INFORMATIONAL DIMENSION OF THE MODERN BATTLE-SPACE

Major-General (r) professor Constantin MINCU, PhD*

Abstract: *The paper briefly presents some of the main aspects of "Informational dimension of the modern battle-space" by taking into consideration the lesson learned from the late military conflicts that were taken and take place in the time being as well as the realities in the field of some modern armed forces.*

Tthere are also presented some main informational activities, there are defined the informational processes and activities, there are reviewed the features and limits of the modern information systems.

Keywords: *informational resource, informational activities, informational processes and environments, C4I.*

The most significant changes in the evolution of humankind are determined by the apparition and development of information based society which neats the way toward globalization. Internet, informatics systems, information and communications technology already allow the diminution of existent gaps, economic development, apparition of a Romanian software industry, national informational infrastructure, as well as the accelerated integration in the electronic commerce and digital era.

We must notice the informational society represents on one hand an opportunity, a way to train and educate, and, on the other hand, a potential risk, a way to threaten and aggression (It should be acknowledged the intense act of info war lead lately by the Russian Federation, inclusively against Romania).

* Entitled member of Romanian Scientists Academy, Member of the Honorific Council of the RSA, Scientific secretary of the Military Sciences Section. Phone: 0722.303.015, Email: mincu_constantin@yahoo.com.

Information was always regarded by countries, political leaders and military commanders. The technological revolution in the field of communication and information lead to the increase of the importance for the later by the possibilities created to collect, process, and store and disseminate but also to attack the information. In the modern informational society borders are ignored and are overlapped any spatial, temporal or moral constraints.

The very necessary informational systems and technologies, technical equipment and associated software are concomitantly vulnerable to unauthorized intrusions, to destruction and incidental and intended changes of data and programs. The actual trend on the amplification of connectivity, particularly to Internet and in Intranet networks increase the risk of vulnerability and becomes increasingly harder to locate an illegal point of access to the network or a user with aggressive behaviour. The vulnerability of the recent informational systems can provoke directly or indirectly huge financial or different type of loses by the "leaking" of confidential information with personal, economic or military character. Intensification of cyber-attacks executed by some state actors should worry us.

By technical-military perspective, the importance of communication and information consists along their indisputable value in the fact there exist more vulnerable targets rapidly and widely accessible and need more means and procedures of protection. The modern armed forces set as main goal of their development strategy to win the informational battle. The basis to win this battle is the successful application of informational technology on whole the battlespace, respectively the digitization of the battlespace of informational type. By the technical perspective, the problems regarding the equipment, technologies, procedures, methodologies and algorithms in the informational operations framework (offensive and defensive) are possible to achieve and controlled.

The conflicts following the World War II by their content, goals, amplitude and means of development benefited by the achievements of technique and technologies particular for informational era – that is increasingly shaping – largely emphasizes what will be defining for the military actions of the future as:

- Performance of actions in all the environments: land, air, water, underwater and cosmos;
- Using diversified forces and means with great mobility, fire power, hit, precision, effect of destruction;
- Using some very performant weapons and systems of weapons with special precision;
- Transparency of the battlespace owed to the conjugation of the activity of observance satellites, airborne radars and means to detect by contact – active and passive;
- Hits applied to contact and in depth, concomitantly to the existence of some efficient protection measures;
- Rapid dispersion and concentration of forces and means;
- Existence of common space of disposition and manoeuvre for the adversaries it confronts with;
- Oversaturated battlespace with the electronic means;
- Great consumption of munitions, petrol, oil and lubricants (POL) and other resources, huge material lose (ways and knobs of communications, artworks), meaningful displacements of populations on ethnical, religious etc. criteria;
- The trend to avoid direct, frontal confrontations among many forces and means and the accent is on the actions lead by small groups with great firepower, relative autonomy in the action, and great diversity of tactical procedures particularly to the flanks, in space and depth of adversary's disposal; the engagement in battle of real professionals.
- The use of techniques and procedures of so-called "hybrid war" (to be studied the case of Ukraine conflict with major involvement which is not assumed by the Russian Federation). Here is the situation to be identified and to be taken timely measures of counteraction.
- Military analysts appreciate the future wars will have *integrator character,* in the sense of participation into conflict of all services of the armed forces which will act in all the environments. Together with those there will also be the cosmic environment used for observance, directing and communication.

In the future war, the cybernetic battlespace will be a reality. This phenomenon raise among other two aspects with particular significance:

➢ Integration of cybernetic process of troops' command with armament systems, the apparition and use of robots, tele guided vehicles and intelligent munitions;

➢ The work methodology in the conditions of cybernetic perspective, elaboration of specific tactical and operative scenarios and particularly the development of some battle actions with the simultaneous use of troops and elements used to monitor the activity of the enemy, reactions of own troops, influence of environmental conditions, opportunity and efficacy of the elaborated decisions.

➢ The need to timely identify and take some concrete measures to continue the command and control of the military forces when the automated means (C4ISR systems) are cut off.

The modern battle lead by different types of units needs the rapid overtaking and transfer of information in the whole battle space.

The battle cyberspace already reveals enough elements that shapes it and confers it many possibilities of development as follows:

⇨ The multitude of automated and armament systems;

⇨ The achievement of coordination of some diverse forces categories and battle armament under the conditions imposed by operative time compression;

⇨ The multi-functionality of fighting forces along the offensive development as well as on defensive actions;

⇨ The preservation of human forces and their use only in particular situations or for strengthening the successes;

⇨ The compensation of physiological limits of commanders, fighters and operators by using the automatic fight systems;

⇨ The use of robots for activities requiring big efforts for a long time, sacrifices or actions in complex conditions.

Referring to the physiognomy of future wars, the westerner military analysts defined the following five trends: increased lethality and dispersion; enhanced volume and precision of fire; massive integration of new technologies; fulfilment of a greater destructive effect; improvement in providing the invisibility of means and in detecting the goals.

Also, a resize of the notion of conflict takes place by adding some new attributes:

⇨ *permanence* – the application of a global strategy that permanently integrates all the informational processes not only in times of crisis or conflict;

⇨ *transversal movement* – the influence of society as a whole and the fundament on multi-disciplinarily approach and concepts of systems' integration;

⇨ *duality* — the disappearance of differences between the military sphere and the civilian one (at national level, the centre of gravity moves toward other fields – banking, financial, energetic, generally toward the civilian infrastructure of which defence becomes difficult with conventional forces and means).

Informational resource is the main category of resources of the modern war and includes the following fields:

- The political, economic, social and military necessary for command and control at the strategic level;
- The military capacity of potential adversaries and the dynamics of war preparations;
- The military doctrines, strategic organization and preparation of military systems, territory, economy and population for defence;
- The possibilities of the armament systems and fight techniques, their use and integration in the conceptions for war leadership;
- The scientific research activity related to defence;
- The orientation of mass-media and the reaction of population to the military conflicts (events from the late two years prove the perverse effect of media war over an important segment of population easily to influence because of the lowered level of correct informing);
- The sphere and the structure of command, cooperation and announcement information, organization and use of informational systems;
- The overall features, the use and evaluation of the cryptographic systems' resistance;
- The ability to counteract the actions of espionage, diversion, terrorism and false news dissemination;
- The level of training and the moral of troops;
- The overall information of economic, financial, social, diplomatic or other nature etc.

Information and Communication Technology offers the possibility of timely information, damages the national and global public opinion, shapes the politicians' actions and produces an accentuated overlap of tactical, operative and strategic levels. It is seen more clearly that a greedy political class can be major factor of vulnerability for a state.

Commandants of each level must be aware that in a world of direct and real-time communications, each isolated event can be seen simultaneously at all the three levels.

Nowadays, the military operations must be based on the knowledge resulted from precise, exact and relevant data and information collected, analysed and diffused by a technical "system of systems".

The integrated information systems as C4I (Command, Control, Computers, Communications and Information) will provide for the commandant possibilities to see, feel, interpret, decide and engage actions at each point of the action strip or in the area of informational (informative) responsibility.

The informational era has as content the explosive use of growth of informatics, communication and cybernetic means of fight and the information becomes the object, mean and procedure for a new field of action – the informational one. If these actions are undergone to the right and successful moment they can prevent conflicts, reduce loses and rapidly stabilize the conditions to develop the military actions.

Unfortunately, nowadays there exists a full understanding of the fact that the informational dimension is not artificial but very real and actual. Also, information is not perceived to its true identity: as weapon, risk factor, operational and technological instrument.

The main characteristics of informational actions are the following:

- the volume of information needed to elaborate decisions and to lead military actions enhance 10-15 times more than in the World War II;
- increases the possibility of information and therefore the specific means become increasingly performant;
- the beneficial influence of information processing on the armament system capacity but also the evil action of disinformation or informatics viruses on the specialized processes achieved with proper computers and software;

- the explosive increase of quantity of information necessary for the fighter to deal with the requests of the modern battlespace;
- the integration and use of intelligent armaments and techniques of battle;
- the development and enhancement of specialized structures by providing information security;
- the cyber feature of military actions and the technological and informational closeness between the command and execution;
- some difficulties in the assignation of the adversaries;
- the multitude of regarded targets;
- the absence of some specific and clear indicators of warning;
- the persistence of effects and the lack of some rapid methods to retrieve the consequences it generates;
- the use of some relative simple, cheap and widely spread technologies;
- The disappearance of disparities between the levels of command.

The main informational activities

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

- *Data* – individual or statistical facts in an uncorrelated form;
- *Information* – a communication, news or message that acknowledges by a situation;
- *Knowledge* – the result of information processing, process in which intervene intuition and human thinking.

There are four key stages of the information's lifecycle: creation, collection, dissemination and use. These stages are distinctive although they have many common features.

The technological development affected the speed and volume of collection and dissemination of information.

The informational revolution leads to the development of some modern interconnected and interdependent systems that cannot be conducted manually.

Information as a strategic military asset was always recognized like this by the commandants particularly in the idea of a better knowledge of adversaries' intentions and concomitantly of own protection, plans and operational stage of military actions. If this information is available in the

military field, from the strategic level of command to the commandants from the tactical level, there can appear a series of problems regarding their trust in integrity, relevance and accuracy of the presented information.

The informational activities from the modern battlespace involve the procurement, transportation, processing, conversion, distribution, use, protection, exploitation and management of information that briefly consist in:

❖ ***Collection*** – the initial acquisition and filtering of data on the basis of the planned needs and their presentation in a form adequate for transmission. These information regard the mission, adversary, own troops, field, weather state and time at disposal. The process of acquiring the information is achieved with the support of electronic systems, of operative activities of research and reconnaissance, of strategic, operative and tactical research, by co-working with the police body and mass-media etc.

❖ ***Transportation*** – the communication of information and data to the receivers of the recipients.

❖ ***Data processing*** – their storage, extraction from the memory dispositive, updating, filtration and synthesis in order to result the minimum of information in a useable form.

❖ ***Conversion of information*** – their transformation from a form in another without loses and without the modification of their precision in order to transmit and display as text, images in fix and movement format, data for computers, etc.

❖ ***Distribution (dissemination) of information*** – the transmission of processed information to potential users.

❖ ***Use of information*** (after data are obtained, analysed and verified) – the updating and awareness of the real situation in order to continuously improve or adapt the military decisions, plans and actions.

❖ ***Protection of information*** – the analysis of vulnerabilities of own forces and means of command and control to the electronic actions, acts of physical destruction, misguidance, propaganda of the adversary as well as the settlement of means to apply and verify the countermeasures. The elements of infrastructure that have to be protected are the databases, networks of computers, systems of communications, research and other auxiliary means from their framework.

❖ ***Exploitation of information*** – the action used to get some advantages for military operational goals of the acquired information. It involves the interception and analysis of adversaries' messages, extraction of information from its databases, establishment of measures to denaturise, to decay or manipulate its informational capacities.

❖ ***Denaturation of enemy's information*** – the attack measures against the command and control regarding the influence, decay or destruction of enemy's information and informational (C4I) systems.

❖ ***Management of information*** – the coordination and careful synchronization of information and C4I informational systems and comprises: the management of electromagnetic spectre, the election of sources and systems used, the provision of some feasible informational flows (with the vertical and horizontal integration), interception of information from many sources.

Informational processes and environments

For the pertinent analysis of informational dimension of the modern battlespace it is very useful to briefly characterize the informational environments with important impact over the military actions' organization and development as follows:

❖ ***The global informational environment*** – it comprises personalities, organizations, systems, etc., many of them outside the military or national or international command authorities control that collects, processes and distributes information at the national and international levels;

❖ ***The national informational infrastructure*** – it comprises public and private telecommunication networks that serve physical and juridical persons, information and their content, databases, hardware terminals and software products for the access to information, personnel collecting, processing, storing and generating new information, etc.;

❖ ***The informational infrastructure of defence*** – it comprises the necessary resources for the transfer, processing, storage and display of information, technical means for command and control, research and other categories of means to broadcast voice, fix and moving images, multimedia services particularly useful for the military field;

❖ ***The military informational environment*** – it consists by military and other categories informational systems and own structures significantly supporting or influencing the military operations;

❖ ***The informational (C4I) systems*** – they consist in infrastructure, structures, personnel and components collecting, processing, storing, transmitting, displaying, distributing and acting in conformity with the acquired information.

The intensive development of information and communication technology created new procedures of data management and processing. They include images, graphics, schemes, digitized maps, and databases which combine with modern techniques of communications (satellites, radio stations with jump of frequency, microwave radio-relays, tropospheric and ionosphere radio stations) and provide global, national and military infrastructures.

Modern systems of information

To the basis of function of command and control system there are information about events, environment, adversary and own troops, that influence or can concern military actions and that following the processes of processing, analysis, storage and valuation grounds the decision and substantially contributes in getting the informational supremacy.

„*Informational supremacy* – represents the ratio of informational domination that offers to the personnel the possibility to use (C4I) informational systems in order to get operational advantages in the conflict or to control a certain situation, concomitantly with the diminution of adversary's possibility to use necessary information to the processes similarly for its troops"[1].

The achievement of informational superiority comprises two components equally as importance – accumulation and protection of own informational capacities and decay of adversary's informational capacities.

Informational superiority depends on:

• The capacity to access a big amount of information from many sources and environments (political, social, economic, military, religious

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

etc.), concerning the adversary and own troops, necessary information in the area of responsibility of the command and control act;

• The diminution of possibilities to use false or null information by using some efficient techniques and procedures to collect and authenticate;

• The performances of sensor systems to collect, process and broadcast on channels of communications the information in different formats;

• The capacity of the communication systems to shortly circulate the whole flow of information, on vertical and horizontal ways;

• The capacity of the command bodies to use the information in the elaboration of decisions as to advance the possible actions of the adversary;

• The level of data and information protection and security regarding own troops and their actions.

The provision of informational superiority is achieved by many procedures as follows:

⇨ The growth of flow by the use of the communications systems with topology, the use of special units, officers and search team. Innovations from the systems of sensors, processors, communications and computers can offer to the commandments better awareness of operative situation by the immediate access about the adversary and own troops;

⇨ The ,,visualization" of the battlespace by the awareness of the current situation of own troops in connexion with the adversary's situation and the weather conditions;

⇨ The projection of final desirable situation – mission accomplishment – sequence visualization of activities own forces fulfil from the initial to the final situation;

⇨ The knowledge of situation by analysis, the acquirement of commandant intention and of battle (operation) conception in direct relation with the disposition and possibilities of the adversary and own forces;

⇨ The permanent management of information in the conditions of collection and processing of huge amounts of information, the diminution of command cycle and short notice decision elaboration.

The materialization of the concept emphasizing "the attack actions oriented toward the informational networks centres"[2] is essential to provide and exploit the informational superiority. This concept is to all the hierarchical levels and contributes to the overlapping of the strategy, operative art and tactics. It finds its substantiality in the integration and coordination of some forces well-informed and logically dispersed in the battlespace.

The elements that contribute to the fulfilment of this intention are three[3]:

⇨ Informational network (C4I) with superior performance that resist and survives to the whole range of physical threats and informational operations;

⇨ Systems of sensors capable to achieve a high level of awareness of the battlespace synchronized with the military operations undergoing;

⇨ Improvement of the capacity to exploit the forces and means by networks of modern and efficient engagement (provision of some new operational capacity for preventive planning, integrated management of forces, the diminution of time of attack over the targets).

Many specialists believe the fundamental shift from the actions based on platforms to actions based on centres, with informational superiority, constitutes a revolution in the military affairs and is in the core of this transformation process.

The technological improvements lead to the considerable growth of quality, precision and opportunity of the information put at the disposal of information compartment, as well as of informative products designed to be used by the commandant. All the staff officers must understand the principles and techniques of the informational activity if they want their plans to be realistic. Consequently, it is important to remember that information offered by the personnel from the information compartment are the result of an analysis based on acquired data but also on other variable or presumed factors.

[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 problematic there must be known the usual terms used in the informative field:

⇨ *data* – specific unevaluated materials resulted from different descriptions that can be used in the fulfilment of informative products;

⇨ *information* – result of data processing;

⇨ *informative products* – result obtained following the analysis and processing of information;

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

⇨ *agency* – organizational structure or person employed in the collection and/or processing of the information for informative goals;

⇨ *supervision* – systematic observance;

⇨ *area of influence* – geographical space inside which the commandant is directly involved in influencing the military actions by manoeuvre and fire support systems under his/her command and control;

⇨ *area of informative responsibility* – geographical space allotted to a commandant wherein he/she is responsible to provide information by using the means at disposal;

⇨ *The area of informative interest* – geographical space about which a commandant asks for information on the factors able to damage the recent and future military actions and their evolution.

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

No.	Big unit, unit or formation	Area of influence (km)	Area of informative responsibility (km)	Area of informative 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, p. 1-2.

The informative cycle comprises many stages[5]:

• *The informational requirements of the commandant provide the orientation, planning and leadership* of current and future informative activities, in agreement with the priorities settled by him/her.

• *The collection* represents the stage wherein the data and information are exploited and delivered to the major staff in order to be analysed and to get desirable informative products.

• *The processing and exploitation of information* represents processes by which the collected data (information) are evaluated, analysed and transformed in informative products that are used in informational-decisional processes.

• *The achievement of informative products* consists in the collection, evaluation, analysis, integration and interpretation of information from one or many sources, in order to get a final product. The time constraints and evolutions in the modern battlespace determines the overlap of phases to process and synthetize the information.

• *The distribution and integration of informative processes* is done by their transfer to the bodies that asked for them in order to be used in the process of decision elaboration and planning the military actions. The personnel of the information compartment from all the levels evaluates the development of informative cycle and the acquired results.

The information system as component element of C4I systems is represented by the aggregate constituted by the personnel, means, procedures and techniques used to obtain and process data, to transmit information and informative products to the compartments and persons involved in command and control processes. It results that an informative cycle starts by the formulation of specific requirements from the command and control processes and closes with the provision of the informative products. Also, there must be observed the interdependencies and strong correlations of the information system with the other subsystems component of the C4I systems: command and control, computer networks, communications systems, armament systems, etc.

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

The reconnaissance of the battlespace involves missions to acquire, by visual observation or other methods of detection, information about activities and resources of the adversary, as well about meteorological, hydrographical and geographical characteristics of a well-defined area.

Surveillance of the battlespace represents the systemic observance of it in order to provide opportune information on the development of fight actions.

As concerns the way of data and information origin, the sources can be constituted by: research of electro-magnetic signals, human elements and different bodies; research by satellite.

Research of electronic signals that aims the discovery, localization and evaluation of electromagnetic radiations of all categories and comprises:

❖ *Research of communications* – that regards the search, interception, localization, analysis and exploitation of radio traffic of the adversary and to provide the evaluation on this basis of its forces' disposition, deployments and intentions;

❖ *Electronic research* – that comprises activities to collect and process potential hostile electromagnetic radiations (excepting some of the communications means) emanated from the nuclear explosions and radioactive sources.

The research executed by humans and the specialized bodies cover all the specific aspects i.e.: observance of adversary's activities; patrols, detachments, etc.

The imagistic research includes forms of research acquired by photos, thermic observance and other equipment capturing images.

The acoustic research acquires data by the collection and analysis of acoustic phenomena. The sensors used for this goal can be passive (receive the noises) or active (transmit pulsating acoustic waves and afterward receive the echo). The sources of acoustic research can be stationary or equipped on the ships, floating platforms, in immersion or on the bottom of the sea.

Sources of information can be: research subunits (observation posts, patrols or research detachments), research subunits of weapons, airships, helicopters, UAVs, means of electronic nature, prisoners and refugees.

Agencies are assimilated with: the information structures (information, artillery, and engineering); operations, aviation and systems of

electronic research; elements of research in the dispositive of the adversary; structures interrogating prisoners, etc.

The techniques used in the surveillance of the modern battlespace regard[6] how the electromagnetic spectre is used by the adversary: in infrared – the images acquired by reception of radiations emitted or reflected by the surface of the objects in the segment from 0.72 to 1 μm; thermic images in infrared able to distinct differences of 0.1°C. This allows for the targets to be detected as images by their visualization or surveillance with the TV; visually, inclusive by photo; in ultraviolet by the reflection of radiations in this field; diverse types of radio-locators; the exploitation of acoustic and seismic waves.

The efficiency of these techniques can be improved by: the use of air platforms with or without pilot able to provide almost real-time information until the tactical commandments; the use of land sensors; signals' processing.

These technical systems can be active or passive. The active systems radiates energy toward the target in order to illuminate and discover it. The passive systems receive the energy radiated by the target.

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

The optical instruments are passive, cheap, light and feasible, but are inefficient on night time. These systems amplifies the light of the ambient by electronic means, thus the observatory can see poor illuminated targets.

Lasers are active systems and have two applications: to discover the target with a precision from ± 5 m to 20 km distance; to mark the targets by illuminating them.

Radars transmit an electromagnetic impulse that is reflected by the target and is again received by the radar. Some radar detects the auto vehicle movement until 24 km and of humans until 3 km.

[6] *JSP 120 (3) Manual of Service Intelligence.* Department of Defence, United Kingdom of Great Britain, London, 1997, p. 39.

The alarming dispositive functions on the basis of seismic or infrared sensors.

The research in the dispositive of the adversary is accomplished for range (6-50 km) and large (over 50 km) distances.

Satellites are also efficient means of research as they achieve the photography and research by radiolocation, etc.

By the perspective of efficient function of research systems there is needed if is possible in real-time to be used some performant specialized technical means, interfaces to adapt the sensors with digital channels of communications with high speed of broadcast and maximum precision.

Also, the information department must posess of automated technical means (performant computers) and specialized software to allow the processing of data and information in opportune time, the growth of information level of the commandments and the diminution of the risk level of informational management.

In this first part, we tried to show again to the people interested by military affairs, some aspects of the role and place of the recent informational systems in the modern war concomitantly taking act the evolutions and lessons learnt of the late conflicts, inclusively the Russian-Ukrainian crisis. We intend, if would be possible, to continue in a future issue of this journal to present the other component elements of the informational systems which will be analysed from the perspective of some recent information.

BIBLIOGRAPHY

*** Law on the classified information protection no. 182/2002, Official Monitor 248/2002 (Translated from Romanian: Legea privind protecția informațiilor clasificate, nr. 182/2002, M.Of. 248/2002).

*** Law on national security of Romania, no. 51/1991, Official Monitor 163/1992 (Translated from Romanian: Legea privind securitatea națională a României, nr. 51/1991, M.Of. 163/1992).

*** Securitatea informațiilor, Centrul de Expertiză în Domeniul Securității, Bucureşti, 2008.

*** Sisteme informaționale – Sesiunea anuală de comunicări ştiințifice cu participare internațională, Editura UNAp, Bucureşti, 2007.

*** Joint Doctrine for Operations Security, Departament 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.

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

ALBERTS, Davids S., Richard E. HAYES, *Planning – Complex Endeavours, CCRP.*

ALEXANDRESCU C. şi alții, *Supremația electromagnetică*, Editura UNAp, Bucureşti, 1999.

ALEXANDRESCU C., *Amenințări informaționale asupra sistemelor de comandă şi control în acțiunile militare moderne "SI-2007".*

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

ALEXANDRESCU Constantin, ILINA Decebal, MINCU Constantin, *Bazele matematice ale organizării sistemelor de transmisiuni,* Ed. Militară, Bucureşti, 1994.

ALEXANDRESCU Constantin, ALEXANDRESCU Gelu, BOARU Gheorghe, *„Sistemele Informaționale Militare" – servicii şi tehnologie*, Editura UNAp „Carol I", Bucureşti, 2010.

DUMITRU Cristea, prof. univ. dr., *Infrastructura de rețea şi informațională în cadrul războiului bazat pe rețea,* Editura CTEA, Bucureşti, 2008.

DUMITRU Cristea, prof. univ. dr., *Sisteme C4I,* Editura Militară, Bucureşti, 2005.

EUROCOM D/1 Tactical Communications Systems. Basic Parameters, 1986.
FRIEDMAN George, 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.
FM 34-1 Intelligence and Electronic Warfare Operations, Headquarters Department of the Army, Washington DC.
GARSTKA John, *Information and Network – Centric Warfare*, J 6 Presentation, Washington, DC, 1998.
MINCU Constantin, dr., GREU Victor, dr., ROTARIU Costel, ing., *Salt de frecvenţă şi contrasalt de frecvenţă,* Editura Militară, Bucureşti, 1998.
MINCU Constantin, dr., TIMOFTE Gruia, dr., *Compatibilitatea Sistemelor Radioelectronice,* Editura Olimp, Bucureşti, 1999.
MUREŞAN M., VĂDUVA Gh*., Războiul viitorului, viitorul războiului*, Editura UNAp, Bucureşti, 2005.
PÂRLOG Nicu, Armele Viitorului, http:/us.mg6.mail.yahoo.com.
Serviciul Istoric al Armatei – *Enciclopedia Armatei României*, colectiv de autori, Editura CTEA, Bucureşti, 2009.
Simpozionul Jubiliar AFCEA, Washington DC, 18-19 Iunie 2006.
TOFFLER Alvin şi Heidi, *Război şi anti-război*, Editura Antet, Bucureşti, 1995.
TOFFLER Alvin, *Powershift, puterea în mişcare,* Editura Antet, Bucureşti, 1995.

Specialty Journals
Gândirea Militară Românească, 2001-2015 years
Buletinul Universității Naționale de Apărare “Carol I”, 2008-2015 years
Revista Forțelor Terestre, 2005-2015 years
Impact Strategic, 2006-2015 years
Revista de ştiințe militare, 2006 – 2015 years
Revista comunicațiilor şi informaticii nr. 2 (10)/2009 – special number
Revista comunicațiilor şi informaticii – special numbr, July 14, 2008.