HADMÉRNÖK

IV. Évfolyam 3. szám - 2009. szeptember

Haig Zsolt
haig.zsolt@zmne.hu

INTELLIGENCE AND ELECTRONIC WARFARE ON THE DIGITAL BATTLEFIELD[1]

Absztrakt/Abstract

A cikk bemutatja a felderítés és az elektronikai hadviselés helyét és szerepét az információs műveletekben. Kiemeli az összadatforrású felderítés jelentőségét, és ismerteti a SIGINT és az elektronikai hadviselés kapcsolatát az információs műveletek rendszerében

The article introduces the place and role of the intelligence and electronic warfare in the information operations. It emphasizes the significance of the all-source intelligence and introduces the connection between the SIGINT and the electronic warfare in the system of information operations.

Kulcsszavak/Keywords: *elektronikai hadviselés, összadatforrású felderítés, információs műveletek, rádióelektronikai felderítés ~ electronic warfare, all-source intelligence, information operations, signal intelligence*

Introduction

The modern armed forces use the electromagnetic field in a wide range for communication, weapon control, intelligence, navigation and force protection. The electronic devices used in these fields increase significantly the application possibilities of military forces. As a result of this the commanders controlling military operations have to pay accentuated attention to the use of the electromagnetic spectrum in their area of responsibility and their area of operations.

On the battlefields nowadays – also so called electronic battlefield or digital battlefield regarding the operations in the electromagnetic dimension – there are numerous electronic devices with different types and designation. These devices work in that information- and electromagnetic environment that makes it necessary to intensify the interoperability capabilities between them.

[1] The paper has been supported by the Bolyai János Research Scholarship of the Hungarian Academy of Science

1. Intelligence and electronic warfare in the information operations

By now in the modern military operations the different infocommunications devices have become indispensable. These devices operate in the digital battlefield, in a solid military information environment, that makes it possible for the commander to have more correct information in real time and to be able to use them in a proper way.

Digitization is the application of information technologies to acquire, exchange, and employ timely digital information throughout the battlefield, tailored to the needs of each decider (commander), shooter, and supporter allowing each to maintain a clear and accurate vision of his battlefield necessary to support both planning and execution.

Digitization provides the warfighter with a horizontally and vertically integrated digital information network that supports unity of battlefield fire and manoeuvre and assures command and control decision-cycle superiority. The intent is to create a simultaneous, appropriate picture of the battlefield at each echelon-from soldier to commander-based on common data collected through networks of sensors, command posts, processors, and weapon platforms. [1]

The ambition to coordinate the operations on the digital battlefield, in a military information environment lead to a revolutionary theory and mentality, which is nothing else than the concept of the information operations. According to this concept the gathering, transmitting, processing, storage and use of the information practiced during the military operations as well as to defend one's own information capabilities and to obstruct the similar systems of the opposite forces along solid principals can result a far bigger success than ever.

„**Information operations** are co-ordinated military activities within the information domain to affect information and information systems to achieve desired effects on will and capabilities of adversaries and others in support of mission objectives while sustaining own information and information systems." [2]

According to the US information operations doctrine: „Information operations are described as the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own." [3]

The two definitions of information operations have in common that they all imply on affecting the information, information systems while protecting one's own.

The main objective of information operations is to achieve information superiority between the friendly decision cycle and that of the adversary. The application of information operations enhances battlefield visualization and improves designation of main effort, control of operational tempo and synchronization.

The core elements of information operations are:

- electronic warfare;
- computer network operations;
- psychological operations;
- military deception and
- operations security.

It should be mentioned that according to some other information operations doctrine, the physical destruction is an element of information operations too.

The information operations are supported by the all-source intelligence and communications and information systems (CIS).

Although electronic warfare has been placed as an action component of information operations, electronic warfare crosses all aspects of information operations and several of the other combat functions.

Electronic warfare „refers to any action involving the use of electromagnetic or directed energy (DE) to control the electromagnetic spectrum or to attack the enemy. EW includes three major subdivisions: electronic attack (EA), electronic protection EP, and electronic warfare support (ES)". [4]

In general these components provide protection, exploitation, disruption and denial of information within the electromagnetic spectrum.

Nowadays the intelligence of the enemy, the terrain, the weather and other – combat effecting objective factors materialize mostly through electric devices. On the battlefield there are numerous intelligence devices with different types and designations. According to this there is a demand that the data gathered this way should be summarized, evaluated, harmonized on given levels and the data have to be accessible for the users. This demand is supplied by the all-source intelligence that supports the information operations.

The **all-source intelligence** is „intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data in the production of finished intelligence. In intelligence collection, a phrase that indicates that in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked." [5]

The different types of all-source intelligence are:

- human intelligence (HUMINT);
- imagery intelligence (IMINT);
- signal intelligence (SIGINT);
- measurement intelligence (MASINT);
- technology intelligence (TECHINT);
- open-source intelligence (OSINT).

The **data fusion technology** of the all-source intelligence assures the gathering, processing, summing up of data collected by different detecting range sensors and the dispensation of results. Hereby the information become more authentic and for example the efficiency of the adverse deception can be cut back significantly, because instead of the former single source intelligence it is possible to get data from different sources of the given target (for example radar intelligence, imagery intelligence, communications intelligence, etc.).

The information operations, the intelligence and the electronic warfare are tightly related just as much they are related with military operations. This connection realizes on one hand with the deliverance of data and target designation information, on the other hand through the fact that the effect of operations happening on one field deal to reach the goal of another field.

The existence of continuous, correct, detailed and real time information is the indispensable condition of the effective sequence of the information operations, which is supplied by the all-source intelligence. The intelligence give a basic support to the information operations by assuring the dissection of the enemy's command and control systems, define its information operation capabilities, and give a feedback on the efficiency of one's own fulfilled tasks.

The all-source intelligence is able to suffice the general and specific intelligence requirements of the information operations. The general **intelligence support of the information operations** means that the intelligence gets all the general information that is necessary to command and control the information operations. The general intelligence demand of the information operations includes the gathering of all those information about the enemy and about the battlefield environment that support the successful realization of the information operations.

The **specific intelligence support of the information operations** means that the intelligence gets all the intelligence information and specific target data that are necessary for the successful realization of the core elements of information operations, namely operation security, military deception, psychological operations, electronic warfare and the computer network operations.

The information operations, especially the electronic warfare as one of its core elements, have a relatively big target information demand. These information on one hand are supplied by the electronic warfare support within the confines of electronic warfare, in form of so called combat information, on the other hand information gathered and valued during the all-source intelligence assure the continuous service of the electronic situation database.

2. The connection between the SIGINT and the electronic warfare

Among the types of all-source intelligence, the SIGINT is in tight connection with the electronic warfare. SIGINT is nothing else, than the intelligence of the enemy's communication (e.g. radio) and non-communications (e.g. radar) devices emanating electromagnetic energy and so it also consists of the communications intelligence (COMINT) and the electronic intelligence (ELINT).

The electronic warfare support – similar to the SIGINT – gets its information from the electromagnetic spectrum used by the enemy. The electronic warfare support provides information about how the enemy uses the frequency spectrum, to sense, identify and use the enemy's deliberate (radio) and non deliberate (infrared radiation of vehicles) emissions.

The fundamental difference between the SIGINT and the electronic warfare support is based on what they use the gathered information for. The electronic warfare support supplies **combat information** which can be used for electronic attacks, artillery and air attacks, for maneuver of the troops, or for prevention of a threat. All this subscribed by the fast analyzing and processing of the electromagnetic signals and the relatively short validity time of the information. At the same time SIGINT provides **intelligence information** based on detailed evaluation and on longer validity time for the commander's decision support. [6]

For the effective fire support the accurate target designation data are also indispensable, which structure is similar to the target information of the electronic warfare. According to this it is obvious that in order to provide the necessary target information for the electronic warfare on one hand combat information of the electronic warfare support is integrated in the all-source intelligence, on the other hand the electronic warfare has an access to the above mentioned intelligence information from this system.

The combat information supplied by the electronic warfare, respectively the intelligence information of SIGINT can be reached through the same data gathering devices. The basic difference between them lies in the depth of the process and in the validity time of the information. Figure 1. depicts the relationship of information operations, SIGINT and electronic warfare.

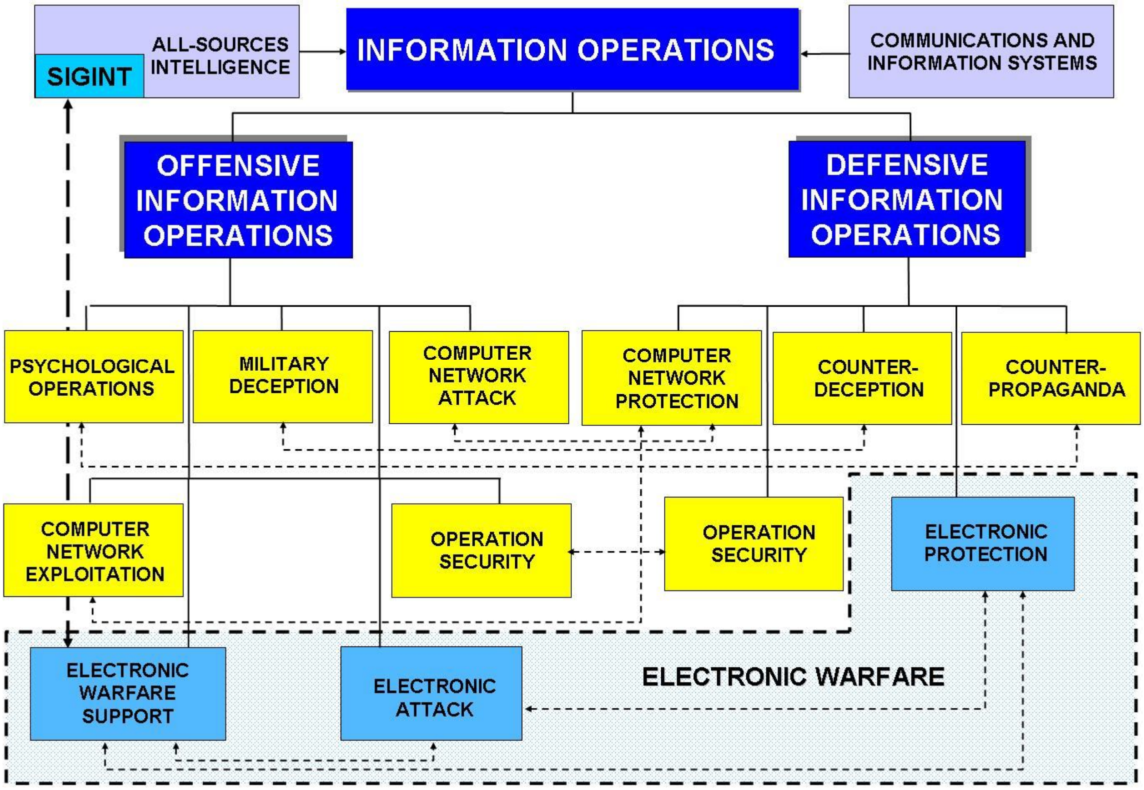

Figure 1. The relationship of information operations, SIGINT and electronic warfare

The electronic warfare support and the SIGINT have to face several technological challenges that put them in a huge task. Low Probability of Interception (LPI) technologies appeared and they spread further such as: spread spectrum systems (direct-sequence spread spectrum - DSSS, frequency hopping spread spectrum – FHSS). The spread of these systems and the exceptional development of the electronic cryptography make the solution difficult of the information content of the encrypted electronic emissions.

These challenges eventuate that the formerly used methods of the SIGINT – and especially these of the communications intelligence (COMINT) – can be used less and less. The modern intelligence devices are basically able to detect the signals of these digital emissions, respectively to define the location of the emissions.

To get the high speed (its parameters fast changing) emissions such receivers are used that process the whole spectrum in one time. So are the Bragg-cell receivers and the digital filter bank receivers based on the theory of the matrix receivers. In the last years the waterfall display has been developed in order to monitor the frequency hopping transmission, and it shows the received signals in frequency-time range.

In case of the interception of the modern methods of transmission none of the above mentioned tools or methods can be used (or only with a slight probability) for radio traffic analysis and content analysis. This decryption task needs a special apparatus and the most modern technology and a huge calculation capacity that can not be used in case of tactical and operational level COMINT. [7]

Due to this fact the primary identifier parameter for the COMINT is not the information content but the "electromagnetic fingerprint" left by the emitter. This means that the

COMINT as an operation form becomes ELINT type, namely it can only define the parameters of the signals and the location of the emission. Inasmuch as there is no possibility to figure out the information content, the further monitoring of the radio traffic becomes senseless. Instead these intercepted radio systems have to get disrupted by an electronic attack (for example electronic jamming). If we parallel look at the functions of the electronic warfare support we can tell that the goal is the evaluation of the received signal's parameters, towards the threat warning or target designation. Thus on a tactical and operational level the difference between the SIGINT and the electronic warfare support disappears.

3. Integrated intelligence and electronic warfare system

Considering the above in modern armed forces on a tactical and operational level in order to satisfy the information requirements as well as to eliminate the parallel activities, the SIGINT and the electronic warfare are planned and accomplished in the so called integrated intelligence and electronic warfare structure based on the same principals and uniform command and control.

The tasks of integrated intelligence and electronic warfare can be placed around the following areas:

- situation development;
- target development;
- counter-intelligence;
- electronic warfare and
- indications and warnings.

The tasks mentioned above are well circumscribable, they can be accomplished separately but their relation to each other, the usability of the data, respectively the devices that can be used for the same task make it necessary to uniformly plan and command and control them.

The intelligence assures the featuring, evaluation and understanding of the electronic order of battle (EOB). To know the electronic order of battle is absolutely necessary to accomplish the information operations – more specifically the electronic warfare as one of its core elements – because the supreme proportion of the information infrastructures consists of different types and sorts of electronic devices. Information regarding the EOB inform about the characteristics of the communications and non-communications devices, about the type and designation of the electronic emission devices, about their frequency range, their modulation, their impulse parameters and about other characteristics of the electromagnetic radiation. These data assist the modeling of the enemy's electronic order of battle. In a view of the technical data:

- it is possible to estimate more accurately the vulnerability of the enemy's electronic devices against an electronic attack and deception;
- it is easier to intercept the emitters and to carry out radio direction finding and
- also the electronic protection of friendly forces can be supported with the data about the enemy's electronic warfare capabilities. [6]

In the integrated intelligence and electronic warfare system belong all those devices and organizations at all levels that are able to do data gathering, data processing, intelligence dissemination, counter-intelligence and command and control of electronic warfare. The integrated intelligence and electronic warfare devices on certain levels are in tight connection with other devices that are available on other levels, so they create a uniform, integrated and coherent intelligence and electronic warfare structure.

Summary

The electronic warfare and the all-source intelligence are of basic importance to carry out the information operations. Based on the information of the all-source intelligence and especially the SIGINT the opposite forces' electronic order of battle can be featured, as well as effectively command and control and carry out the information operations. Based on modeling the enemy's electronic order of battle it is possible to perform a successful electronic attack against the opposite forces' electronic systems and targets, respectively it is possible to protect the own similar systems effectively.

The basic requirements of the creation of modern, capability-based armed forces are to develop the information capabilities and to achieve and sustain the information superiority. Thus in the modern armed forces – on tactical and operational level – in order to supply the information demand and in order to apply the SIGINT and the electronic warfare harmonized, integrated intelligence and electronic warfare systems have been created. Due to the Prague Capability Commitment (PCC) Hungary also referred to create capability-based armed forces, and formulated the need to provide the information superiority. [8] This of course can be realized only with up to date SIGINT and electronic warfare devices as well as with the creation of integrated intelligence and electronic warfare organization. Thus the Hungarian Defence Forces must take significant development steps on this field.

References

[1] Faruk Elaldi: Artillery Automation. Digital Battlefield 1999. AFCEA Türkiye International Seminar 29-30 september 1999 Ankara http://www.afcea.org.tr/afceatr/makaleler/AFCEA99_Bildiri_Session1.pdf (downloaded: 19. 08. 2009.)

[2] TR-SAS-057: Information Operations – Analysis Support and Capability Requirements. Final Report of RTO Task Group SAS-057. October 2006.

[3] Joint Publication 3-13: Information Operations. 13. February 2006

[4] Joint Publication 3-13.1: Electronic Warfare. 25. January 2007

[5] Joint Publication 2-0: Joint Intelligence. 22. June 2007

[6] Haig, Zsolt–Várhegyi, István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005.

[7] Ványa, László: Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre. Doktori PhD értekezés. ZMNE, Budapest. 2002.

[8] Úton a XXI. század hadserege felé. http://www.honvedelem.hu/cikk.php?cikk=13776 (Downloaded: 12. 08. 2003.)