Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI: 10.21474/IJAR01/7392
DOI URL: http://dx.doi.org/10.21474/IJAR01/7392
ISSN NO. 2320-5407

RESEARCH ARTICLE

INFORMATION OPERATIONS CENTER - TASKS AND RESPONSIBILITIES.

Zhivko Zhelev.

Manuscript Info

Manuscript History

Received: 11 May 2018
Final Accepted: 13 June 2018
Published: July 2018

Keywords:-
information operations, establish capabilities, Information Operations Center**.**

Abstract

Establish capabilities for conducting information operations by the armed forces of the Republic of Bulgaria is subject to the acceptance of conceptual and organizational approach to their development. The report presents the organizational approach, presents the structure, tasks and responsibilities of the Information Operations Center of the Armed Forces, which can be establish. It is inherently a strategic level in the planning and conduct of information operations in national format.

Introduction:-

Nowadays, the armed forces are faced with the necessity to function not only in the classical earth, sea and air environment, but also in a new and dynamically developing information environment. According to NATO publication MC 0422/4, 2012, "the information environment comprises the information itself, the individuals, organizations and systems that receive process and convey the information, and the cognitive, virtual and physical space in which this occurs"[1]. The same document also provides a definition of an information operation that is "a staff function to analyze, plan, assess and integrate activities focused on the information environment rather than a capability in its own right. As a staff function, information operations provides the Commander with an assessment of the information environment and a mechanism to plan and coordinate information activities on a continuous basis to achieve information effects in support of operational objectives"[2] Similarly, information operations in the AJP-3.10 Allied Joint Doctrine, for Information Operations have been defined as "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"[3].

These operations can be targeted both against decision-makers and against the automated management systems that provide them. And the effectiveness of such actions is determined by the degree of dependence of the decision-making process on such systems. These actions can aim to influence data, information and knowledge in three main ways:

1. Taking special psychological, electronic or physical actions that add, alter or remove information about the environment from the datasets of different individuals or groups;
2. By taking action to influence the infrastructure that collects, processes and stores information;
3. By influencing the process of obtaining, interpreting and using data, information and knowledge[4].

[1] MC 0422/4, NATO Military Policy on Information Operations, 2012, p.3.
[2] MC 0422/4, NATO Military Policy on Information Operations, 2012, p.3.
[3] AJP-3.10 Allied Joint Doctrine, for Information Operations, 2009, p. 23.
[4] JP 3-13 Information Operations, 2012, p. 19–21.

Corresponding Author:-Zhivko zhelev.

Achieving the objectives of information operations requires the creation of capabilities to conduct them in two main aspects:

1. Development of doctrines;
2. The development of the structures for planning and conducting information operations.

These structures are built on a strategic, operational and tactical level. The article proposes the possible organization and tasks of the Information Operations Center, which is the strategic level in planning and conducting information operations.

This center may be part of the Ministry of Defense. The reason for this is the essence of the information warfare, information operations and, in general, the information counter-discovery, constituting discreet collection, manipulation, dissemination and destruction of information on political, economic, infrastructure, social and military activities, both opposing forces and own and allied forces.

Analyzes of the similar structures in the NATO Armed Forces shows that the core activities of the Center should be:

1. Developing capabilities for conducting and participating in information operations (war);
2. Development of the regulatory framework for the Armed Forces for the preparation and conduct of information operations;
3. Training of soldiers for participation in information operations in national and multinational format;
4. Preparation of civilian specialists from departments and structures dealing with information operations;
5. Identification and counteraction of foreign information activities threatening national security;
6. Providing information security to the armed forces;
7. Developing tools for the impact of information operations on the conduct of defensive and offensive information activities, both in the conduct of joint operations and without the direct intervention of military forces;
8. Monitoring the information environment;
9. Preparation and conduct of situational games, including on a national scale for counteraction and protection against unfriendly information impact;
10. Coordination of all information activities in the Ministry of Defense, security services and other departments and organizations;
11. Selection and control of messages transmitted to approved news agencies and media;
12. Studying and developing the means and methods of information warfare and information operations

It would be a good idea for the Center to be taken over the responsibility of the Deputy Minister of Defense and to manage his work by an administrative head. The reason for this is the direct link between the activity carried out and the policy pursued by both the ministry itself and the political leadership of the country. That is why the participation of non-military representatives in the information operations center is also necessary. In addition, the latter may also be conducted without the direct intervention of military force. This will be determined by the goals and approaches to be achieved.

In order to ensure that the tools and techniques of information operations are applied in accordance with their purpose, it is appropriate to include the following structural elements in the center: an information environment monitoring group; a group for the planning and coordination of information activities; a cyber-defense group; a media group; a research and training group (figure 1).

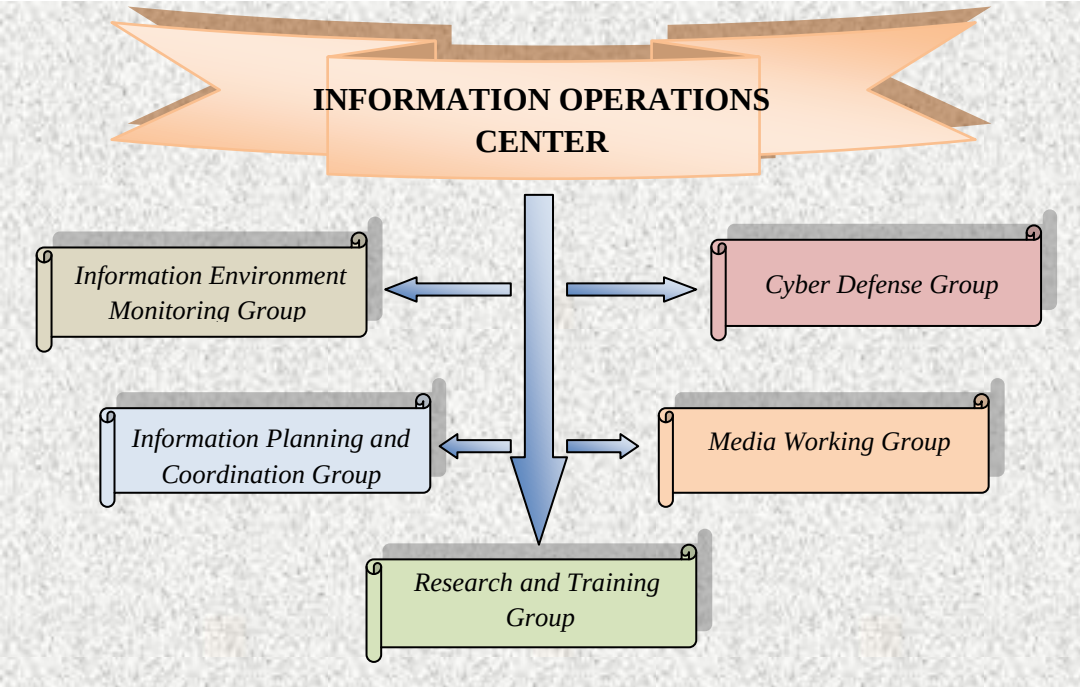

Figure 1:-Structure of the Information Operations Center

Information Environment Monitoring Group:-
The Group conducts tracking and analysis of information environment activities affecting national interests, focusing on potentially destructive action. Identification of possible sources of information aggression, the beginning and character of information attacks on governmental, financial, infrastructure, social, military or civilian objects on the territory of the country or located abroad, but related to national security. The group should also maintain a database of already malicious and hostile actions against the country and forecasting potential information attacks.

Information Planning and Coordination Group:-
The Group is responsible for planning, preparing and conducting all information activities at strategic level, developing information strategy and policy as a permanent instrument of national power, developing plans to counter information attacks against the country, and plans for active action against organizations and sites committed information aggression against the country. The Group coordinates and supports the interaction and work with international organizations to which the country is a member in the implementation of the Union Information Policy and the support of multinational joint information activities in the interests of the Union. The Group prepares opinions and advice to the country's political and military leadership on information security and state of the country. When the country is involved in armed conflict or the involvement of the forces of the country, it needs to be able to participate in the planning process at the strategic level, develop the guidelines for the development of information operations at the operational level. It directly supports/ the operations of the Operations Coordination Group.

Cyber Defense Group:-
The group is responsible for conducting operations on computer networks and the electromagnetic spectrum. Linking these activities is dictated by existing channels for broadcasting and retransmission of programs on both the air and the networks. It is also irrelevant the fact that individual components overlap and / or complement them. The group should support the development and development of approaches to protect its own networks and channels for the transmission and storage of information. Assist the development of security filters to influence the dissemination of information on the global network to and from the country, as appropriate, to track the activity of the main servers providing network operation, disseminated information and, if necessary, and to make recommendations for limit their harmful impact. The group provides monitoring the activities in the ether and to observe the normal operation of navigation systems serving state institutions, armed forces and private organizations, and to provide

recommendations for their security. The cyber defense group forms information security measures and develops approaches to recovering from cyber-attacks. In general, the group should direct its work to ensure the proper functioning of the state administration, transport, communications, energy, armed forces and the financial system.

Media Working Group:-
The group prepares and develops methods of interaction with the media in the interest of the country's information policy. It is responsible for the dissemination of information through electronic and printed media, their selection, and editing and presentation time. It selects media, editors and journalists to receive process and disseminate information from the country's government and the armed forces, subject to certain rules of conduct. The group forms the media approach to maintain a favorable public attitude towards government, armed forces, and self-acting allied operations. It analyzes the main stream of disseminated media information and develops approaches to neutralize or mitigate the negative impact on society and the armed forces. The group organizes periodic briefings, press conferences and meetings to reflect the activities of our armed forces when participating in coalition operations. The media working group prepares recommendations and proposals to monitor, discredit and limit the activity of malicious media, organizations and individuals in the interest of national security.

Research and Training Group:-
The group studies and develops the methods of information impact, organizes the acquisition of capabilities for conducting information operations by introducing innovative and non-standard approaches to impact or protection. The group develops the procedures and requirements for working with the different tools and techniques of information operations, forms approaches for protection against undesirable impact in the information environment and on the information infrastructure. It formulates the technical requirements for the upcoming information systems. The group prepares situational games to increase the readiness of specialists from different agencies to work under information impact conditions or in the interest of information operations. It analyzes potential impact approaches and offers procedures to limit the damage they cause. It conducts training of civilian specialists, especially journalists and computer specialists, as well as of military personnel for participation in the planning and conducting of information operations. The group participates in the development of new information weapons and tests how to use them against the military and political leadership of opposing forces. Periodically conducts military exercises that simulate attacks against their own information infrastructure. During the training session, it is looking for the weaknesses in the information security of automated systems with different applications. Selects and prepares personnel to work in the field of information operations of all kinds of armed forces.

Thus, the proposed structure and core responsibilities of the Center may be subject to change and development, but the formation of such a center would not only have a positive impact on the building and development of intelligence capabilities by the armed forces but also their involvement in a multinational format. In his face, a leadership structure will be set up to manage, coordinate and prepare the armed forces to conduct information operations and participate in information warfare. This would have a very dissuasive effect against any information and military aggression on the country. With the involvement of our armed forces in possible conflicts or operations in a national or multinational format, the information activities carried out would result in significant savings in resources and in the reduction of combat losses. On a purely national scale, defending the country from malicious information impacts would have a positive impact on political, economic and financial stability. The impact on the social sphere is also irrelevant. Protecting the performance of our own culture and values would have a profoundly beneficial impact on todays and future generations, which in today's globalizing world would contribute to the preservation of national identity.

Bibliography:-

1. NP-1, Doktrina na Vaorazhenite sili na Republika Bulgaria, MO, Sofia, 2017.
2. AJP-3.10 Allied Joint Doctrine, for Information Operations, 2009.
3. JP 3-13 Information Operations, 2012.
4. MC 0422/4, NATO Military Policy on Information Operations, 2012.