

SECURITY OF COMMUNICATIONS AND INFORMATICS SYSTEMS WITHIN THE MODERN BATTLE SPACE

Dorin CHIRCA

“Nicolae Bălcescu” Land Forces Academy, Sibiu, Romania
dorinchirca@yahoo.com

Abstract: *A basic requirement for a modern communications system is the protection of the communications services provided and of the information transmitted through them. This consists of a set of security measures and procedures organized in accordance with the legal provisions in force within each military structure, for the protection of the stored, processed and transmitted information through communications and informatics systems against threats and actions/inactions that may affect their confidentiality, integrity, availability and authenticity or may affect the operation of communications and informatics systems. In these circumstances, the development of communications equipment and the growing integration of the related technical equipment is accompanied by the emergence of numerous means and processes whereby unauthorized access to classified information may be achieved, both by direct interception of the traffic – especially the one transmitted by electromagnetic waves and the unintended (parasite) radiation of the communications and computing equipment. Therefore, a secure communications system within the modern battle space cannot be conceived without technical equipment needed to protect classified information, mainly based on automatic encryption and on appropriate organizational measures.*

Keywords: security of communications and informatics systems, modern combat space, electromagnetic spectrum, electronic and electromagnetic threats

1. The definition and characteristics of the modern combat space

The twentieth century has known the outbreak of war from its traditional dimensions (land and sea) and has known its expansion into a modern combat space that also includes aerospace and electromagnetic environments.

Today, armed conflicts know a new dimension, of another nature, which is a process of the emergence of war into a new environment, namely in the information environment.

The current concepts of space and time are influenced by cyber technology and the automation of combat actions management, the basic principles of combat determine

changing mechanisms and actions to achieve them.

The fundamental features of the modern conflict area, in terms of its external perception are:

- rate of changes or dynamics of combat actions;
- the constantly increasing lethality of individual armaments and high-precision targeting systems;
- the amplitude of conflict area.

The first characteristic is imposed by increasing the destructive effect of the ammunition, increasing the speed and range of the projectiles and of the carriers, correlated with the increase in probability of targeting precision, as a result of the

integration of dynamic search and correction functions in high-precision targeting systems.

Increasing lethality in the battlefield determines higher combat potential, with effects on reconsidering operational rules and missions, and from the point of view of countermeasures, induces a greater degree of dispersion and increased mobility.

The current spectacular development of communication systems (digital transmissions, multimedia architectures, the Internet, hardware and software platforms) that the C4I campaign systems comprise, drastically reduce the time of collection, identification, classification, dissemination and use of information, leading to increased decision-making quality.

Information and command on the scale of "real time" and the inherent mobility of the equipment, determines a very high rate of changes in situations, with major effects on reconsidering the management structures, informational flows and the staff responsibilities in planning, organizing, decision-making, coordination and control processes.

The extent of the current conflict space is expanding at "global" level as a result of the possibilities of aerial, cosmic and naval means, the dispersion of military bases and the existence of rapid deployment forces.

Current doctrines and operational strategies emphasize the ability to project power over large distances, with higher speeds, the emphasis is on the need for combined arms operations and for those operations that are combined with other allied forces, the "JOINT" type.

2. General aspects and the influence of the conflict area on leadership.

Each of the subsequent armed conflicts led to an increasingly accelerated configuration of the electromagnetic field as a new component of the battle space which must be conquered and dominated before the decisive victory.

On the other hand, the electromagnetic field represents the environment in which

electronic and/or electromagnetic signals occur and evolve. The signal theory establishes two areas of existence for these (time and frequency) and provides the mathematical instrument for moving from one domain to another, namely Fourier's transformed function.

Through fire and movement (manoeuvre), the three dimensions of the physical space are conquered and occupied. The electromagnetic field is conquered, mastered and used for one's own benefit through the use of signals and "hosts" a particular threat, different from the common threat of physical destruction, which it does not exclude.

The need to dominate the electromagnetic field, to rely on electromagnetic superiority, becomes evident if the following extremely serious arguments are taken into account:

- Obtaining freedom of action and ensuring execution capability is severely compromised if the possibility of exercising command and control functions is not available;
- Surprise, security, joint action and flexibility are difficult to achieve when there is no freedom in using the electromagnetic spectrum;
- The importance of the threatened objective, namely the C4ISR system, absolutely necessary since the beginning of the battle;
- The importance and volume of electronic and electromagnetic threats have increased considerably, which may materialise into:
 - detection, interception and radio location capability that air or aerospace platforms can offer;
 - disrupting actions performed by the enemy;
 - the continuous danger of electronic deception;
 - the threat of physical destruction that radiation can cause to electronic devices (in the near future could concentrate enough electromagnetic energy to cause

the remote destruction of any type of means).

The fight for electromagnetic superiority stimulates the dynamics of the concepts, forms and processes of employing forces, the emergence of new arms/ branches and specialties. The magnitude, diversity, subtlety, confidentiality and efficiency of actions within the electromagnetic field have led to the development of a new concept and of a new branch: "Electronic warfare". Electronic warfare describes and highlights a specific confrontation, the electronic and electromagnetic signals are used in operations.

It can be said that electronic warfare, unlike the fight with fire and manoeuvres, is a unidirectional confrontation. Electronic warfare structures are always the aggressor. They lead offensive actions, including search, processing and dissemination of information. C4ISR systems are always the victims. They implement electronic protection measures, which electronically/electromagnetically protect the information carrier signals.

Another important feature is that the signals are generated in the electromagnetic field, while the equipment and devices that produce them are in the physical space.

As a result, electronic warfare systems and C4ISR systems are subjected to both the generic threat of physical destruction, specific to the physical space, as well as the specific threat of electromagnetic destruction, owned by the electromagnetic field.

So, the survival capability of the operational and tactical echelons, which operate these systems, is always linked to this double threat.

3. Electromagnetic Spectrum Management

In these circumstances an efficient management of the electromagnetic field is required. Electromagnetic field management, in spectrum and time, for the benefit of one's own forces is achieved by:

- organizing and rigorously planning the emissions (communications means operation) and traffic;
- strict management of the power regime;
- simultaneous use of multiple frequency ranges;
- close collaboration between the structures empowered to use the electromagnetic field;
- exercising a competent and efficient control, both in administrative and operational planning;
- flawless execution of work in the electromagnetic field by all users, efficient use of allocated frequencies and encryption keys;
- professionalisation of personnel;
- integrating electromagnetic field actions into all operations ensuring efficient and complementary support between structures, branches and specialties.

However, in order to obtain electronic superiority, the technological level of the means used and the degree of their integration into the system remain the fundamental problems. The implementation of advanced electronic means is one of the necessary conditions for ensuring freedom of action into the electromagnetic field and creating the prerequisites for preventing electronic surprise.

4. Influences of the modern battlefield on the security of communications and informatics systems

The experience of wars has proved abundantly that where the communications and informatics system is slightly reliable, the immediate result is loss of information credibility for command, report, cooperation and warning, and the poor quality links increase the reaction time, reduce flexibility and increase discouragement. So, the communications and informatics system must have a high survival capacity, the main concern being the implementation of high-stability integrated communications systems that are as far as possible protected from

interception, jamming and nuclear electromagnetic impulse.

Of course, a particular importance is the organization of a developed, continuous and firm operating system, based on a stable communications and computer system, with great capacity to transmit information, both on the spot and, especially, on the move.

Therefore, the dispersed deployment of the forces and the weapons, the operation on several directions, of front and depth, with a well-prepared and higher-ranking enemy in forces and weapons characterized by great mobility, requires a well-developed communications and informatics system consisting of a large number of users, most of whom will be on the move. In this way, communications must provide reliable support capable of transmitting large streams of information in any situation, aiming to achieve independence from losses caused by the enemy through its actions. Users need to transmit and receive large amount of information for leadership, cooperation and warning, requiring a large number of uninterrupted operating channels.

Related to these issues, complex problems arise in ensuring the electromagnetic compatibility of electronic weapons in operation.

These factors, also completed with the increased level of industrial electromagnetic jamming and other types of jamming (cosmic atmospheric), determine that in the event of a scientific failure of the working frequencies, the unintentional jamming (mutual disturbance) may essentially affect the quality of radio and radio-relay communications. The problem of successfully ensuring electromagnetic compatibility can be solved by decreasing the level of mutual jamming caused by the electronic weapons operating on adjacent channels, down to the minimum level admitted at each reception point or by increasing the general level of jamming protection using appropriate technical and organizational methods and means.

Very important in ensuring the reliability of the communications and informatics system is the degree of engineering protection achieved in the siting of electronic weapons. Thus, in offensive and in hasty defensive operations, the stability of the communications and informatics system is lower and inherently the losses suffered will be greater, affecting the traffic and volume of information that will be used for leadership.

The battle rhythm has a special influence on the possibilities of providing links, due to the great time needed to install and recover the communications means and their lower capacity to operate on the move.

As there is a possibility for the enemy to intercept communications and to conduct misinformation by introducing false information, especially in the decisive moments of the operation, the security of communications and the automatic classification of the flow of transited information have a great influence on the process of commanding the troops.

Analyzing situations in which the conflict space influences the security of communications and informatics systems, it can be concluded that the modernisation of communications is an objective necessity, determined by the characteristics and outcome of modern warfare. The particular importance of the communications and informatics systems in the optimum, timely and uninterrupted leadership of the forces and the organic equipment leads to the necessity of organising them by modern principles that ensure great reliability and the necessity to provide state-of-the-art communications and information systems equipment.

In modern warfare conditions, the enemy may have at its disposal an arsenal developed by means of cosmic, aerial and complex terrestrial research, modern and powerful electronic warfare weapons and significant capabilities for employing scout-diversion and airmobile troops. It can also perform strikes with high-precision targeting systems, aviation, missile systems,

artillery and electronic combat weapons for the purpose of disrupting leadership, especially by locating and destroying the communications and informatics systems in the command posts involved in the operation.

As the nervous system is essential for the human body in coordinating its component parts and finally the whole, the communications and informatics system, in the modern combat space, is a component of vital importance for commanding forces on the battlefield.

Analyzing the above mentioned aspects, I believe that the endowment of formations and units with state-of-the-art communications and informatics technology, which provide protection against the enemy's electronic and cyber war actions, should represent a priority for the Romanian Armed Forces.

Ensuring the protection of information transmitted through communications and informatics systems is an objective necessity and also a mandatory measure in order to prevent the opponent's informational attack.

References

- [1] Dumitru Cristea, *Sisteme C4I*, București, Editura Militară, 2005, pp. 242-351.
- [2] Roceanu Ion, *Fundamente ale sistemelor C4I*, București, Editura Universității Naționale de Apărare, 2004, pp. 201-250.
- [3] Timofte Gruia, *Organizarea sistemelor de comunicații pentru operațiile multinaționale*, București, Editura Academiei de Înalte Studii Militare, 1996.
- [4] Dumitru Cristea, Timofte Gruia, *Sisteme de comunicații militare*, București, Editura Academiei de Înalte Studii Militare, 2003.
- [5] Timofte Gruia, Tudose Emil, Gabriel Constantin, *Protecția informațiilor în sistemele de comunicații militare moderne*, București, Editura INEDIT, 2006, pp. 112-125.
- [6] Dragomir Parkov, Veselin Tselkov, Rusin Petrov, Ilia Kraicev, *Security in Computer Systems*, Information Aspects of Security and Development of Modern Societies, pp. 99-103, AFCEA- Sofia, 11-13 septembrie 1996.
- [7] FM, 34-60 *Counterintelligence Handbook*, Headquarters, Department of the Army, Washington DC, 3 October 1995.