MILITARY COMMUNICATIONS SYSTEMS MODERNIZATION ACCORDING TO NEW OPERATIONAL, INFORMATIONAL AND TECHNICAL REQUIREMENTS OF THE BATTLESPACE

Colonel (ret.) professor Gruia TIMOFTE, Ph.D [*] **(*Academy of Romanian Scientists, 3 Ilfov, 050044, Bucharest, Romania)***

Abstract: *The paper highlights, briefly, new developments and approaches, experiments in the modernization of tactical communication systems, the field most requested in theaters of operations. In the second place, the preparatory measures for the transition from analog to digital technology concomitant with the implementation of the new data-centricity concept. The results obtained in scientific research and new and various revolutionary technical products have a strong impact, many of them already requested and purchased. These are presented in the documents developed by specialized bodies at the end of 2023.*

Keywords: *application, digital, innovation, modernization, network, security.*

1. Introduction

Modern military communications systems will be based on rapid installation, sheltering and masking, electronic protection measures against discovery by detection in any area of the electromagnetic spectrum. Anyway, the discovery must be accepted as a risk and the physical protection of the units in the device against direct and indirect fire executed with different categories of weaponry is necessary. Likewise, those arising from attacks carried out with special or non-conventional forces behind the contact alignment, in the tactical and operational depth, modern military communications must resist acts of sabotage or the destruction of some of their parts, continuing to function with reduced capacity for processing and transmitting information.

2. The electronic actions of potential adversaries

The communication systems must be designed, made and used in such a way as to resist or reduce the effects of physical actions such as the following[1]:

- anti-radiation missiles that are directed at the electromagnetic beam;

[*] Full member of the Academy of Romanian Scientists, email: timmy.gruia@yahoo.com

[1] Timofte, Gr., *Concepte si cerinte privind sistemele de comunicatii militare*, AISM Publishing House, Bucharest, 1999.

- means of research and discovery arranged on the ground, in the air or on satellites that use the infrared range, radar stations; video and photo equipment;
- weapons of destruction by lasers;
- radio frequency weapons;
- nuclear explosions and similar impulses produced by other means;
- other dangers (cyber-attacks that affect with predilection the software at the address of the communication systems).

2.1. Physical and electronic attacks

It is assumed that the military communication systems will be installed and used in a combat space with the most modern equipment that uses the electromagnetic spectrum. Under these conditions, the future risks to communication systems will depend on the following factors:

- the operational requirements of potential adversaries regarding the exploitation of our communication systems;
- the adversary's perception of the real vulnerability of our communication systems;
- the technological level of performance achieved by the communication and IT (Information Technology) systems at the beginning of the 21st century;
- divides in signal intelligence (SIGINT = Signal Intelligence) and electronic attack on C4 systems (Command, Control, Communications and Computer).

Signal intelligence is the generic term used to describe communications intelligence and electronic intelligence when there are no express requirements to differentiate these two types of intelligence or to cumulate their effects.

Communications intelligence includes measures to obtain information and technical characteristics derived from the functioning of communications in the electromagnetic spectrum.

In the area of responsibility of the big operative unit, all categories of radio lines (HF=3-30 MHz, VHF=30-300 MHz, UHF=300-3000 MHz, SHF=3-30 GHz, EHF=30-300 GHz) are subject to the actions of signal intelligence and the electronic attack on the C4 systems, as follows:

- high-precision receivers with frequency synthesizers capable of performing measurements with a high degree of accuracy and certainty;
- the jamming stations with 20 kW with directional antennas, variable modulations to achieve the maximum neutralization effect;
- the angle measurement and jamming will be carried out in the same way as at the radio relay stations;

- interception with high-sensitivity receivers that use high-gain antennas and that cover frequency ranges over 18 GHz. The means will have signal demultiplexing capabilities.

In the support communication networks, it is estimated that the adversary will try to obtain information by intercepting radio stations, in relation to the type of wave propagation used: ground-air communications; some radio and radio relay communications, etc.

This includes electronic warfare measures to prevent or reduce the enemy's effective use of the electromagnetic spectrum. These include the following three categories of measures: jamming, disinformation and electronic neutralization. Moreover, it is obvious an adversary will prefer to physically destroy a target (objective) than to neutralize it electronically[2].

The control regarding the execution of the electronic attack against the C4 systems will probably be centralized and led from the highest level of command. The forces and means appropriate to this purpose will be specified and installed up to the combat device of the division (similar). The command and control of these means is recommended to be provided with automatic data processing systems (automated systems).

3. Operational requirements regarding communication systems

The communication networks will be configured with a level of redundancy to ensure connection paths between the main device elements, even if 50% of them are destroyed, assuming that the destructions are produced relatively uniformly within them. Communications and data lines must create reliable, redundant, secure and compatible networks with similar characteristics.

Tactical communications systems will be designed and developed to incorporate maximum protection elements, including techniques that ensure a low probability of interception, exploitation and against jamming[3]:

- ensuring the security of communications - by applying all the protective measures to prevent the access of unauthorized persons to valuable information;
- security which includes transmission security, cryptographic security, cyber security, physical security etc.;
- requirements regarding communication systems, miniaturized, robust communication equipment capable of transmitting data in graphic and alphanumeric form.

[2] Teodorescu Constantin, *Războiul electronic contemporan*, Sylvy Publishing House, Bucharest, 2002.
[3] *Data Science*, Tehnica Publishing House, Bucharest, 2018.

3.1. Electromagnetic compatibility

The *electromagnetic compatibility* of a device (electrical or electronic system) consists in its ability to fulfill the functional requirements at the designed parameters in an environment with specified disruptive levels and not to generate disturbances:

- the level of electromagnetic compatibility – the value of the electromagnetic disturbance for which the EMF must be kept stationary;
- the compatibility margin - the difference in decibels between the level of immunity to disturbances of the system and the level of disturbances acting on it;
- subject to the actions of signal intelligence and the electronic attack on the C4 systems.

In the usual (conventional) situations, the risk is higher near the contact alignment, but under the conditions of the new operational concepts, it is assumed that there is the same risk for all communication lines in the entire area of responsibility of the operative big unit.

The main methods used for spectrum management and ensuring intersystem electromagnetic compatibility are technical, logical-mathematical, organizational and operational[4]. The technical methods include those of design, construction and testing to achieve an acceptable level of compatibility. Logical-mathematical methods take into account the multitude of factors of all categories for the management of the electromagnetic spectrum.

3.2. Interoperability of communication systems

The organizational methods aim at the correct disposition in the field of means and radio-electronic systems in compliance with the norms and requirements that reduce or eliminate interferences.

Interoperability is defined as the ability of systems, units or forces to offer and accept services to/from other similar entities and to use each other's services to effectively cooperate together.

The interoperability steps of the communication systems highlight the way in which operational efficiency can be increased, and the interoperability requirements defined by structuring, automating the exchange and interpretation of data.

According to the intended purpose, interoperability can be of the following types:

- vertical interoperability – the ability to distribute information at all command levels;
- horizontal interoperability – the ability to distribute information to all components;

[4] Tanenbaum A., *Retele de calculatoare*, Tehnica Publishing House, Bucharest, 2016.

- internal interoperability – the ability to distribute information both horizontally and vertically;

- external interoperability – the ability to support the consultation and cooperation process by sharing information with all participants.

The field of implementation includes series of standards and products used to obtain interoperable communication systems.

Operational interoperability standards - specify the meaning, content and use of information that must be exchanged between forces and/or commands.

Procedural interoperability standards - specify the format and representation of information that must be exchanged between forces, commands and advisory bodies.

The IT procedural interoperability standards are bit-oriented, the communication procedural ones realize the informational exchange, and the technical ones specify the characteristics for the informational exchange.

Operational interoperability standards specify the meaning, content and use of information that must be exchanged between forces and/or commands. These standards include the meaning of objectives for military and political consultation, operational requirements, doctrine and procedures, standard military terminology and support requirements for consultative processes.

Procedural interoperability standards specify the format and representation of information that must be exchanged between forces, commands and advisory bodies. These standards contain the form of documents, terminology, operational procedures for data communications. These can be: bit-oriented computer standards and communication standards.

The technical interoperability standards specify the physical, electrical and functional characteristics of the equipment that performs the informational exchange.

4. Scientific results and innovation at the end of 2023

The market value of military communications will increase from 24.2 billion dollars in 2023 to 35.4 billion dollars in 2028. The rapid developments in communication technologies include communication satellites, data encryption systems, HF radio means, high resolution video devices, data sensors, research means, interoperable research systems. It is intended to create real platforms that work in real time. As far as computing platforms are concerned, the intention is to use some solutions for centralizing very large amounts of data from dispersed sources, with an estimate of cost reduction over time, high redundancy and fast recovery in case of disasters, real-time collaboration, etc. Tactical communications could be conducted via all modes namely, written, oral, visual and auditory. The tactical communications

market is segmented on the basis of type, technology, platform and application areas and the difference in users target market:

- On the basis of type, the tactical communications market is segmented into soldier radio, manpack radio, vehicular intercommunication radio, data radio high capacity and others;
- On the basis of technology, the tactical communications market is segmented into time-division multiplexing and next-generation network;
- On the basis of platform, the tactical communication market is segmented into airborne, shipborne, land and underwater.
- On the basis of application, the tactical communications market is segmented into ISR (Intelligence, Surveillance and Reconnaissance), communications, combat, command and control and others[5].

Conclusions

The problems bring into attention are particularly laborious and with consistent costs, but which will recover in the medium and long term. Particularly important are the facilities obtained with the efficient support of technology. The briefly presented example, due to the informational restrictions imposed on these categories of information, is not unique. All military domains will have a similar facility.

Some important conclusions can be drawn: the initiative starts from the civil environment, as in the case of the "data-centricity" concept; the process will expand very quickly; the authorities have launched consultations in order to achieve a balance between benefits and expenses; a new "competitive" field opens.

BIBLIOGRAPHY

FREEMAN, R., Telecommunication System Engineering, John Willey& Sons Company, New York, 1998;

TIMOFTE Gr., Concepte si cerinte privind sistemele de comunicatii militare AISM Publishing House, Bucharest, 1999;

TEODORESCU Constantin, Războiul electronic contemporan, Sylvy Publishing House, Bucharest, 2002;

[5] „Military Communications Global Market Report 2024", available at thebusinessresearchcompany.com/mil-com/, accessed on 10.06.2024 and „Tactical Global Market by Type, Global Forecast to 2027", available at maketsandmarkets.com/mil-com/, accessed on 12.06.2024.

TANENBAUM A., Rețele de calculatoare, Tehnica Publishing House, Bucharest, 2016;

EUROCOM Tactical Communications System, WEU, BRUSSELS, 1999;

„Military Communications Global Market Report 2024", available at thebusinessresearchcompany.com/;

„Tactical Global Market by Type, Global Forecast to 2027", available at maketsandmarkets,com/;

Data Science, Tehnica Publishing House, Bucharest, 2018;