maintaining the relationships with their clients. Finally, *various interest groups* (including political parties, public organizations and associations) and other *non-state actors* who communicate with their participants and supporters.[28]

While analyzing the actors, the doctrinal military theory states that one of the main challenges in the contemporary information dimension and key initiator of activities within it is dramatic and constant diffusion of information and technologies used by individuals as well as minor and non-state actors and countries.[29] The low price for the activities carried out in the information environment, either via social media, official press, cyber activity or some other means, has given non-state and minor actors certain advantages and options for acting on an international scale, the ones they could only dream about twenty years ago. The diffusion of power enabled by information technology has enabled individuals and groups to influence global international sphere. The ability of information operation, for the purpose of social and political changes, used to be an exclusive power of states. Nevertheless, nowadays, even individuals have the ability to create, transform and share the information on a global scale, so as to mobilize social and political activities and changes.

Rapid information sharing questions the ability of certain countries to control their population and maintain internal political stability.[30] The access to information and information platforms, almost in real time span, gives the public the possibility and platform for impugning the legitimacy of actions of state authorities in crisis situations. These public forums can influence the public opinion and impose public evaluation of activities of security forces as unacceptable practice, as well as to increase the public's sensitivity to collateral damage.[31] It often occurred that the legitimate forces were

[28] Inta Brikše, *The information environment: theoretical approaches and explanations*, pp. 383-384. Brikše I (2006). In: Informācijas vide Latvijā: 21. gadsimta sākums. Riga: Zinātne, pp. 368–415. Available at: https://www.szf.lu.lv/fileadmin/user_upload/szf_faili/ Petnieciba/sppi/mediji/inta-brikse_anglu.pdf

[29] Joint Concept for Operating in the Information Environment (JCOIE), United States Department of Defense, 25 July 2018

[30] Robert Ehlers, *Making Old Things New Again: Strategy, the Information Environment, and National Security*, January 3,2017.

[31] Colin S Gray, *Recognizing and understanding revolutionary change in warfare: The Sovereignty of Context. Carlisle*, Strategic Studies Institute, U.S. Army War College, 1 February 2006. https://ssi.armywarcollege.edu/2006/pubs/recognizing-and-understanding-revolutionary-change-in-warfare-the sovereignty-of-context. 01/11/2021.

unprepared and incapable of answering to the large amount of multi-channel information actions and propaganda sent via text, video, audio or photos shared via the Internet, social media, satellite television and the traditional media.

Adaptable non-state actors skillfully use the information to get the edge over state actors. That requires the understanding of the information dimension and the activities carried out in it, i.e. the activities of information warfare.[32] Due to everything abovementioned, in the analysis of the information dimension actors, their ability to carry out the activities of information warfare and operations is analyzed separately, as shown in Table 2.

Table 2 – *The capabilities and activities actors operate with within the information dimension*

The types of information-operation activities	Activities	Target groups/aims	The aim of the activity	Who carries out the acti
Electronic warfare	Electronic attack	Physical/ information	To destroy, To disturb, To postpone	Individuals, Government institutions, Military
	Electronic defense	Physical	To secure the usage of electromagnetic spectrum	Individuals, Companies, Government institutions, Military
	Support activities	Physical	To identify and locate the threat	Military, Intelligence bodies
Computer-network operations	Computer offensive operations	Physical/ information	To destroy, To disturb, To postpone	Individuals, Government institutions, Military
	Computer defensive operations	Physical/ information	To protect the computer network	Individuals, Companies, Government institutions, Military
	Computer intelligence operations	Information	To collect information from the computer and the opponent's computer network	Individuals, Government institutions, Military
Psychological operations	Psychological propaganda activities	Cognitive	Influencing the opponent's emotions, behaviour and decisions	Companies, Government institutions, Military
Military deception	Deception	Cognitive	To deceive	Military
Operational security	The operation security of one's own forces	Cognitive	To negate	Companies, Government institutions, Military
Close related activities	Civil-military relations	Cognitive	Influence	Government institutions, Military
	Public businesses	Cognitive	To inform	Government institutions, Companies
	Public diplomacy	Cognitive	To inform	Government institutions

[32] Joint Concept for Operating in the Information Environment (JCOIE), United States Department of Defense, 25 July 2018.

The American military theory defines the information operation as the coordination of five central activities used to operate within the information dimension. These activities are psychological operations, military deception, operational security, electronic warfare and computer-network operations.[33]

The presented analysis of the information dimension actors, although having structural approach at its basis, with its qualitative attitudes on the abilities of individuals and non-state actors compared to state actors and military forces, provides additional quality and functional aspect of the information dimension analysis, emphasizing the importance of the analysis of operational capabilities in the information dimension, as well as shortcomings and weaknesses of state actors within these activities.

Using PMESII and ASCOPE matrices in the information dimension analysis

The militaries and intelligence-security services of western countries use different combination of models in order to improve the perception of environment.[34] These models, which are mostly based on the analysis of “national power instruments”, are also known as acronyms DIME, DIMEFIL, ASCOPE and PMESII.[35]

The method for the analysis of security environment, i.e. operational environment when speaking about military forces, called PMESII, is a holistic approach for the environment analysis developed by the U.S. Department of Defense in order to improve the analysis of external environment and to develop better strategies for the security threats in Iraq and Afghanistan.[36] The US Armed Forces Manual for conducting combat operations abroad, named FM 3-0, focuses significantly on the usage of the PMESII method for the analysis of the external factors which could

[33] Милан Миљковић, *Посебност информационих операција у раду савремених обавештајних служби*, Факултет Безбедности, Београд, 2016, pp. 29-30.

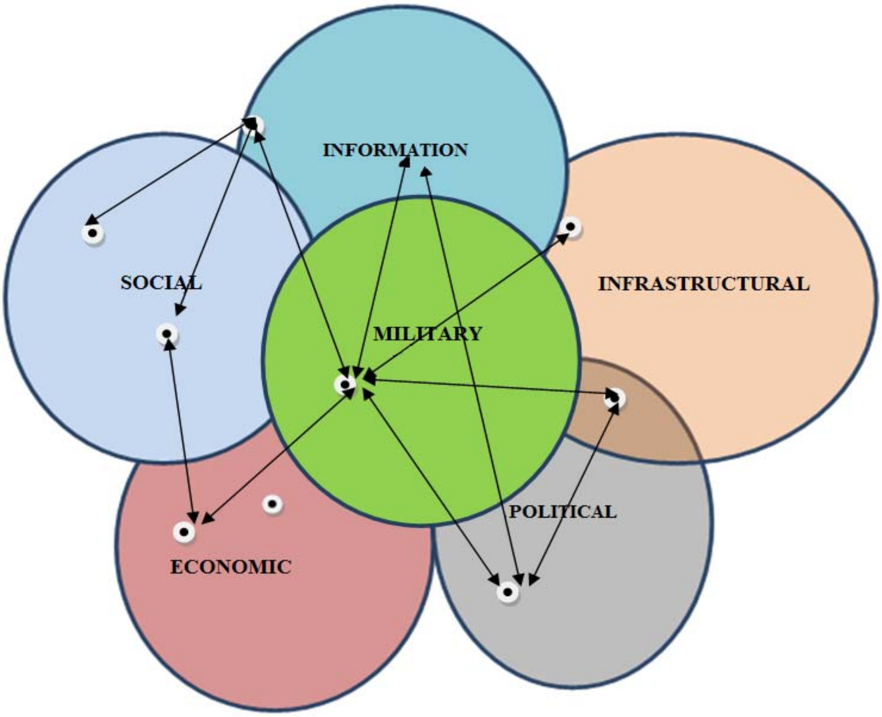
*Посебност информационих операција у раду савремених обавештајних служби (mpn.gov.rs)*https://nardus.mpn.gov.rs/handle/123456789/ 8473.

[34] Look at: Fred Bruls and A. Walter Dom, „Human Security Intelligence: Towards a Comprehensive Understanding of Complex Emergencies“, *Open Source Intelligence in the Twenty-First Century New Approaches and Opportunities,*
https://walterdorn.net/pdfHumanSecurityIntel_Bruls-Dorn_OSI-Book_Palgrave-Macmillan_June2014.pdf; Jack Kern, 'Understanding the Operational Environment: The Expansion of DIME, Military Intelligence (2007), Vol. 33, No. 2, p.l., https://www.proquest.com/docview Understanding the Operational Environment: The - ProQuest, 21/12/2021.

[35] Acronyms: DIME (*diplomatic, information, military and economic*); DIMEFIL (*diplomatic, information, military, economic, financial, intelligence and law enforcement*), ASCOPR (*areas, structures, capabilities, organizations, people and events*) и PMESII (*political, military, economic, social, information and infrastructure*).

[36] *Researching with pmesii-pt analysis*, Researching with PMESII-PT Analysis > DINFOS Pavilion > Article

influence American military operations.[37] This model has become a standard for the analysis of the external environment of peacekeeping operations carried out by the NATO member states.[38] The factor, i.e. the dimension explored by the PMESII method is the information dimension as well.



Picture 3 – *The security environment as a "system of systems" with interrelations*[39]

Philosophically speaking, this method is of great significance because it observes the security environment as a "system of systems", which interact with each other. In other words, the interaction of the information dimension with other dimensions of security environment is observed. The doctrinal theory points out that the information variable shows the nature, the scope and the effects of individuals, organizations and systems that collect, process, share or influence the information in the security environment. The

[37] Look at: US Army, Field Manual 3-0: Operations (Washington, DC, 2008).

[38] The *PMESII* method is one of the several techniques of the analysis of security environment, including: SWOT analysis (strengths, weaknesses, opportunities, threats), *PESTLE* analysis (political, economic, social, technological, legal and environmental), and *QUEST* analysis (the technique of rapid environment scanning).

[39] Ibid.

information environment considers formal and informal means of communication among people, as well as the usage of the effect of global information environment on a certain security environment. The examples of questions used for the analysis of connections with the information variable are: what is the nature of the public communication media; how controlled or open is the information environment; what are the opponent's possibilities for waging information warfare in specified operation environment.[40]

The PMESII method is often combined with the ASCOPE method. The combination of these two methods provides a useful tool for military forces, for the purpose of better understanding and analysis of security environment. Namely, the ASCOPE method is used for the analysis of civilian aspect of security environment in the following dimensions:

– *areas*: the analysis of influence of key civilian areas on military operations and vice versa;

– *structure*: the analysis of physical infrastructure, such as facilities, bridges, roads, railways, and communication towers;

– *capabilities*: the analysis of capabilities needed in the environment for the maintenance and improvement of life, such as food, emergency services, and health care;

– *organizations*: the analysis of approach, activity and organizational set of non-military groups and institutions in the environment, taking into account their influence on population, military missions and vice versa;

– *people*: the analysis of the civilians in the environment in the context of opinion, action and political influence;

– *events*: the analysis of the events in the environment which influence the population, military operations, non-military organizations, religious and national holidays and elections.

Due to the complexity of the table and the article theme, only the information dimension which was analyzed in accordance with the ASCOPE method will be presented.

Table 3 – *The analysis of the information dimension using the ASCOPE method*[41]

The analysis of the information factor– ASCOPE method	
Areas	– The area covered by a public broadcaster – The area with access to social media – The area where the method "through the grapevine" is used – The area where "graffiti" are used

[40] *Operational Environment and Army Learning*, Headquarters, Department of the Army, Washington, DC, 26 November 2014, pp. 1-6, https://armypubs.us.army.mil/doctrine/index.html

[41] *The conduct of information operations*, ATP 3-13.1, Headquarters, Department of the Army, Washington, DC, 04 October 2018, p. 2-6., https://irp.fas.org/doddir/army/atp3-13-1.pdf. 01/11/2021; *The application of COIN doctrine and theory,* A Counterinsurgent's Guidebook, Counterinsurgency Training Center – Afghanistan, KABUL, Version 2: November 2011, p 12. https://info.publicintelligence.net/CTC-A-COIN-Guidebook.pdf .11/12/2021.

Structures	– Mobile telephone service tower – Antenna or an object for TV and radio program transmitting – Physical Internet structure – The postal service – Printing
Capabilities	– The media operations – Printed press – Social media platforms – Literacy rate – Intelligence agencies – The Internet access
Organizations	– The media agencies – Public relations agencies and public opinion polls – Groups and agencies for social media – Press agencies
People	– Political decision maker – Supervisors – Religious leaders – The Internet influencers
Events	– Censorship – Publishing of important events and dates – Launching breaking news via the Internet – Press briefing – Taking the broadcasting off the air

The PMESII method, although based on the analysis of the information dimension elements, provides new quality of analysis, because it presents the nature, the scope, and the effects of individuals, organizations and systems that collect, process and act in the information environment. The application of the ASCOPE method enriches the analysis, taking into account that the familiar elements of the analysis are observed in a qualitatively different way and “the events of importance for the information dimension” are introduced as the element of analysis. These methods assist better organization, synthesis and application of the information as a key part of strategic thinking and decision-making.

The analysis of threats and possible opponent’s operation in the information dimension

After the aforementioned approaches of structural analysis, in the further text, the doctrinal approach of the information dimension functional analysis shall be analyzed, which helps presenting the influence of the information dimension on the activities of military forces in a more picturesque way, as well as identifying potential threats and weaknesses, which can be used by military forces in a conflict as the protection from these threats.[42] This analysis method model has four phases:

– Defining the information dimension,

– Describing the effects of the information dimension,

– The assessment of the information situation and threat, and

– Establishing the opponent's direction of operation in the information dimension.

Within the information dimension defining phase, the parameters of its three spheres (physical, information, cognitive) within the operation area of one's own forces are identified, specifically those that can influence one's own forces, i.e. those that could negatively affect the course of one's own operations and the decision-making process of one's own command staff. For that purpose, the following elements of the information dimension are analyzed:

– *terrain (and weather)* which influences the content and the flow of information from physical, geographical and atmospheric aspect,

– *population*, where the demographic and linguistic factors are studied,

– *social structures*, where informal social networks are identified,

– *state (authority) and military information-communication infrastructure* for the command purposes as well as for the authorities' decision-making purposes,

– *civilian information and communication infrastructure* which shares the information throughout the whole information environment,

– *the media within the operation zone* that can influence the operations of both one's own forces and that of the opponent,

– *independent and non-governmental organizations* whose attitudes differ from the official ones.

Within the second phase of describing the effects of the information dimension, the properties of the information environment, which were identified during the first step, are being analyzed for the purpose of determining their influence on one's own operations and the opponent's operations in every dimension. Same as previously, in this phase as well, the emphasis is placed on describing the possible influence of the activities of the opponent's forces, of terrain, of weather conditions, as well as of the civilian factors, on the activities of one's own forces. In this phase, it is important to determine the possibilities of the information operation of the opponent's forces, conceptual and doctrinal attitudes regarding the information operation, i.e. the capabilities for influencing the information dimension. Describing the way in which civilian environment could influence the operations of one's own forces and that of the opponent, assists choosing and determining the aims of one's own information operation (information attack, defense or stabilization) or a suitable combination of actions. The Table 4 illustrates the analysis of possible influence of the media, population and communication infrastructure on all the three spheres of the information dimension.

[42] *The conduct of information operations*, ATP 3-13.1, Headquarters, Department of the Army, Washington, DC, 04 October 2018, p. 2-1., https://irp.fas.org/doddir/army/atp3-13-1.pdf. 01/11/2021.

Table 4 – *The example of analysis of possible influence of the media, population and communication infrastructure on the areas of the information dimension*[43]

The media	**Cognitive**	The media broadcasters have an overall positive attitude towards our security forces and operations.
	Information	The media news covers approximately 68% of the population and focus primarily on reporting on cases of crime, corruption and social issues.
	Physical	The radio-infrastructure is outdated, the number of satellite equipment has decreased, a combination of stationary and non-stationary antennas for mobile telephone service is present.
Population	**Cognitive**	The support for the ruling party is partial. There is no open support for the actions of the security forces.
	Information	The population already exchanges information "through the grapevine", and it mostly shows interest in economic and social issues.
	Physical	75% of the population are Serbs, and 25% others. 65% of the population lives in urban areas.
Information-communication infrastructure	**Cognitive**	The population partially puts their trust in infrastructure.
	Information	Due to the unreliable infrastructure, the exchange of information is difficult so the population exchanges information to great extent via unreliable sources.
	Physical	Due to limited land communication network, mobile telephone service is used as an alternative. The towers of mobile telephone service are target for an attack which makes them unreliable.

Within the third step, *information situation and threats in the information dimension* are *assessed*. In this phase the opponent's possibilities for information operation, their doctrinal principles, tactics, and techniques are analyzed, including the way they deploy their forces for operation in this dimension. Ideally, the analysis of the opponent's operation in the information dimension is based on models and patterns. Two common tools used are determining the pattern of the opponent's information operation and the analysis of its "gravitation centres". The patterns of the opponent's information operation are the result of thorough analysis of the opponent's capabilities, weaknesses, doctrinal principles and desirable tactics, techniques, and actions which, as a result, lead to developing the models of the opponent's information operation. They are presented visually (on a map or a digital map), while respecting the basic doctrinal principles of the opponent's information operation and they usually comprise three different patterns:

– the pattern of decision-making or the opponent's information exchange,
– the pattern of the opponent's information infrastructure,
– the pattern of application of the opponent's information operation doctrine.

[43] *The conduct of information operations*, ATP 3-13.1, Headquarters, Department of the Army, Washington, DC, 04 October 2018, p. 2-11., https://irp.fas.org/doddir/army/atp3-13-1.pdf. 01/11/2021.

The opponent's decision-making pattern shows the "people's knots and relations" which the opponent uses for the information exchange, with special emphasis on the ways in which political and military leaders receive and exchange the information. In order to create this pattern, it is necessary to understand the opponent's organizational structures, important connections and interrelations among key personnel who influence the decision-making process. The opponent's information structure pattern shows the assets used for the information exchange. The pattern of the opponent's information operation doctrine models the way in which the opponent deploys or uses their own information resources and possibilities.

The fourth step in the analysis is *determining the direction of the opponent's operation in the information dimension* and it encompasses six-step procedure including: identifying the probable aims of the opponent and the final desired state in the information dimension, identifying all possible variants of the opponent's operation in the information dimension, the evaluation and gradation of each variant of the opponent's operation according to its significance, detailed modeling and elaborating of each variant of the opponent's operation, determining the aims of the opponent's information operation for each variant, and determining the data the opponent needs to initiate the planning of each variant of operation.

Although the opponent's operation patterns respect the opponent's doctrinal principles, typical methods and patterns of operation, they have to show how the opponent could operate by adjusting their forces, capabilities, and doctrine to a specific operation environment. The Table 5 shows the example of the opponent's information operation pattern.

Table 5 – *The example of the opponent's information operation pattern*

THE PATTERN OF THE OPPONENT'S INFORMATION OPERATION	
The aims of the opponent's information operation: – To prevent the opposing side from collection intelligence data. – To degrade the opponent's command and information system. – To encourage the dissatisfaction of civilians with the opponent.	
Public information	**Task**: To emphasize collateral mistakes and usage of unadjusted force by the opposing armed forces in the media. **Aim**: To discredit the mission of the opposing coalition. **Method**: The international media, local radio and TV.
Propaganda	**Task**: To influence the public opinion (displaced civilians). **Aim**: To disturb the coalition operations. **Method**: Printed propaganda materials, AM radio program, HUMINT officers.
Electronic warfare	**Task**: To disturb the opponent's armed forces radio communication at the opponent's tactical level. **Aim**: To prevent collecting data on one's own forces on the first line. **Method**: Electronic warfare unit.
Special operations	**Task**: To attack the opponent's command positions. **Aim**: To slow down the opponent's offensive operations. **Method**: Direct action, artillery fire.

The presented approach of the analysis of threats and possible opponent's operation in the information dimension is a more quality analysis, taking into account that its results should identify potential possibilities, threats and weaknesses in the information dimension which military forces could use in a conflict, i.e. to protect themselves. The special emphasis is placed on the significance of the analysis of pattern regarding the opponent's decision-making, as well as determining the possible directions of the opponent's operations in the information dimension.

Conclusion

The domestic military theory so far has not provided comprehensive understanding of the properties, or the classification and analysis of the modern information dimension of security environment. Namely, our doctrinal theory provided only the classification of the information dimension into cognitive, physical, and information area, only describing the elements of these areas in short terms without further understanding of their inner connections and relations. This is not a solid basis for quality analysis which would provide the military forces with basis for understanding and evaluation of possible way of the opponent's information operation. Foreign doctrinal literature provides more examples of classification and analysis of the information dimension of different quality levels.

When it comes to general properties of the information dimension, it can be concluded that its complexity and multidimensionality make the evaluation of the security environment more difficult. In connection with that, the analysis of the information dimension itself helps identifying threats with more accuracy, as well as potential information possibilities which military forces could use in a conflict.

The understanding of the foreign theoretical-doctrinal approaches to classification and analysis of the information dimension points out that one part of the approach concerns only with the partial structural analysis, providing insight into elements and areas only, only levels, or actors and their abilities to act in the information dimension, with low level of analysis of their inner relations and connections, thus making them insufficiently functionally applicable for military forces. It is positive that the aforementioned approaches point out to the significance of the cognitive area of the information dimension, as the most significant and crucial area of analysis and the target of the information operation. The approach which, structurally speaking, provides the understanding of the global, national, and military context of the information dimension, brings extra quality, because it provides understanding of the inner relation of these levels, as well as of relevant opponent's capacities and capabilities.

The analysis of the information dimension actors, with its qualitative attitudes on the capabilities of individuals and non-state actors compared to state actors and military forces, brings extra quality and functional significance stressing out the importance of analyzing the operation capabilities in the information dimension, as well as shortcomings and weaknesses of state actors in these activities.

The application of the PMESII method, although initially based on the analysis of basic elements of the information dimension (subjects, systems, and organizations), can be described as a quality analysis because it shows the nature, the scope and the effects of individuals, organizations, and systems that collect, process and act in the information environment. In addition, it is a useful tool for further understanding and analysis of the information dimension in which the security forces are located, especially in the opponent's environment. The application of the ASCOPE method enriches the analysis, taking into account that it observes the already familiar elements in a qualitative different way, and also introduces the „events of significance for the information dimension“ as the element of analysis. These methods assist better organizing and synthesis of the information as a key part of strategic thinking and decision-making.

The doctrinal approach, which is directed towards the analysis of threats and possible opponent's operation in the information dimension, is a functional analysis comprising four phases as follows: 1) defining the information dimension, 2) describing the effects of the information dimension, where PMESII and ASCOPE matrices are used, 3) assessing information situation and threat, within which the possible pattern and the doctrine of the opponent's information operation in a concrete situation are determined, and 4) determining the direction of the opponent's operation in the information dimension.

It can be concluded that only comprehensive analysis, which observes elements, areas, levels, actors and their operation capabilities in the information dimension, as well as the analysis of threats and possible opponent's operation in that dimension, can provide military forces with a complete image of the information dimension but also functional information about the possibility to influence the potential opponents by operating in this dimension and thus contribute to accomplishing both military goals and those of national security.

Literature

[1] *Allied Joint Doctrine for Information Operations*, AJP-3.10, NATO, 2015.

[2] *Capstone Requirements Document: Global Information Grid 70* (GIG), JROCM 134-01, U.S. Joint Forces Command, Aug. 30, 2001; *U.S. DoD Information Technology Security Certification and Accreditation Process (DITSCAP).* U.S. Department of Defense, DoD Instruction 5200.40, Dec. 30, 1997.

[3] Colin S Gray, *Recognizing and understanding revolutionary change in warfare: The Sovereignty of Context. Carlisle*, Strategic Studies Institute, U.S. Army War College, 1 February 2006. https://ssi.armywarcollege.edu/2006/pubs/recognizing-and-understanding-revolutionary-change-in-warfare-the sovereignty-of-context. 01/11/2021.

[4] *Critical Infrastructure Protection XV*, 5th IFIP WG 11.10 International Conference, ICCIP 2021, Virtual Event, March 15–16, 2021, Revised Selected Papers.

[5] Дејан Стојковић, „Израда стратегијских докумената Републике Србије у области безбедности и одбране”, *Војно дело*, 6/2018, стр. 180.

[6] *Доктрина информационной безопасности Российсой Федерации*, утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895, https://Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 09.09.2000 N Пр-1895) (утратила силу) | ГАРАНТ (garant.ru)

[7] *Доктрина Војске Србије*, Медија центар „Одбрана”, Београд, 2010, стр. 101.

[8] *Доктрина информационной безопасности Российской Федерации* (утверждена Указом Президента РФ № 646 от 5 декабря 2016 г., https://Совет Безопасности Российской Федерации, Доктрина информационной безопасности Российской Федерации (scrf.gov.ru)

[9] Fred Bruls and A. Walter Dom, „Human Security Intelligence: Towards a Comprehensive Understanding of Complex Emergencies", *Open Source Intelligence in the Twenty-First Century New Approaches and Opportunities,*
https://walterdorn.net/pdfHumanSecurityIntel_Bruls-Dorn_OSI-Book_Palgrave-Macmillan_June2014.pdf;

[10] Global Information Infrastructure, https://itlaw.fandom.com/wiki Global Information Infrastructure | The IT Law | Fandom;

[11] *Information Operations, FM 100-6*, Headquarters, Department of the Army, 1996.

[12] *Information Operations, Joint Publication 3-13*, 20 November 2014.

[13] Inta Brikše, *The information environment: theoretical approaches and explanations*, p 383-384. Brikše I (2006). In: Informācijas vide Latvijā: 21. gadsimta sākums. Riga: Zinātne, pp. 368–415. Available at: https://www.szf.lu.lv/fileadmin/user_upload/szf_faili/Petnieciba/sppi/mediji/inta-brikse_anglu.pdf

[14] Isaac R. Porche III, „Emerging Cyber Threats and Implications". *RAND Corporation* Santa Monica, CA, 2016.
https://www.rand.org/pubs/testimonies/CT453.html, приступљено 07.03.2022. године.

[15] Jack Kern, „Understanding the Operational Environment: The Expansion of DIME, Military Intelligence" (2007), Vol. 33, No. 2., https://www.proquest.com/docview Understanding the Operational Environment: The – ProQuest, 21/12/2021.

[16] *Joint Concept for Operating in the Information Environment* (JCOIE), United States Department of Defense, 25 July 2018.

[17] *Joint Doctrine for Information Operations (Joint Pub. 3-13),* U.S. Joint Chiefs of Staff, Oct. 9, 1998.

[18] Концептуальные взгляды на деятельность вооруженных сил Российской Федерации в информационном пространстве, Министерство обороны Российской Федерации, 2011.

[19] Милан Миљковић, „Изазови у раду обавештајних служби у информатичком добу", *Безбедност* 3/2020, стр. 148.

[20] Милан Миљковић, Драган Јевтић, „Сукоби у информационом простору из угла савремене војне мисли у Руској Федерацији – искуства за безбедност Републике Србије", *Национални интерес*, Београд, број 2021/2, стр. 108.

[21] Милан Миљковић, Драган Јевтић, „Сукоби у информационом простору из угла савремене војне мисли у Руској Федерацији – искуства за безбедност Републике Србије", *Национални интерес*, Београд, број 2021/2, стр. 107.

[22] Милан Миљковић, *Посебност информационих операција у раду савремених обавештајних служби*, Факултет Безбедности, Београд, 2016, стр. 29-30.

[23] Milan Miljkovic, Vangel Milkovski, „Challenges facing information environment in contemporary conflicts", *Archibald Reiss Days 2020*, Belgrade, 18-19 November 2020, Thematic conference proceedingsof international significance, University of Criminal Investigation and Police Studies Belgrade, 2020
/http://eskup.kpu.edu.rs/ dar/article/view/230/117, 08/11.2021.

[24] Myriam Dunn, *Information Age Conflicts A Study of the Information Revolution and a Changing Operating Environment*, Zurich, November 2002, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/ ZB_64.pdf/ Information Age Conflicts (ethz.ch)

[25] *National Information Infrastructure (NII),* https://itlaw.fandom.com/ National Information Infrastructure | The IT Law| Fandom *;*

[26] Нежданов Игорь Юрьевич, *Технологии информационных войн в интернете*, https://studylib.ru/doc/2333221 Технологии информационных войн в интернете (studylib.ru), 25/12/2021.

[27] *Operational Environment and Army Learning*, Headquarters, Department of the Army, Washington, DC, 26 November 2014. https://armypubs.us.army.mil/doctrine/index.html

[28] *Planner's Handbook for Operational Design*, Joint Staff, J-7, Joint and Coalition Warfighting Suffolk, Virginia, 7 October 2011, p A-14;

[29] *Researching with pmesii-pt analysis*, Researching with PMESII-PT Analysis, DINFOS Pavilion, Article. 12/12/2021.

[30] Robert Ehlers, *Making Old Things New Again: Strategy, the Information Environment, and National Security*, January 3,2017. https://thestrategybridge.org/the-bridge/2017/1/3/making-old-things-new-again-strategy-the-information environment-and-national-security, 25/10/2021.

[31] *The conduct of information operations*, ATP 3-13.1, Headquarters, Department of the Army, Washington, DC, 04 October 2018, p. 2-6. https://irp.fas.org/doddir/army/atp3-13-1.pdf, 01/11/2021.

[32] *The application of COIN doctrine and theory,* A Counterinsurgent's Guidebook, Counterinsurgency Training Center – Afghanistan, KABUL, Version 2: November 2011, https:// info.publicintelligence.net/CTC-A-COIN-Guidebook.pdf. 11/12/2021.

[33] Tomasz Kacała, „Military Leadership in the Context of Challenges and Threats Existing in Information Environment", *Journal of Corporate Responsibility and Leadership*, https://www.researchgate.net/publication/ 297751621, 08/12/2021.

[34] *US Department of Defense Strategy for Operations in the Information environment*, June 2016, DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf (defense.gov)

[35] US Army, Field Manual 3-0: Operations (Washington, DC, 2008).

Summary

The information dimension of the modern security environment is characterized by complexity, the abundance of unstructured information and numerous conflicts that are fought through information warfare. The stated complexity of the modern information dimension and the problem of correctly perceiving the security environment raises the question of application of modern and proven methods for their analysis. These methods are a useful tool for understanding the information dimension, especially if it is about a foreign or opposing environment, and they help organizing, synthesizing, and applying information as a key part of communication planning and strategic thinking and decision making.

Structural analysis of the information dimension includes the analysis of: a) *elements of the information dimension*, primarily information infrastructure, systems and devices for collecting, transmitting, processing and delivering information, information and their flows, as well as personnel and organizations performing various activities related to the information; b) *areas of the information dimension*, i.e. physical, cognitive, and information areas; c) *levels of the information dimension*, which are divided into global, national and military-security levels; and d) *actors of the information dimension*, primarily individuals, non-state and state actors, directing the analysis to their ability to act in the information dimension, i.e. performing information operations.

The functional phase of information dimension analysis, on the other hand, contains the following phases: 1) defining the information dimension, 2) describing the effects of the information dimension, using PMESII and ASCOPE matrix, 3) assessing information situation and threat, within which a possible pattern and the doctrine of information action of the opponent in a specific situation are determined, and 4) determining the directions of action of the opponent in the information dimension.

It can be concluded that only a comprehensive analysis, which considers all the elements of the structure of the information dimension, as well as the elements of functional analysis, provides the military with a complete understanding of the information dimension and functional information on the possibility of shaping the information dimension for the purpose of acting against the opposing forces easier accomplishing of gains.

Key words: *the information dimension, analysis, PMESII and ASCOPE method, the pattern of information action of the opponent*