Bulletin of "Carol I" National Defence University
10.53477/2284-9378-22-78

FEATURES OF SMALL TACTICAL UNITS' ACTIVITIES IN THE INFORMATION ENVIRONMENT

Lt. col. Georgi Belchev, PhD*

This article discusses the challenges faced by small tactical units when operating in the information environment. Globalization, the development of communications and the complexity of combat operations increase its importance in conducting tactical activities. The article examines the characteristics of the information environment and some tools that can be used in the decision-making process. Additionally, some of the capabilities that small tactical units should possess are analyzed. Their importance derives from current capabilities and practical experience.

Keywords: tactical units; information environment.

Introduction

Tactical activities take place in the operating environment which retains its complexity of elements and interconnectedness. The fundamental domains of the operating environment are land, sea, air, space and cyberspace which are affected by actor's activities, facilities, population, geography, weather, terrain, natural disasters, the information environment, the electromagnetic environment (EME), and chemical, biological, radiological and nuclear (CBRN) threats and hazards (NATO, AJP-3.2, 2022, 1). In practice, the aforementioned elements do not exist independently, but they are inter-linked and many processes take place among them.

Nowadays, small tactical units are beginning to pay more and more attention to the information environment. In recent years this is a result of globalization and the connectivity of every part of the world. The majority of the population lives in cities, it has many means of communication, constantly exchanges data in various forms and has freedom of action. These facts make it much more difficult to control the dissemination of information, whether it is in the form of data, photos, video or voice communication. Therefore, the requirement is imposed on the small tactical unit commanders to understand the information environment, to raise their awareness and to build skills to meet the successful execution of the ordered activities. In this trend, the research in the present article is directed to the analysis of the conceptual apparatus and formulation of the capabilities necessary to conduct tactical activities in the modern information environment.

**Vasil Levski National Military University, Bulgaria*
e-mail: *gbbelchev@nvu.bg*

Information environment

One of the main concepts used in the present research is information environment. The term is not new, but it can be endowed with increasing importance for small tactical units. An information environment comprised of the information itself, the individuals, organizations and systems that receive, process and disseminate information, and the cognitive, virtual and physical space in which this occurs (NATO, AAP-06, 2021, 68; NATO, AJP-3-10.2, 2020, Lex-5). Information, as an element, can have physical or immaterial expression depending on how it is disseminated. Actually, there are more characteristics, most of them are the quantity of issues and the speed of dissemination, as well as the borders of dissemination. Each one is important and needs to be defined for each source or object in the environment. In addition to the objects and subjects in the information environment, the regulatory frameworks governing public relations in this sphere are also important. In this case, we can talk about censorship or limiting the spatial dimensions of the environment. Therefore, if we have discovered an object that collects information, but at the same time we know that it cannot disseminate information freely, then its influence is excluded or eliminated.

However, in modern conditions, it is very difficult to define the boundaries of the information environment. Global communications work constantly and people from different places exchange data constantly. If information is obtained in one place, it can be disseminated to the other end of the world. This feature contrasts with the spatial parameters of the area of operation. In these conditions, the work of the small tactical unit commanders will be significantly more difficult and, in most cases, it cannot even enter their combat powers. Therefore, when carrying out tactical activities, the possibility of disseminating information outside the area of responsibility should be taken into account and, in addition, structural elements within the area should be affected.

with quantitative indicators for each object. The characteristics are with different content and the determination of weight coefficients is necessary. For example, the commander should assign ratings for each characteristic from 1 to 6 with each value having a description of what it contains. In this case, a value of 1 can mean for the quantity of issues – a minimum amount, and for the speed of dissemination – very slow. Accordingly, the opposite value is assumed for the value 6.

For the dissemination area, the values need to be related to certain spatial dimensions. For example, for value 1 – the dissemination area is within the settlement's borders, value 2 – the dissemination area goes up to 20 km^2, value 3 – the dissemination area goes up to 40 km^2 etc. This

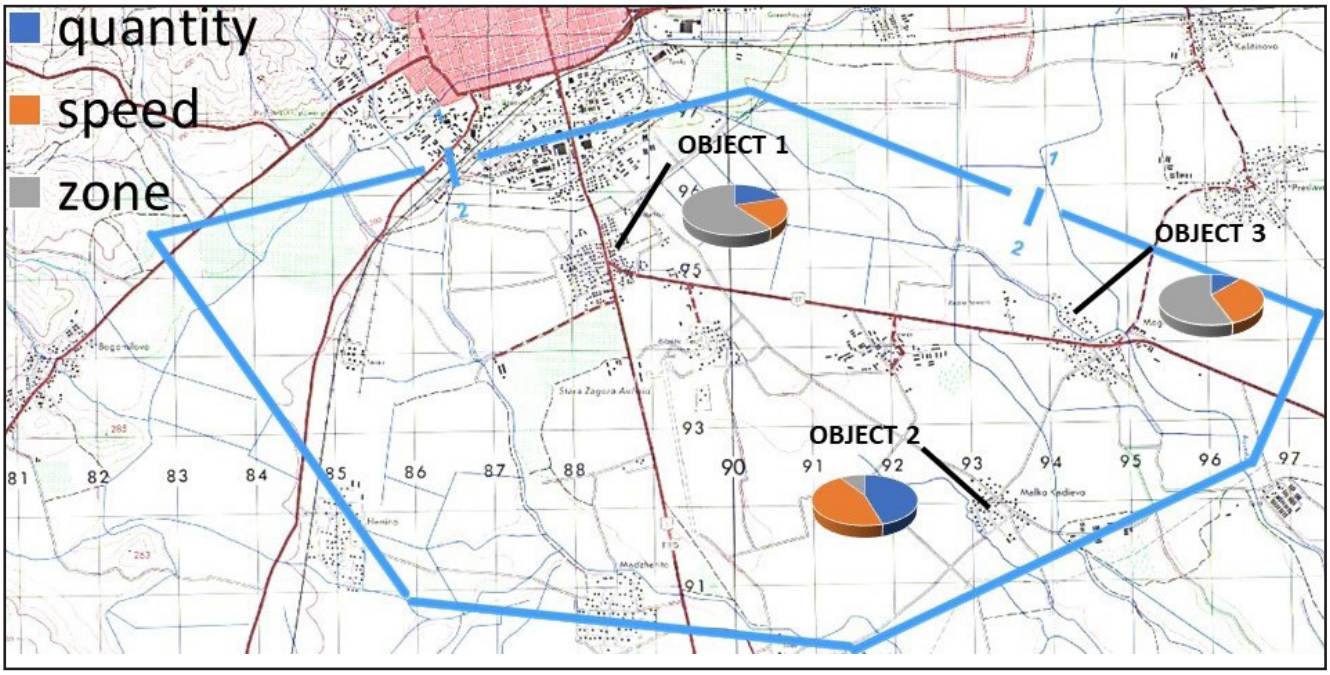

Figure 1 *Information objects model for the area of operation*

Referring to the results of the information environment analysis, a proposal for a tool can be defined when planning a given activity in an environment where information environment is essential. In the mission analysis, it is important to determine the objects that receive, process and disseminate the information and to develop a model of the area. To visualize the explanations about the current research we compiled figure no. 1.

The area of operation boundaries and the objects that receive, process and disseminate the information are present in this model. The quantity of issues, the speed of dissemination and the borders of dissemination (zones) are determined

activity needs to be performed before planning the tactical activities or the operation. It is appropriate to draw up an operating procedure or instruction in which the values of the three characteristics of the information objects are described. In this way, each commander can easily compile the presented model and make a real assessment of the information environment.

The location of each object should be indicated with grid or with a line as shown in Figure 1. This will reduce the spatial error when determining its location. In the case that the object changes its position, an area in which it is most likely located can be determined.

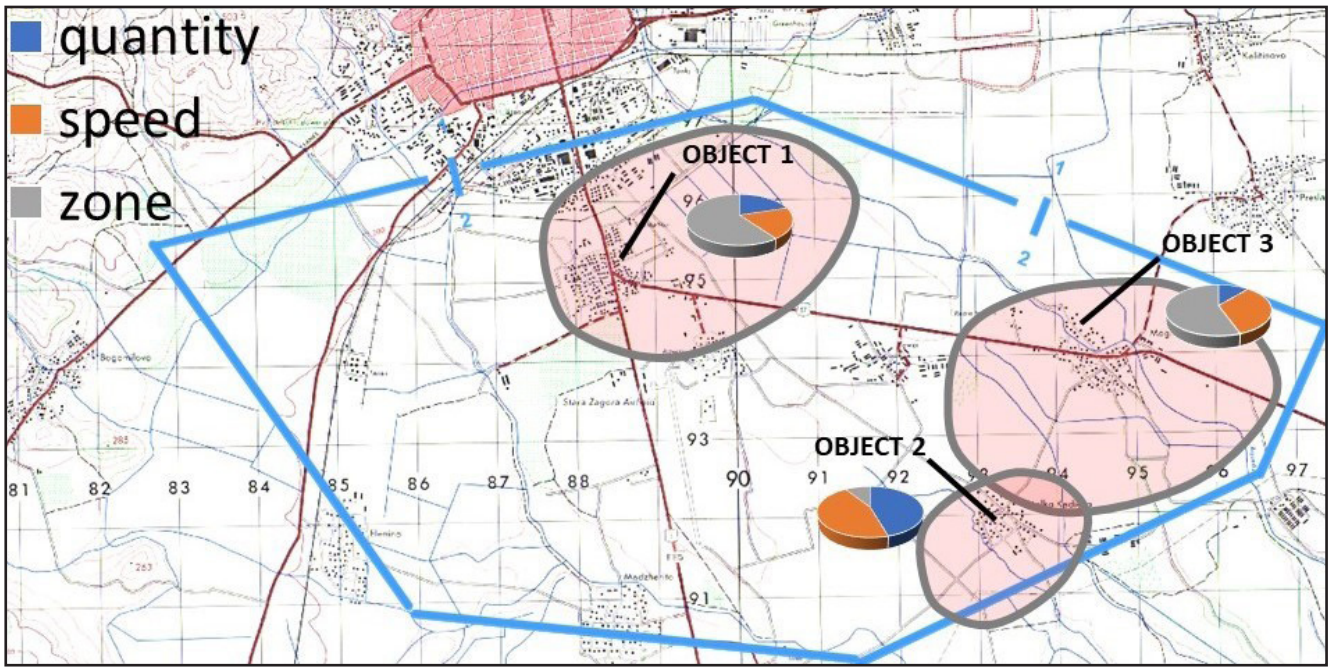

Figure 2 *Information dissemination zones for objects in the area of operation*

Additionally, depending on the "zone" indicator, spatial parameters can also be defined to be graphically represented in figure no. 2, which is compiled to visualize the explanations about the current research.

The development of the terrain information model can provide information on which areas are appropriate to conduct operations without the opposing forces gathering data about them. At the same time, zones can be formed where activities could be easily detected and future activities and their likely nature predicted. Therefore, during planning, these areas should be avoided or the presence of own forces should be reduced. For better results, the zones that each object collects information from should be marked on the map. If the intended activities should be misleading or false, then the opposite solution should be sought to be induced. In this case, it is necessary to plan deception activities where the adversary will necessarily discover friendly forces and receive information about their activities, thereby misleading him.

Areas where operations take place are usually saturated with sensors that receive and transmit information. In these conditions, it is also important to indicate the degree of credibility. Each person perceives the same data in a different way, and there is a great possibility that it will change when transmitted again, depending on his social status. This is one of the most important features of the information environment, namely the exchange of information and its distortion or misunderstanding.

Analyzing the process of information exchange, or how we transmit and the opponent receives messages, we reach the next important point related to the information environment. These are its domains: physical, virtual, and cognitive (NATO, AJP 3.10, 2015, 1-2). In practice, they cannot be defined and visualized, but only their essence can be described. The three domains also exist in normal life, but most people do not even think about their importance and continue to receive and disseminate information in various forms. To visualize the explanations about information flow through the three domains we compiled figure no. 3.

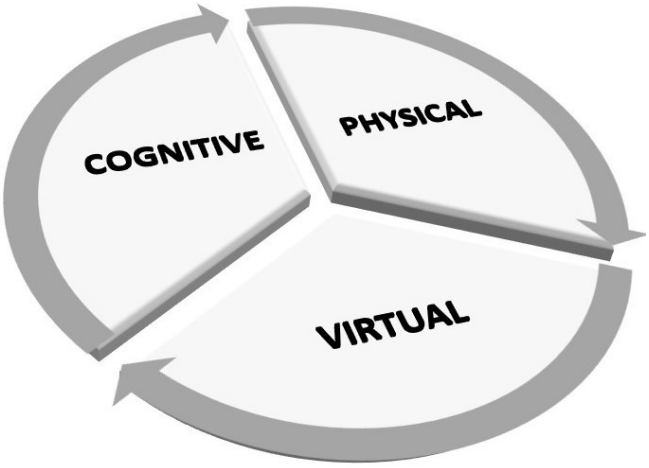

Figure 3 *Information environment domains*

In the information environment, every single object or organization collects information that is processed, filtered and arranged. As a result, the data is structured and recorded on different types of physical media.

The physical domain is what is seen and can be transmitted in any material form. It relates to the ability of people to perceive data through their senses. Usually, the physical dimension is the totality of all media such as newspapers, photos, documents, video, audio, articles, TV shows, reports, events/facts and others. These items provide data that can be collected whether or not the collector finds them important. Suffice that they are related to the operation which is being conducted or will be conducted.

The virtual domain is represented by a set of data that provide the necessary information to conduct of tactical activities. In another sense, this domain is the content of its physical and structural forms and its main element is the information. The information can be processed, arranged, transformed and disseminated. Additionally, the information is an object of protection from adversary forces that seek to acquire, destroy or replace the data in it. With this activity, the information protection function is implemented, which ensures security during conducting operations. Typically, these capabilities are built at the battalion level and above, that have the appropriate sections and personnel to do this.

The cognitive domain provides the link between the other two domains. This area of the informational environment is imaginary and is the most difficult to understand. Unlike the other two domains, the cognitive domain is entirely in the area of human understanding and functional areas. This means that it is difficult to develop a reliable software or similar virtual product that can implement the necessary activities in this area. Usually, the skills of personnel are formed based on the social, cultural, religious and historical characteristics of the society to which they belong. Globalization, to a certain extent, reduces this feature, but nevertheless each person remains more or less attached to the upbringing he received in his native country. The cognitive domain makes it difficult to predict the activities of the opposing forces due to the fact that it cannot be determined how they can perceive data from the physical forms of information. Therefore, planning tactical activities is drastically more difficult and the risk of their implementation increases.

Nowadays, civilians and media of all kinds are an invariable part of the battle areas. At the same time, the smart devices they have at their disposal allow taking video and photo footage from a distance without even being noticed. The dissemination of acquired data happens instantly without wasting hours of data transfer. All these conditions require tremendous acquisition of capabilities by small tactical units that are adequate to the environment.

Small tactical units' capabilities

There is a variety of opinions about these capabilities, depending on the hierarchical levels. The next few paragraphs will introduce thosem that should be possessed by the small tactical units for which this article is intended. Identification of small tactical units' capabilities is based on analysis of NATO and US Army publications. The main capabilities and techniques for activities in the information environment are: presence, profile and posture, soldier and leader engagement, military deception, soldier camera, destruction and lethal action.

Presence, profile and posture are used to describe and characterize a set of elementary tactical activities performed to achieve the necessary aims (NATO, AJP 3.10, 2015, 1-12). Presence relates to the units' physical presence on the battlefield or in the area of operation. This is one of the most common methods of influencing the adversary's intentions. Presence in some cases can interrupt an adversary's intention. The use of this element haphazardly is not advisable and must be in accordance with the requirements of the senior commander. The planned presence or absence in a certain area, as well as its periodic implementation, could contribute to the achievement of the planned aims or deceive the enemy in his planning.

Profile is the value by which the presence of the units is measured. In other words, it determines the quantity and quality of troops that perform the main tasks. A profile is a tool that can be used to manipulate enemy intelligence about one's own presence on the battlefield. In certain situations, it is necessary, with the available forces and means, to create the impression of a much larger number

of units, by conducting successive maneuvers of the same units. This activity is associated with military deception, which to a certain extent gives a wide field in the planning and execution of this capability. In most cases, own forces always try to hide or not show all the availability of forces and assets in the area. This activity is performed when the enemy should not determine our main intention, direction or area in which we have concentrated our efforts. Unlike presence, profile gives commanders the freedom to demonstrate their combat skills in tactical mission settings.

Posture is the third element of the capability analyzed and embodies the content of the message we want to send with the presence and profile we have implemented. In certain cases, we may seek to convey hostility, in others a friendly intention. Of course, this all depends on the specific mission or main objectives. Achieving these goals is done with elementary activities such as carrying additional equipment and weapons, behavior of individual soldiers, intimidation and others. Normally, profile and posture are conducted under specific instructions and cannot be changed in large limits because it will disturb the achievement of the major objectives. In such situations, posture is an element that can be manipulated and used by commanders to realize the freedom of their decision and their intent.

Presence, profile, and posture make up therefore a set of interconnected capabilities that enables commanders, within the objectives of the operation in which they are engaged, to define and implement their intentions without exceeding the overall framework.

Soldier and leader engagement make up an individual capability (NATO, AJP 3.10, 2015, 1-15). In practice, it is usually implemented by the commander, whose behavior is supported by his unit. This capability cannot be carried out haphazardly, but must be consistent with the overall objectives of the operation. Typically, soldier and leader engagement use personal behavior to convey messages and information when establishing contacts with the local population. The performance of this capability requires preliminary training to avoid mistakes and misunderstanding of the transmitted information. In most cases, soldier and leader engagement are part of information operations and adhere to their requirements.

Military deception is a part of every tactical activity in the information environment (NATO, AJP 3.10, 2015, 1-13). Its forms are usually implemented in a complex manner – concealment, imitation, disinformation and demonstration. Each of them has its advantages and disadvantages, which predetermine their place in the sequence of tactical activities performed. Concealment is associated with camouflage and deceives opposing forces about our presence on the battlefield and the location of own positions. Imitation is used when we want, with little effort and resources, to create the illusion of the presence of a much larger unit. Disinformation is usually associated with information operations and its aim is without using the resource of units to deceive the enemy about our presence or absence on the battlefield. Demonstration is the use of forces and means to perform deceptive maneuvers without getting in contact with the enemy.

Military deception can be used for an individual soldier, equipment, unit, data, and information exchange. It is necessary for the commanders, when planning each activity, to rely on the use of methods of military deception (US Army, FM 3-13, 2016, 9-3). Their focus is on adversary intelligence and decision-making teams. In this way, they can be misled, causing their activities or inaction to benefit the operation which is conducted by our own forces. Military deception should not be conducted haphazardly and should be coordinated with the higher authority. In this way, wrong decisions in the execution and main plan of the operation will be avoided.

In certain cases, it is concluded that the information disseminated in the information environment can be altered or used for propaganda purposes. This is largely used to manipulate the local population to oppose and sabotage our activities. Using cameras to record the actions being performed is a capability that can reduce this problem (US Army, ATP 3-13.1, 2018, 3-3). The video footage obtained can be used to contradict the reports and reveal the true intentions of the commander in conducting the operation. This capability should be used within certain limits and when it is necessary, as it can go to undesired effect.

Destruction and undertaking lethal actions are a very finite capability that can be used in

the information environment (US Army, ATP 3-13.1, 2018, 3-2; Michael, 21, 4). Its main purpose is usually to intimidate and create chaos in the opposing forces. Disadvantages related to the consumption of resources and the danger of collateral damages and casualties reduce the effectiveness of this capability, which causes its less frequent use.

Military information support operations, civil affairs operations, electronic warfare, cyberspace operations and others are also presented in the sources used for this article. They are excluded due to the fact that they are not used by the small tactical units targeted by the research.

Conclusions

Information environment nowadays has been increasing its size, complexity and speed of data dissemination. This requires its decomposition, analysis and evaluation. An analysis about the domains (physical, virtual, cognitive) and relationships among them in the information environment is conducted in the article. It would help commanders and their personnel to conduct tactical activities. At the same time, small tactical units' education and training should be aimed at acquiring capabilities and techniques give an adequate response to threats and challenges, as well as ensuring the appropriate speed and synchronization of activities. The main capabilities and techniques for activities in the information environment are as follows: presence, profile and posture, soldier and leader engagement, military deception, soldier camera, destruction and lethal action. Each one of them is analyzed and additional information is given.

BIBLIOGRAPHY

Department of the United States Army. 2018. *ATP 3-13.1 The Conduct of Information Operations.* Washington, DC: Department of the Army. [in English].

Department of the United States Army. 2016. *FM 3-13 Information operations.* Washington, DC: Department of the Army. [in English].

Department of the United States Army. 2021. *Soldier and Leader Engagement.* Washington, DC: Department of the Army. [in English].

NATO 2015. *AJP-3.10 Allied Joint Doctrine for Information Operations.* [in English].

NATO 2020. *AJP-3.10.2 Allied Joint Doctrine for Operations Security and Deception.* edition A, version 2. [in English].

NATO 2021. *AAP-06 NATO Glossary of Terms and Definitions.* [in English and French].

NATO 2022. *AJP-3.2 Allied Joint Doctrine for Land Operations.* edition B, version 1. [in English].

Schwille, Michael, Welch, Jonathan, and others. 2021. *Handbook for Tactical Operations in the Information Environment.* [in English]. Santa Monica: RAND Corporation, 2021. ISBN: 978-1-9774-0759-7.