INFORMATIONAL SYSTEMS AND TECHNOLOGIES IN CURRENT AND FUTURE MILITARY CONFLICTS

Lieutenant-General (Ret.) Associated Professor Constantin MINCU, Ph.D[*]

***Abstract**: In this article, the author briefly presents some of the more important aspects of "The Role and Place of Informational Systems and Technologies in Current and Future Military Conflicts", taking into account lessons learned from recent military conflicts that have taken place in recent years, including (although partially) from the war launched by the Russian Federation on 24.02.2022 against Ukraine. Hopefully the political and military authorities in Romania will study and deepen the realities of this unfortunate war, drawing the necessary conclusions for the Romanian Armed Forces and for our entire society.*

***Keywords**: information systems and technologies, informational activities, informational processes and environments, C4I systems.*

The most significant changes in the evolution of humanity are those determined by the emergence and development of the information-based society, which paves the way for globalization. The Internet, information systems, information and communication technology (ICT), already allow the reduction of existing gaps, economic development, the emergence of a Romanian software industry, national information infrastructures, as well as faster integration in e-commerce in the digital age.

It should be noted that the **information society** is, on the one hand, an opportunity, a way of training and education and, on the other hand, a potential risk, a way of threat and aggression (note the intense information war in recent years, by the Russian Federation against EU and NATO states, including Romania). Starting with January 2022, Russia launched massive cyber-attacks against Ukraine, and from 24.02.2022 massively intensified these attacks against government entities, banks, critical infrastructure elements (utility networks, transport, health system, etc.). Despite all the

[*] Entitled member of Romanian Scientists Academy, member of the Honorary Council of the Romanian Scientists Academy, Vicepresident of Military Sciences Section. Phone: 0722303015, E-mail: mincu_constantin@yahoo.com

taken countermeasures, the negative effects were major, leading to economic disruption and loss of human lives, without the aggressor being punished in any way so far.

It can be concluded that the technological revolution in the field of communications and information has led to an increase in its importance through the possibilities created by collection, processing, storage or dissemination, but also by attack using multiple intelligent weapons systems.

In the modern information society, political boundaries are ignored and all spatial, temporal or moral constraints are passed over with serenity.

The much-needed **information systems and technologies, technical equipment and related software** are at the same time vulnerable to unauthorized penetration, accidental or intentional destruction and modification of data and software. The current trend of increasing connectivity, especially on the Internet and Intranet networks, increases the risk of vulnerability, making it increasingly difficult to locate an illegal access point on the network or a user with aggressive behaviour. Also, the vulnerability of current information systems can lead to huge financial or other losses, directly or indirectly, through the "leakage" of confidential personal, economic or military information. We should be concerned about the intensification of cyber-attacks by state actors (Russia, China, Iran, North Korea, etc.).

From a technical-military point of view, the importance of communications and information lies, in addition to their indisputable value, in the fact that they consist in several vulnerable, rapidly accessible and widespread targets that require more and more means and procedures of protection. Modern armies have made winning the information battle a primary goal of their development strategy. The basis for winning this battle is the successful application of information technology on the entire battlefield, namely the digitization of the battlefield and informational activities. From a technical point of view, problems related to equipment, technologies, procedures, methodologies and algorithms in information operations (offensive and defensive) are possible to achieve and control. Russia's current war against Ukraine confirms the idea.

Conflicts after the World War II, through the content, objectives, scope and modalities of the development that benefited from the achievements of the technology, particularly ones of the information age - whose outline is becoming increasingly clear -, largely highlight what will be defining for the military actions of the future such as:

- carrying out actions in all environments: on land, in the air, on water, under water and in the cosmos;
- the use of diversified forces and means, with great mobility, firepower, range, precision, effect of destruction;
- the use of high-performance weapons and weapon systems with great precision;
- the transparency of the combat space due to the conjugation of the activity of the observation satellites, the airborne radars and the means of detection by contact - active and passive;
- hits applied both in contact and in depth, simultaneously with the existence of effective protection measures;
- rapid dispersion and deployment of forces and means;
- the existence of the common space of disposition and manoeuvre for the opponents;
- the combat space oversaturated by electronic means;
- high consumption of ammunition, fuels and other resources, huge material losses (roads and communication nodes, works of art), significant dislocations of the population on ethnic, religious etc. criteria;
- the tendency to avoid direct, frontal confrontations between numerous forces and means, the emphasis being on the actions carried out by small formations, with a great firepower, relative autonomy in action, a great diversity of tactical procedures, especially on the flanks, at intervals and in the depth of the opponent’s dispositive; hiring real professionals in the fight.
- the use of techniques and procedures of the so-called „hybrid war” (to study the case of the conflict in Ukraine with major involvement, not assumed by the Russian Federation). It is necessary here to identify and take countermeasures in advance. Unfortunately, Russia has taken the next step, triggering aggression with all the military means at its disposal;

- ➢ military analysts believe that future wars will have an integrative character, in the sense of participating in the conflict of all categories of armed forces that will act in all environments. To these are added the cosmic ones of observation, direction, and communication.
- ➢ in the war of the future, cyberspace will become a reality. This phenomenon raises, among other things, two aspects with special significance:
    - ➢integration of the process of computerizing the command of the troops with the armament systems, appearance and use of robots, remote-controlled vehicles and intelligent ammunition. The role of attack and observation drones can be studied more closely;
    - ➢the methodology of working in the conditions of cybernetization, the elaboration of specific tactical and operative scenarios and, especially, of the development of combat actions with the simultaneous use of troops and elements by which the activity of the opponent is monitored, the reactions of own troops, the influence of environmental conditions, the effectiveness of the elaborated decision.
- ➢ the need to identify in time and take concrete measures to continue the command and control of military forces in case of the fall of automated means (C4ISR systems). In Russia's aggression against Ukraine, the command and control centres were „hunted”.

Modern combat, led by units of various types, requires the rapid retrieval and transfer of information throughout the battlefield.

The cyberspace already reveals enough elements that shape it and give it many possibilities for development such as:

- ⇨ the multitude of automated and armament systems;
- ⇨ coordination of various categories of forces and weapons in combat, under the conditions imposed by the compression of operational time;

- ⇨ the multifunctionality of the fighting forces during the development of the offensive, as well as, especially, during the defence;
- ⇨ conservation of human forces and their use only in special situations or to consolidate successes;
- ⇨ compensation of the physiological limits of commanders, fighters and operators by using automated combat systems;
- ⇨ use of robots for activities that require great effort, long time, sacrifices or actions in complex conditions.

Regarding the physiognomy of future wars, Western military analysts have defined the following five trends: increased lethality and dispersal; increased fire volume and accuracy; massive integration of new technologies; achieving a greater destructive effect; improvements in ensuring the invisibility of the means and in detecting the objectives.

There is also a resizing of the notion of conflict by adding new attributes:

- ⇨ *permanence* - the application of a global strategy that permanently integrates all information processes, not only in times of crisis or conflict;
- ⇨ *transversality* - influencing the society as a whole and basing it on multidisciplinary and the concepts of systems integration;
- ⇨ *duality* - the disappearance of the differences between the military and the civilian sphere (at national level, the centre of gravity moves to other fields - banking, financial, energy, in general to civilian infrastructure whose defence, with conventional forces and means, becomes very difficult).

The information resource is the main category of resources of modern warfare and covers the following areas:

- political, economic, social and military that are necessary for strategic command and control;
- the military capacity of potential adversaries and the dynamics of war preparations;

- military doctrines, organization and strategic preparation of military systems, territory, economy and population for defence (here Romania still has a lot of work);
- the possibilities of weapons systems and combat techniques, their use and integration in the concepts of waging war;
- scientific research activity dedicated to defence;
- the orientation of the mass media and the reaction of the population to military conflicts (The events of the last two years demonstrate the perverse effect of the media war on an important segment of the population, easily influenced by the low level of correct information, an example in Romania are trolls freely attacks on news sites and social networks);
- the scope and structure of command information, cooperation and notification, organization and use of information systems;
- general characteristics, use and evaluation of the strength of cryptographic systems;
- the ability to counter espionage, diversion, terrorism by spreading false news;
- the level of training and morale of the troops;
- general information of a political, economic, financial, social, diplomatic, etc. nature.

Information and communication technology provides real-time information, affects national and global public opinion, shapes the actions of politicians and produces a strong interplay of tactical, operational and strategic levels. It is becoming increasingly clear that a greedy and impassive political class can be a major factor of vulnerability of a state.

Commanders at all levels must be aware that in a world of direct, real-time communications, any isolated event can be known simultaneously at all three levels.

In the army of the century at the beginning of which we are, military operations will be based on the knowledge resulting from precise, accurate and relevant data and information, collected, analysed and disseminated through a technical „system of systems".

C4I integrated information systems (Command, Control, Computers, Communications and Information) will provide commanders with opportunities to see, feel, interpret, decide and take action at any point in the action strip or in the area of informational (informative) responsibility.

The information age has as its content the explosive increase of the use of cybernetics in communications and means of combat, the information becoming the object, the means and the procedure of a new field of action - the informational one. If these actions are carried out in a timely and successful manner, they can prevent conflicts, reduce losses or quickly stabilize the conditions for military action.

Unfortunately, at present there is no full understanding that the information dimension is not a fabricated one, but is as real and current as possible. At the same time, the information is not perceived in its true identity: as a weapon, a risk factor, an operational and technological tool.

The main features of information actions are the following:

- the volume of information necessary for the elaboration of decisions and the conduct of military actions increases 10-15 times more than the one circulated in the World War II;
- the possibility of information increases and, as a result, the specific means become more and more efficient;
- the beneficial influence of information processing on the capacity of weapons systems, but also the detrimental effect of misinformation or computer viruses on specialized processes performed with appropriate computers and software;
- the explosive increase of the amount of information necessary for the fighter to face the demands of the modern combat space;
- integration and use of smart weapons and fighting techniques;
- development and improvement of specialized structures to ensure information security;
- the cybernetic character of the military actions and the technological and informational approach between command and execution;
- some difficulties in specifying the opponents;
- the multitude of targeted targets;
- the absence of specific and clear warning indicators;
- the persistence of the effects and the lack of quick methods to remedy the consequences they generate;

- the use of relatively simple, cheap and widespread technologies;
- disappearance of differences between control levels.

Main informational activities

The specialized papers define the main concepts used in this field, as follows:

- *data* – individual or statistical facts in an uncorrelated form;
- *information* – a communication, news, that informs someone of a situation;
- *knowledge* - the result of information processing, a process in which intuition and human thinking intervene.

There are also four key stages of the information life cycle: its creation, collection, dissemination and use. These stages are distinct, although they have many features in common.

Technological development has affected the speed and volume of information collection and dissemination.

The information revolution has led to the development of modern interconnected and interdependent systems, which can no longer be manually managed.

Information, as a strategic military good, has always been recognized as such by commanders, especially in the idea of a good knowledge of the opponent's intentions and, at the same time, as his own protection, plans and the operational stage of military actions. If this information is available in the military field, from the strategic command level to the tactical command level, a number of issues may arise regarding their confidence in the integrity, relevance, and accuracy of the presented information.

The information activities in the modern battlespace involve obtaining, transporting, processing, converting, distributing, using, protecting, exploiting and managing information, briefly, their content consisting of:

- ***Collection*** - acquisition and initial filtering of data based on planned needs and their presentation in a form suitable for transmission. This information covers the mission, the opponent, your own troops, the terrain, the weather and the available time. The process of obtaining information is carried out with the help of electronic systems, of operative research and reconnaissance activities, of strategic, operative and tactical research, by collaborating with the police and mass media, etc.

- ***Transport*** - communication of information and data to the receiving devices of the recipients.
- ***Data processing*** - storage, retrieval from memory devices, updating, filtering and synthesizing them to result in minimal information in a usable form.
- ***Conversion of information*** - transforming it from one form to another without loss and without changing their accuracy in order to transmit and display in the form of text, still and moving images, data for computers, etc.
- ***Distribution (dissemination) of information*** - transmission of processed information to potential users.
- ***Use of information*** (after the data is obtained, analysed and verified) - updating and knowing the real situation in order to continuously improve or to adapt military decisions, plans and actions.
- ***Information protection*** - analysis of the vulnerability of the forces and own means of command and control to the actions of electronic nature, physical destruction, misleading, and propaganda of the opponent as well as establishing the means, application and verification of countermeasures. The infrastructure elements that need to be protected are databases, computer networks, communication systems, research and ancillary means within them.
- ***Exploitation of information*** - the action by which advantages are obtained for military operational purposes from any acquired information. This involves intercepting and analysing the opponent's messages, extracting information from his databases, taking measures to distort, degrade or manipulate his information capabilities.
- ***Distortion of the opponent's information*** - the measures of attack on the command and control aimed at influencing, degrading or destroying his information and information systems (C4I).

- ***Information management*** - careful coordination and synchronization of information and information systems (C4I), and includes: management of the electromagnetic spectrum, choice of sources and systems to be used, ensuring reliable information flows (with vertical and horizontal integration), interception of information from several sources.

Informational processes and media

For the pertinent analysis of the informational dimension of the modern combat space, it is very useful to briefly characterize the informational media that have an important impact on the organization and development of military actions, as follows:

- ***global information environment*** - includes personalities, organizations, systems, etc., many of them outside military control or national command authorities, which collect, process and distribute information nationally and internationally;
- ***national information infrastructure*** - includes public and private telecommunications networks, satellite, terrestrial and radio technologies serving individuals and legal entities, their information and content, databases, hardware terminals and software for accessing information, staff collecting, processes, stores and generates new information, etc.;
- ***defence information infrastructure*** - includes the necessary resources for the transfer, processing, storage and display of information, technical means for command and control, research and other categories of means for transmitting voice, still and moving images, multimedia services especially useful to the military field;
- ***military information environment*** - consists of information systems and structures of their own and of the adversary, military and other categories, which support or significantly influence military operations;
- ***information systems (C4I)*** - consists of the infrastructure, structures, staff and components that collect, process, store, transmit, display, distribute and act in accordance with the obtained information.

The intensive development of information and communication technology has created new procedures for data management and processing. These include images, graphics, diagrams, digitized maps, databases that combine with modern communication techniques (satellites, frequency hopping radio stations, microwave radio relays, tropospheric and ionospheric radio stations) and provide global, national and military infrastructure.

Modern information systems

The command and control system is based on information about events, the environment, the adversary and their own troops, which influence or may affect military actions and which, following the processes of processing, analysis, storage and capitalization, substantiate the decision and contribute substantially to information supremacy.

"*Information supremacy* - is the degree of information dominance that gives staff the ability to use information systems (C4I) to gain operational advantages in conflict or to control a particular situation, while reducing the opponent's ability to use information needed for similar processes for its own troops"[1].

Achieving informational superiority comprises two equally important components - the accumulation and protection of one's own informational capabilities and the degradation of the opponent's informational capabilities.

Informational superiority depends on:

- the ability to access a large amount of information from various sources and environments (political, social, economic, military, religious, etc.), about the opponent and his own troops, necessary information in the area of responsibility of the command act and control;
- reducing the possibilities of using false or null value information by using efficient collection and authentication techniques and procedures;

[1] Joint Doctrine for Operations Security, Departament of Defense, Washington, DC, 1994, p. 63.

- the performance of sensor systems to collect, process and transmit information in different formats on communication channels;
- the ability of communication systems to convey, in a short time, the entire flow of information, both vertically and horizontally;
- the ability of the control bodies to use the information in making decisions so as to anticipate the probable actions of the opponent;
- the level of protection and security of data and information on own troops and their actions.

Ensuring information superiority is achieved through several procedures, as follows:

- ⇨ increase the flow by using topology communication systems, using special units, officers and research teams. Innovations in sensor, processor, communications, and computer systems can provide commanders with a good understanding of the operational situation through immediate access to information about their adversary and troops;
- ⇨ "visualizing" the battle space by knowing the current situation of one's own troops in connection with that of the opponent and with the environmental conditions;
- ⇨ designing the final desirable situation - fulfilling the mission - sequential visualization of the activities that the own forces carry out, from the initial situation to the final one;
- ⇨ knowing the situation through analysis, mastering the intention of the commander and the conception of the fight (operation) in direct connection with the disposition and possibilities of the opponent and of his own forces;
- ⇨ permanent information management, in the conditions of collecting and processing very large amounts of information, reducing the duration of the command cycle, making decisions in a short time.

Essential for ensuring and exploiting the informational superiority is the materialization of the concept that highlights „attack actions aimed at the centres of the information network"[2].

This concept is applicable at all hierarchical levels and contributes to the intertwining of strategy, operational art and tactics. It finds its substantiality in the integration and coordination of well-informed and logically dispersed forces in the battlefield.

The elements that contribute to the realization of this desideratum are three[3]:

- ⇨ high-performance information network (C4I) that resists and survives the full range of physical threats and information operations;
- ⇨ sensor systems capable of achieving a high level of knowledge of the combat space synchronized with the conduct of military operations;
- ⇨ improving the capacity to exploit forces and means through modern and efficient engagement networks (ensuring new operational capabilities for preventive planning, integrated force management, reducing target attack time).

Many experts believe that the fundamental shift from platform-based to centre-based actions with information superiority is a military revolution and is at the heart of this transformation process.

Technological improvements have led to a considerable increase in the quality, accuracy and timeliness of the information provided to the information department, as well as the information products intended for use by the master.

All staff officers must understand the principles and techniques of information activity if the plans are to be realistic. At the same time, it is important to note that the information provided by the staff in the information department is the result of an analysis based on both the available data and other factors that are either variable or only assumed.

[2] John Garstka, *Information and Network – Centric Warfare*, J 6 Presentation, Washington, DC, 1998, p. 4.

[3] *Joint Vision 2010*, Department of the Army, Washington, DC, 1998, p. 36.

In order to facilitate the understanding of the specific issue, it is necessary to know the usual terms used in the informative field:

⇨*data* – specific unrated materials resulting from various descriptions that can be used in making informative products;

⇨*information* – the result of data processing;

⇨*informative product* – the result obtained from the analysis and processing of information;

⇨*source* – a person or object from which information can be obtained;

⇨*agency* – organizational structure or person engaged in collecting and/or processing information for informational purposes;

⇨*surveillance* – systematic observance;

⇨*area of influence* – the geographical area within which the commander is directly involved in influencing military actions through manoeuvring and fire support systems under his command and control;

⇨ *area of information responsibility* – the geographical area allocated to a commander in which he is responsible for providing information, using the means at his disposal;

⇨*area of information interest* – the geographical area about which a commander requests information on factors that may affect present and future military actions, and their evolution.

Some values regarding the tactical areas of responsibility mentioned are presented in the following table[4].

No.	Great unit, unit or formation	Area of influence (km)	Area of information responsibility (km)	Area of information interest (km)
1.	Battalion	0-6	0-6	0-20
2.	Mechanized brigade	0-20	0-12	0-50
3.	Mechanized division	0-30	6-50	0-150
4.	Army corps	0-100	50-150	0-250

[4] *Intelligence Handbook*, Romania and UK, Regional Training Centre, Bucharest, 1998, pp. 1-2.

The information cycle comprises several stages[5]:

- *The information requirements of the commander ensure the orientation, planning and management* of the information activities, current and future, in accordance with the priorities established by him.
- *Collection* is the stage at which data and information are exploited and delivered to the General Staff for analysis and to obtain desirable information products.
- *Information processing and exploitation* are the processes by which the data (information) collected are evaluated, analysed and transformed into information products that are used in information-decision-making processes.
- *The realization of information products* consists in collecting, evaluating, analysing, integrating and interpreting information from one or more sources, in order to obtain a final product. The time constraints and the evolutions of the modern battle space determine the more and more consistent interpenetration of the processing and synthesis phases.
- *The distribution and integration of information products* is done by transmitting them to the bodies that requested them to be used in the process of drafting the decision and planning military actions. Information department staff at all levels evaluate the progress of the information cycle and the obtained results.

The information system as a component of C4I systems is the set of personnel, means, procedures and techniques by which data are obtained and processed, through which information and information products are transmitted to departments and persons involved in command and control processes. It follows that an information cycle begins with the formulation of specific requirements in the command and control processes and ends with the provision of information products. Also, it should be noted the interdependencies and close correlations of the information system with the

[5] *JP 2-01, Joint Intelligence Support to Military Operations*, Joint Staff, Washington, DC, 1996, Cap. II, pp. 1-3.

other component subsystems of the C4I systems: the command and control system, computer networks, communication systems, weapons systems, etc.

Battle space reconnaissance involves missions to obtain, by visual observation or other detection methods, information about the opponent's activities and resources, as well as the meteorological, hydrographic and geographical characteristics of a well-defined area.

Surveillance of the battlefield is a systematic observation of it in order to ensure timely information on the conduct of combat operations.

Depending on the provenience of the data and information, the sources may consist of: research of electromagnetic signals; human elements and various organs; satellite research.

The research of electronic signals aims at the discovery, location and evaluation of electromagnetic radiation of all categories and includes:

- ❖*communications research* - which aims at searching, intercepting, locating, analysing and exploiting the radio traffic of the opponent, ensuring the evaluation on this basis of the disposition, movements and intentions of his forces;
- ❖*electronic research* - which includes the activities of collecting and processing potentially hostile electromagnetic radiation (except for those of the communication means), emanating from nuclear explosions and radioactive sources.

The research carried out by the people and the specialized bodies covers all the specific aspects, such as: the interrogation of the prisoners; observing the opponent's activity; patrol; detachments etc.

Imaging research includes the forms of research obtained through photography, thermal observation, and other equipment that captures images.

Acoustic research obtains data by collecting and analysing acoustic phenomena. The sensors used for this purpose can be passive (receive noise) or active (transmit acoustic pulsating waves and then receive the echo). Acoustic research sources can be stationary or installed on ships, floating platforms, diving or on the seabed.

Sources of information may be: research subunits (observation points, patrols and research detachments), weapons research subunits, airplanes, helicopters and drones, electronic means, prisoners and refugees.

Agencies are assimilated with: information structures (information, artillery, genius); operations, aviation and electronic research systems; research elements in the opponent's device; structures interrogating prisoners, etc.

The techniques used in the surveillance of the modern combat space aim at the use by the opponent of the electromagnetic spectrum: Infrared - the images obtained by receiving the radiation emitted or reflected by the surface of the objectives in the segment from 0.72 to 1 μm; infrared thermal images that can distinguish 0.1° C differences. This allows targets to be detected as images by viewing or monitoring with the TV; visual, including photography; in ultraviolet by radiation reflection in this field; various types of radio locators; exploitation of acoustic or seismic waves.

The efficiency of these techniques can be improved by: using aerial platforms with and without a pilot capable of providing near real-time information up to tactical commands; use of terrestrial sensors; signal processing.

These technical systems can be active or passive. Active systems radiate energy to the target in order to illuminate and discover it. Passive systems receive energy radiated by the target.

Some limitations in the use of these techniques are determined by the direct visibility to the target, the atmospheric and meteorological conditions, the characteristics of the target (size, ability to reflect or radiate energy) and its contrast with the environment, as well as some specific countermeasures (masking, radio silence, misleading, manoeuvre restrictions).

Optical instruments are passive, cheap, light and reliable, but they are ineffective at night. These systems amplify the ambient light with electronic means so that the observer can see dimly lit targets.

Lasers are active systems and have two applications: detection with an accuracy of ± 5 m up to a distance of 20 km; marking targets by illuminating them.

Radars transmit an electromagnetic pulse that is reflected by the target and received back by the radar. Some radars detect the movement of the vehicle up to 24 km and the movement of people up to 3 km.

Alarm devices operate on the basis of seismic or infrared sensors.

The search in the opponent's dispositive is performed with means for medium distances (6-50 km) and long distances (over 50 km).

Satellites that perform photography and radiolocation research, etc. are also effective means of research.

From the point of view of the efficient operation of the research systems, it is necessary, if possible in real time, the use of high-performance specialized technical means, interfaces for adapting the sensors with the digital communication channels with high transmission speed and maximum accuracy.

Also, the information department must have technical means of automation (high-performance computers) and specialized software that will allow the processing of data and information in a timely manner, increase the level of command information and reduce the level of risk of information management.

In this first part, I have tried to bring to the attention of those interested in military issues, some aspects of the role and place, the current information systems in the modern war taking note of developments and lessons learned from recent conflicts, including the Russian-Ukrainian crisis. I wonder if it will be possible to continue, in a future issue of this journal, with the other components of information systems, analysed in the light of recent information.

BIBLIOGRAPHY

*** Legea privind protecţia informaţiilor clasificate, nr. 182/2002, M. Of. 248/2002 (In English: Law no. 182/2002 on the protection of classified information, Official Monitor 248/2002);

*** Legea privind securitatea naţională a României, nr. 51/1991, M. Of. 163/1992 (In English: Law no. 51/1991 on national security of Romania, Official Monitor 163/1992);

*** Securitatea informaţiilor, Centrul de Expertiză în Domeniul Securităţii, Bucureşti, 2008;

*** Sisteme informaţionale – Sesiunea anuală de comunicări ştiinţifice cu participare internaţională, Editura UNAp, Bucureşti, 2007 (In English: Information systems - Annual session of scientific communications with international participation, NDU Publishing House, Bucharest, 2007);

*** Joint Doctrine for Operations Security, Department of Defense, Washington, DC, 1994;

*** *Joint Vision 2010*, Department of the Army, Washington, DC, 1998;

*** *Intelligence Handbook*, Romania and UK, Regional Training Centre, Bucharest, 1998;

*** *JP 2-01, Joint Intelligence Support to Military Operations*, Joint Staff, Washington, DC, 1996, Cap. II;

*** *JSP 120 (3) Manual of Service Intelligence.* Department of Defence, United Kingdom of Great Britain, London, 1997;

***FM 34-1 Intelligence and Electronic Warfare Operations, Headquarters Department of the Army, Washington DC;

***Simpozionul Jubiliar AFCEA, Washington DC, 18-19 Iunie 2006;

ALBERTS D.S., HAYES R. E., *Planning – Complex Endeavours, CCRP;*

ALEXANDRESCU C. şi alţii, *Supremaţia electromagnetică*, Editura UNAp, Bucureşti, 1999;

ALEXANDRESCU C., *Ameninţări informaţionale asupra sistemelor de comandă şi control în acţiunile militare moderne "SI-2007";*

ALEXANDRESCU C., TEODORESCU C., *Războiul electronic contemporan*, Editura Sylvi, 1999;

ALEXANDRESCU C., ILINA D., MINCU C., *Bazele matematice ale organizării sistemelor de transmisiuni,* Ed. Militară, Bucureşti, 1994;

ALEXANDRESCU C., ALEXANDRESCU G., BOARU G., *„Sistemele Informaţionale Militare" – servicii şi tehnologie*, Editura UNAp „Carol I", Bucureşti, 2010;

DUMITRU C., *Infrastructura de reţea şi informaţională în cadrul războiului bazat pe reţea,* Editura CTEA, Bucureşti, 2008;

DUMITRU C., *Sisteme C4I,* Editura Militară, Bucureşti, 2005;

EUROCOM D/1 Tactical Communications Systems. Basic Parameters, 1986;

FRIEDMAN G., fondatorul STRATFOR, *„România trebuie să înveţe să fie mai periculoasă pentru a exista, să fie un risc pentru ruşi, germani şi de ce nu, americani”*, interviu NotNews.ro, 16 noiembrie 2010, Bucureşti;

GARSTKA J., *Information and Network – Centric Warfare*, J 6 Presentation, Washington, DC, 1998;

MINCU C., GREU V., ROTARIU C.., *Salt de frecvenţă şi contrasalt de frecvenţă,* Editura Militară, Bucureşti, 1998;

MINCU C., TIMOFTE G., *Compatibilitatea Sistemelor Radioelectronice,* Editura Olimp, Bucureşti, 1999;

MINCU C., „Politica actuală a Federației Ruse – un mister ascuns într-o enigmă”, Revista de Științe Militare nr. 4.2021;

TOFFLER A., TOFFLER H., *Război şi anti-război*, Editura Antet, Bucureşti, 1995;

TOFFLER A., *Powershift, puterea în mişcare,* Editura Antet, Bucureşti, 1995.

Speciality journal

Romanian Military Thinking, years 2015-2021;
“Carol I” National Defence University Bulletin, 2015-2021;
Strategic Impact, years, 2015-2021;
Military Science Journal, years 2015-2021;
Annals Series on Military Sciences, years 2015-2022.