Annals of the Academy of Romanian Scientists
Series on Military Science
Volume 1, Number 1/2009

COMMAND AND CONTROL SYSTEMS – CURRENT AND FUTURE DEVELOPMENTS

Colonel Professor Gelu ALEXANDRESCU, PhD
Colonel (ret) Professor Gheorghe BOARU, PhD

Introduction

The long wanted world peace has not been brought about by the 21st century either and it may not be achieved so soon. There may not be world peace or maybe peace must be redefined the same way warfare has been. Today, there are military conflicts between state coalitions and a political regime from another country. The declarations of war specific for the 20th century are not in accordance with international laws, but interests of all kinds make possible the existence of conflict hotbeds. When the crisis management process fails, military conflicts are imminent. The essential changes of the security environment, Romania's adherence to NATO and the pursuit of national interests impose that the Romanian military forces participate in such conflicts.

Current military conflicts bring about major changes throughout the military domain (i.e., military art, doctrines, organization, training, equipment, action, etc), but all these transformations have a common element: technological progress. Throughout our troubled history, technological progress has directly influenced the military at all levels. One armed combat law says there is a close connection between the military forces' technological level and the way the latter acts. However, in the past decades, the military forces have significantly influenced the technological progress by directly financing technological researches. This financing is based on new action concepts the armed forces wanted to use but did not have the necessary technical support.

The increase of the information component role associated to military action at the expense of the energy component has determined major theoretical and practical changes. Now in a military action it is necessary to control information in the confrontation environment and have at least information superiority. The military wish to concentrate effects and not forces has imposed progress of the information and decision support information systems and their transformation into integrated command and control systems. The integrated command and control systems have developed from command, control and communication system to systems of command, control, communications, computers, enemy and terrain intelligence, surveillance and reconnaissance.

In order to know the prospects of command and control systems, we must analyze first the information warfare and one of its targets – the command and control system. By comparing different concepts of information warfare or operations within the US, UK and Romanian doctrines and also NATO doctrine we can understand the potential differences. Thus we can identify the most important factors which determine or influence the development of the command and control systems and even infer their prospects under the impact of the respective factors.

1. The command and control system – the information warfare and operations target. Viewpoints of foreign and Romanian military experts

The information warfare concept results from the fact that information and information technology are increasingly important for national security and military confrontation. Consequently, future conflicts will be characterized by the fight to control and dominate information because those who will master the information warfare techniques will have an advantage over the others. Starting from this, Marin C. Libicki wanted to demonstrate that information warfare cannot be considered a separate technique of waging classic warfare; in exchange, there are seven forms of information warfare because they imply denial, protection, manipulation and degrading information: command and control warfare, intelligence-based warfare, electronic warfare, psychological warfare, “hacker” warfare, economic information warfare, cyberwarfare.

Emphasizing the difficulty of defining information warfare, the same author considered that it should be considered a heterogeneous mosaïc of the seven forms of manifestation, which can encompass vast areas of human activity (i.e., political, economic, cultural, social, etc.), beyond the military organizations’ responsibilities. Thus, information warfare is very little described in the official military publications. However, there are several doctrines of information operations which approach military actions in our field of interest.

In the US doctrine, information warfare is defined as "information operations during crisis or conflict to achieve or promote specific objectives focusing on specific one or more enemies." Information operations are defined as actions executed "to affect enemy information and information systems at the same time with defending own information and information systems." They focus on information and information systems in order to affect a process based on information, no matter if it is human or automatic.

British military specialists have developed the *information campaign concept,* defined as the coordinated transmission of information by the entire governmental activity in order to influence the decision-makers in the appropriate way determined by political objectives and at the same time protecting own decision-makers. The central element of the concept is based on the fact that any action or inaction sends a message from which the partisan, neutral and hostile audience derives and aggregates deductions which determine their actions.

The British Ministry of Defence contribution to the information campaign consists of the coordinated use of any military capability to influence the target audience at any level and prevent it from imposing its will by using information and media operations. Information operations are defined as coordinated actions executed to influence an enemy or potential enemy, in support of political and military objectives by undermining its will, cohesion and ability to decide due to affecting its information, information systems and information-based processes at the same time with protecting own decision-makers and decisional processes.

Starting with 2006, Romania uses SMG/FOP-3.15 information operations doctrine, according to which information operations are synchronized and coordinated actions, planned and conducted in order to get the desired effects over the will, understanding and capabilities of the enemy, potential enemy or other entities approved by the National Command Authority, supporting the achievement of the commander's objectives by affecting the information and information-based processes at the same time with capitalizing own information, protecting and enforcing own information-based systems. Their purpose is to affect or influence the key elements for the decision factors or opinion leaders: will to act, power of understanding and their perception regarding the respective situation; capabilities/means at their disposal to act accordingly.

The NATO Allied Joint Doctrine AJP-01(B)/2002 publication defines information operations as those actions supporting political or military objectives in order to influence the decision-makers by affecting information, information-based processes and the systems of command, control, communications and information used by them at the same time with exploiting and protecting own information and/or information systems.

Therefore, the information warfare concept is explicitly used only by the US army to differentiate peacetime information operations from the crisis or conflict ones. Thus, the term "warfare" should be translated and interpreted as "confrontation" focusing on both attack and defence.

Also, the targets aimed at by information operations differ within the four analyzed doctrines. While we agree that one of doctrines' roles is to set limits within which commanders can use their force and means, there are significant differences in approaching conceptually the information operations.

There are different definitions given to information operations. This difference emphasizes the dynamic and vast character of the concept. Also, this diversity is due to other different angles to approach the issues when the technological progress overcomes the classical ways to wage war specific for the 20th century.

Only the British doctrine approaches the connection between the political decision and military actions affecting the information environment and also synchronization or coordination with the national power elements when they conduct actions with impact on the information environment.

2. Command and control systems used for the conduct of military operations

"Command and control" (C2) is the term used today for the conduct of military forces. This term is relatively recent and replaces the word "command" or "conduct" used in the past. The "command" concept appeared before other concepts such as "politics" or "industrial management" and developed separately because of the different traits of warfare compared to other human actions. The evolution of the "command" concept was influenced by three factors: time, the serious consequences of errors and the concern for diminishing confusion during military actions.

Studying foreign military publications, we came across several definitions of "command and control". Thus, NATO uses two closely connected terms, associated but not synonymous. Command is the authority invested in a person. It is the process through which a commander imposes his intentions or will on his subordinates in order to execute a certain action. It contains the authority and responsibility for the forces allocation and deployment with the purpose of accomplishing the mission received by the commander. Control is the authority exercised by a commander. It is the process through which a commander, assisted by his staff, organizes, directs and coordinates the activities of the forces allocated.

Analyzing the two concepts above, we can draw several conclusions. Firstly, the command is "an authority and a responsibility" whereas control is just "an authority". The term "authority" must be understood as "having the right to…"

and the term "responsibility" as "being responsible for…". The control authority can be delegated to another subordinated person or structure. At the same time, command cannot be delegated because the responsibility is only the commander's. Secondly, the command is "an invested authority", while control is "an exercised authority". Thirdly, command refers to forces (the commander allocates forces and assigns missions) and control refers to activities (i.e., the commander organizes, directs and coordinates the activities of subordinated forces).

The American army uses more nuanced and slightly different definitions. Thus, the command is the authority the commander exercises legally on his subordinates due to his rank or appointment. The command includes authority and responsibility for the effective use of available resources and also for planning the use, organization, direction, coordination and control of military forces in order to accomplish the mission received. Also, it includes the responsibility for the subordinated personnel's health, morale and discipline. The control is the authority exercised by a commander on a part of his subordinates' activities.

We can notice an important difference between NATO and US concept. In our opinion, this difference emphasizes the fact that, given the alliance's character, a NATO commander has a lower degree of authority on his subordinate forces than a "national" commander.

Analyzing the military actions in the industrial era, we can state that there was not just one command and control conceptual model. There are at least six conceptual approaches, shown in fig. 1 which, when applied, were successful on the battlefield.

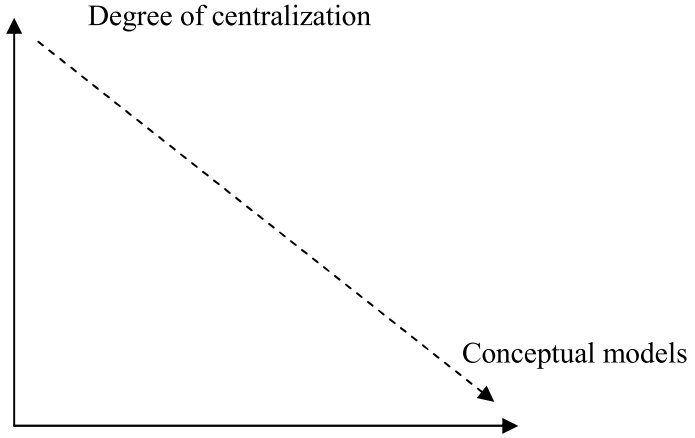

Figure no 1. The centralization degree of different C2 concept

The major differences between the six concepts are closely linked to the degree of centralization they imposed. The most important factors that influenced the evolution of different concepts are: the military action physiognomy (static

actions or maneuver warfare; the continuity of communications between echelons (i.e., sequential or continuous); the professional competence of the commanders and subordinated forces.

Most part of the philosophy and practice in the field of command and control was developed and improved during the industrial era. The current principles of command and control are valid in the military and civilian fields. These principles are division, specialization, hierarchization, optimization, coordination, centralized planning and decentralized execution. The most modern approach of the command and control mechanism in the industrial era was a linear one. The commanders divided the combat space and the military actions in phases, used specialization, optimization and centralized planning to improve the subordinated force's action and used the decentralized execution and other cyclic processes to ensure the flexibility of their efforts compared to the changing situation of the armed confrontations.

While for the command and control terms there are not big differences, the definition and use of the term "command and control system" is different. NATO Allied Joint Doctrine AJP-01(B) shows that, in order to exercise his command and control authority, the commander and his staff use standard procedures and the Alliance's Communications and Information System. Together, these two command and control processes form a command and control system which the commander, his staff and subordinates use to plan, direct, coordinate, control and support military actions.

In the US army, the term "command and control" means exercising the authority and directing the subordinated forces (organic or temporarily subordinated) by a commander with the purpose of accomplishing the mission. The command and control system represents the means, communications, procedures and people essential to a commander for the planning, guidance and control of the subordinated forces.

Military experts have different opinions when they explain "what a modern C2 system is and what it is made up of". In some cases, the C2 system is considered a mere technical system destined to help the commander and his staff in conducting the command and control processes. In other cases, the C2 system is considered a complex system, made up of two main parts: on the one hand, the technical system and, on the other, the commander, his staff and the working procedures. Another definition explains the C2 system as a sum of C2 subsystems or nodes.

Another approach uses the organization and the information system theory. Thus, any organization has a decision system, an information system and an operational system. Other military experts divided the C412 systems and analyzed

their subsystems such as: the command and control subsystem; local and extended computer networks; information subsystem; interoperability.

All of the variables above are correct and logical as long as they are considered from the viewpoint their authors had. The logic of the analyses done leads us to an evolutionist approach of the C2 systems.

3. Development prospects of the command and control systems

From the conceptual point of view, the future of C2 systems is based on the full integration of the command and control processes in the information system. Because the decision remains the people's attribute, it is essential that the future C2 system allow the use of three categories of decisions:

1. "The obvious decision" appears when all the necessary information is known and there is no degree of uncertainty. It can even be automatized at least at the level of some rules of engagement.
2. "The simple decision" is the one for which a set of appropriate variables and the selection criterion between them is well-known and understood. This type of decision can be partially automatized.
3. "The complex decision" cannot be automatized and is the one for which we do not know the appropriate variables and the selection criterion. It is solved through courses of action.

A large number of the commander's tasks and activities can be easier executed using simulation technologies. Until now, these technologies have been used only for analyses and training. However, in the future, the commanders' efficiency will be improved by using simulation programs designed to facilitate the development and analysis of the courses of action, reviewing the plan of action and monitoring the military action.

In order for the future C2 systems to be effective, they must permit new methods of collaboration between the staff and new methods of interaction with the information means and sources. To achieve this desideratum, we will have to build a wide range of man-machine interaction technologies which should increase the speed and efficiency of the interaction between the user and the computer.

Real-time simulation

A large number of the commander's tasks and activities can be easier executed using simulation technologies. Until now, these technologies have been used only for analyses and training. However, in the future, the commanders' efficiency will be improved by using simulation programs designed to facilitate the development and analysis of the courses of action, reviewing the plan of action and monitoring the military action.

The future simulation programs specially designed for use during military actions could be named real-time simulations – RTS. Based on a sufficiently high calculation power, RTS will facilitate the real-time analysis of the implications of applying a certain decision. RTS will simulate the development in time of the courses of action and will provide timely information about each simulated course of action. Based on this information, the commander will make the right decision.

The RTS beneficial effects are multiple. The most important are: improving the situation, preventing the excess of information and decreasing the decisional cycle.

With the help of RTS, the staff will be able to analyze more adequately several courses of action simultaneously. During simulations, the problems about forces' synchronization will be automatically solved. Then, the results of the simulations will be used as a criterion of assessment and selection of the courses of action. Another advantage of using RTS is diminishing the number of people involved in the courses of action analysis. RTS will be able to run on a single computer and will need a single operator.

While reviewing the plan of action, different functions of a force (fire support, direct air support, mobility and counter-mobility, etc.) will be revised much easier in order to coordinate the subordinated forces and to fully grasp the approved plan of action. Reviewing the plan with RTS help represents a major advantage because the participants from the subordinated echelons do not have to go to the higher echelon point of command. It is enough to connect several monitors of the subordinates to the computer from the higher echelon by RTS.

A "monitoring agent" software program notices at once the significant deviations from the initial plan and warns the commander if the success of the initial plan is in danger and if a new decision is necessary.

Today it takes a significant part of the technologies to design and build an RTS. However, there are still many problems to solve both from the conceptual and technological viewpoints.

There are two methods to represent the virtual space the military action will take place in. The 2D method (two dimensions) is advantaged by the smaller hardware requirements and because the current commands are used to work on flat maps. The 3D method (three dimensions) allows for a more complete and intuitive approach of the simulation but will require powerful hardware platforms and the intense training of commands to use three-dimensional maps.

The "monitoring agent" types of software will require the asynchronous and very often interrogation of the RTS database. But this database is dynamic and permanently changed by the simulation. In order to maintain the integrity of the

RTS base, it is necessary to develop a new database dynamic management technology which permits to fill in and interrogate the RTS database.

In order to make a rigorous prediction of the results of a military action, the simulation entities must behave the same as the real units they represent. The future way of action of a military entity is closely connected to its former performance in similar military actions and a series of factors for each entity (i.e., morale, quality of personnel, level of education, experience, etc). The same applies for the enemy forces. I tis therefore necessary to develop a technology which highlights the different behavior of an entity of the same type.

There are several methods to integrate simulation in a C2 system. Simulations can be used in all phases of a military action. The greatest benefit will be obtained when the current staff procedures will be replaced by new revolutionary ones. At present, there are several technologies which can be developed in order to be included in an RTS system. The other necessary technologies can be demonstrated in the near future. Given the current technological development, we can estimate that the first real-time simulation system will be operational in 2010.

Technological perspectives

In order for the future C2 systems to be efficient, they must allow for new ways of cooperation between the personnel and new ways of interaction with the information means and sources.

To achieve this desideratum, a wide variety of man-machine interaction technologies will be necessary (together with the necessary physical devices) by which the speed and efficiency of the interaction will be 10 times as high. The necessary technologies include: voice recognition in free conversation, handwriting continuous recognition, following the person and face mimic, virtual reality and 3D graphics, “handheld” device integration with other data introduction and display devices, teamwork and joint display of results, etc.

Moreover, the automated data recording will make the presentation and assessment of the respective data more efficient. This improved type of multi-mode recording will ensure an institutional memorization of the activity in a command, which will be accessed at any moment. Also, it can be used to create “macro” or “intelligent agents” programs for the automation of routine tasks. Taking notes will be streamlined by the “public common notes” technology. All meetings will be recorded, watched and processed in order to permit their future indexing, browsing and summarizing.

All this will be created using flexible tools of software application to design and develop the software programs. This in turn will permit the software

developers to create new programs or adapt the old ones when the situation requires. Fewer people will be necessary to configure the systems and create the additional access interfaces to new data bases or sources.

Until now, the following software technologies have been demonstrated: JANUS – voice recognition; NPEN++ - handwriting recognition; MULTIMODAL TOOLKIT – access interface control; ARIADNE MAP TOOL – object visualization against a map background; PEBBLES – teamwork and data common display; ALICE – 3D space creation and display; CSPACE – meeting electronic recording and creating "evolutional" documents (through updating or creating new versions). These technologies are to be developed and integrated in the future C2 systems.

Data display perspectives

One of the main topics approached by the C2 system designers is the information display technique. Analyses and many experiments have been made to determine those display techniques permitting the immediate understanding of the changing situations in modern military actions. The most recent innovation in this field is "blobology" – the ink stain technique.

Current monitors use a bidimensional, static display system saturated with all sorts of diagrams. To represent forces, standard symbols are being used as they were also used during the World Wars. In fact, the current symbols mislead commanders about the real power of the forces represented by symbols. Looking at a symbol, the commander has to imagine the composition, deployment, combat power and other factors of the forces represented by that symbol.

The need to create a superior information display technique will be even more stringent in the future, when commanders will have plenty of information from a multitude of sources. Therefore, from the human point of view, there are only two practical solutions to manage a huge amount of data and information. The first solution refers to the automation of the process in order to increase the working speed. The second solution refers to the information intuitive display to increase the information density in the visual field.

Following the change of forces and terrain representation model, the information intuitive display will lead to their easier and faster understanding by the human observer. The decrease of information amount will not be necessary, only of its display in a different manner.

The people's perception will be thereby enhanced by increasing the available mental resources, reducing the search time, improving the ability to recognize habits (templates), increasing the number of deductions and of the monitoring realm.

These last few years, the "ink stain" technique has been developed in many phases.

The first phase used the conventional military symbols. The second was improved by using several force attributes such as the discovering area and the hitting area. Thus, we could instantaneously answer questions such as "What can I see and what can't I see?" "What can I hit and what can't I hit?". The third phase comprises several factors which can influence the forces representation by means of stains. The fourth phase brings about major improvement by including attributes at the level of entities. This permits passing from the representation deduced by interpolating data (i.e., gravity center, terrain, combat form, etc) to a representation based on the real-time position of all the entities.

The representation by means of component entities is much better than the traditional model. Displaying some elements of combat power and their orientation can be easily emphasized. Graphics can be adapted in accordance with the situation or the user's demands. Certain details or detail combinations can be selected for display. The free space and the space with forces is more accurately shown. The commander can interact with the real data of the subordinated forces without affecting them by the summary or presentation made by another person or program.

The visual effects have deep impact on the people's ability to explore data, assimilate information and produce knowledge. The benefits and consequences of a correct implementation are: increasing the speed to understand, improving the quality of adopted decisions, increasing the paces of military action, improving the decision-making process in conditions of fatigue or lack of experience, using smaller and more mobile command and control structures and also increasing communication and collaboration during planning and conducting the military action.

Digital identity

The information security in the future C2 system is a major challenge. Because the informational highways go beyond borders, locked doors are not enough to protect one of the most valuable goods – information. All the organizations admit the need to respond to the explosive traffic increase of electronic information from both their concern to protect their own data and to instrument this new environment for competitive advantages.

Information security is the key to these two requirements. We need the same degree of safety and trust in electronic information as well as in traditional ones. The answer to this challenge can be given by the digital identity, meaning the digital representation of the human identity in the interaction with other machines

or people within the networks. The digital identity must have the degree of complexity and robustness its use implies within a C2 system. In other words, certain systems reclaim a more robust digital identity because the degree of trust in the information sent can vary significantly in accordance with the type of system.

Implementing the concept of digital identity within some information systems involves firstly the development of software applications dedicated to digital identity management. Although such applications are more complex than the most sophisticated password management system, their achievement leads to major benefits in system management, security and productivity.

The development of digital identity technologies will change the world of computers, as the development of networks did a few years ago. The introduction of the digital identity concept seems to lead to a significant increase of the system complexity but, once integrated into the applications, this complexity becomes transparent to users, producing a rapid increase of scalability and productivity.

One of the most important implementations of the digital identity is the digital signature. The concept and utility of digital signature were defined and recognized several years before the first practical achievement, the initial scheme for the digital signature remaining today one of the most practical and versatile techniques available. Subsequent researches led to other techniques with significant advantages on the functionality and implementation; all these achievements are based on the asymmetrical cryptography, also known as public-key cryptography.

The digital signature of a message is a configuration of digits depending on a certain secret key owned only by the signatory (private key) and the content of the signed message. The signature must be submitted to a safe verifying mechanism so that none of the parties denies its actions during the transaction, and any litigation can be solved equitably by a third party without knowing the signatory's private key.

Acquisition perspectives

In 1994, Wilhelm Perry, the US Secretary of State, signed a directive which changes the US army acquisition system. Part of the Acquisition Reform Act, the new ministerial directive directed the armed forces services towards commercial-off-the-shelf in order to reduce acquisition costs by eliminating the design expenses of some systems with only military specifications. This directive forced the procurement programs directors to study the free market of products and services in order to discover the civilian commercial products which could be bought and used in the military field. The purpose of the American administration was to transfer the costs of product research, development and testing to producers.

An immediate consequence of the new American policy was the loss of influence of the American army in the field of electronics and computers. While in the 70s the American army bought more than 30% of the production of this sector, in the 90s it bought less than 0.5%. Thus, the development of the new generations of electronic products was determined by the needs of civilian consumers and the world market tendencies, transforming the military sector into a simple spectator.

The second consequence was the creation of a paradox. On the one hand, the acquisition program directors were happy with the low acquisition costs of electronic products. On the other, the users of the purchased products were unhappy with the latter's rapid wearing out due to the emergence of better ones. Moreover, the new generation of components cannot be used in the old systems due to compatibility problems and building characteristics.

This paradox increased in time because of the tight spiral of technological development. While in the 90s the rhythm of change was 3-4 years, today new generations of processors appear every six months. Thus, how could it be possible to maintain for 10 or 15 years systems that are 2 to 3-year old and for which there are no spare parts anymore?

The biggest problem of the commercial-off-the-shelf represents meeting the military requirements these products are used for. There are very few computer and communications products sold on the civilian market that meet the military specification at the same time without constructive modification. Moreover, in the testing phase of some products proposed for acquisition, nobody agrees to diminishing the key parameters of performance established by the future users for the respective class of products.

Starting with 2000, the American administration initiated the implementation of a new strategy in the field of civilian acquisitions. The so-called strategy to "adopt, adapt and develop" permits the acquisition at competitive prices of the commercial-off-the-shelf after they are modified or adapted to meet the military specifications. The working system is quite simple.

Firstly, some commercial products on the market are adopted by military institutions (they establish the possibility and opportunity of using them by the armed forces).

Then the producer adapts the products to meet the military specifications. After introduction in the procurement, they are developed in order to reach 10-15 years in service. There are three options to be considered: upgrade, rebuild or buy-back. Each option has its pros and cons. Selection of each option can be made for each product according to the cost-efficiency ratio and other criteria.

Conclusions

Modern C2 systems are very expensive. The future C2 systems will be even more expensive and the technological spiral is tighter every day. The hardware platforms and communication means have a shorter life every day because of their wearing out. Because of this, our hopes are linked to the software development. The upgrade or creation of new software applications can extend the life span of the hardware platforms and communication means. However, the software field is an expensive one because it incorporates the most modern products of human intelligence.

Moreover, "integration" is at present the most used word by the military decisio-makers. Likewise, in the filed of C2 systems, integration represents and will represent one of the most important directions. The higher the integration cost, the more different the C2 systems. Thus, it is necessary to centralize the C2 systems policy in order to reduce future integration costs.

In our opinion, the decision for acquiring any C2 system must be made at a higher military echelon and this echelon must also be responsible for the future upgrades until the respective system is decommissioned.

BIBLIOGRAPHY

1. Doctrina operațiilor informaționale SMG/FOP – 3.15, 2006.
2. AJP – 01 (B) Allied Joint Doctrine, NATO HQs, 2002.
3. AJP – 3 Allied Operations, NATO HQs, 2001.
4. Joint Doctrine for Information Operations, JP 3-13, 1998.
5. Joint Doctrine for Command and Control Warfare, JP 3-13.1, 1996.
6. Field Manual FM 106, Information Operations, 2003.
7. Joint Doctrine for Operations Security JP 3-54, 1997.
8. Joint Doctrine for Psychological Operations JP 3-53, 1996.
9. Joint Doctrine for Military Deception JP 3-58, 1996.
10. Joint Doctrine for Electronic Warfare JP 3-51, 2000.
11. Information Operations, Joint Warfare Publication 3-80, UK, 2002.
12. *NATO Glossary of Terms and Definitions AAP – 6,* 2002.
13. *Department of Defense Dictionary of Military and Associated Terms*, 2003.
14. Alberts D., Gratska J., *Network Centric Warfare – Developing and Leveraging Information Superiority,* 1999.
15. Boaru Gh., Pungă A., *Războiul informațional în viziunea unor specialişti militari străini şi români,* Sesiune de comunicări ştiințifice, UNAp „Carol I", 2007.

16. Boaru Gh., Pungă A., *Implicațiile războiului de comandă şi control asupra planificării acțiunilor militare,* Sesiune de comunicări ştiințifice, UNAp„Carol I", 2006.
17. Boaru Gh., Pungă A., *Etica atacului rețelelor de calculatoare din compunerea sistemelor de comandă şi control moderne,* Sesiune de comunicări ştiințifice, Universitatea Națională de Apărare„Carol I", 2006.
18. Boaru Gh., Pungă A., *Comunicarea în confruntarea informațională,* Sesiune de comunicări ştiințifice, Universitatea Națională de Apărare„Carol I", 2006.
19. Boaru Gh., *Războiul informațional şi operațiile informaționale*, Editura UNAp. 2004.
20. Libicki Marin C., *What is Information Warfare?,* 1995.
21. Roceanu I., *Fundamente ale sistemelor C4I,* Editura U.N.Ap., Bucureşti, 2004
22. Timofte Gruia, *Stabilitatea sistemelor C4I2 în condițiile războiului informațional intens,* Simpozion ştiințific, Universitatea Națională de Apărare, Bucureşti, 2004.