Annals of the Academy of Romanian Scientists
Series on Engineering Sciences
ISSN 2066 - 8570 Volume **4**, Number **2**/**2012**

SPECIAL AND MILITARY COMMUNICATIONS AND INFORMATION SYSTEMS AS VITAL PART OF THE CRITICAL INFRASTRUCTURES IN ROMANIA. SECURING THEIR PHYSICAL AND INFORMATIONAL PROTECTION

Constantin MINCU[1]

Rezumat. *Articolul prezintă câteva argumente asupra necesităţii studiului infrastructurilor critice din România, incluzând diferite sisteme şi reţele de comunicaţii şi informatice militare şi speciale. Se evidenţiază rolul şi locul unor astfel de sisteme şi reţele - resurse vitale pentru buna funcţionare a societăţii (asigurarea siguranţei vieţii cetăţenilor, a bunurilor materiale de bază, a serviciilor publice cele mai importante), precum şi câteva măsuri care trebuie luate pentru protecţia fizică şi informaţională, în cazul unor acţiuni militare ostile, al dezastrelor naturale sau al altor fenomene negative. În final, se formulează câteva concluzii şi propuneri.*

Abstract. *The article presents several arguments on the need to study the critical infrastructure in Romania including various systems (networks) and special military communications. It emphasizes the role and place of such systems and networks to provide national defense and security and the risks and vulnerabilities faced by these infrastructures, and some necessary measures to be taken for the physical and informational protection in the case of hostile military actions, natural disasters or other negative phenomena. Finally some conclusions and proposals are formulated.*

Keywords: *Systems, Special Military Communication, National Defense and Security*

1. Arguments for approaching this topic

Critical infrastructures – vital resources for the good functioning of the society (ensuring the citizens life security, of the basic material goods, of the most important public services) have been for a number of good years in the attention of the political, economic and military leaders in several countries in the world and has become the object of studies, plans and actions of some international organizations (UN, NATO, EU).

The concept of **„critical infrastructure"** was officially used in July 1996, in the United States, in the preamble of a normative act elaborated by the White House, entitled: **Executive Order Critical Infrastructure Protection.**

Considering that security, economy and even survival of the industrialized world would be dependent on three key closely inter-related[1] elements: **energy,**

[1]Mg. Gl. (ret), Ph.D., Member of the Academy of Romanian Scientists, mincu_constantin@yahoo.com

communications and computers – the normative act explained and defined critical infrastructure[2] as **"part of the national infrastructure that is so vital that the destruction or making them incapable of functioning may seriously diminish the defense or the U.S. economy[3]."**

Later, the sphere of content of this word will be extended and the theme developed. Especially after the 9/11 moment – the first proof that no country, no matter how strong it is, even the United States, will not be able to defend itself on its own its vital centers (**telecommunications,** supply systems for electricity and water, gas and petrol deposits, banks and finances, **military command and infrastructures centers,** emergency services, etc.).

The National Strategy to Secure Cyberspace designates the following **critical infrastructures:** "public and private institutions in the field of agriculture, food, water supply, public health, emergency services, governing, **defense industry, software and telecommunication,** energy, transport, banking and finance systems, chemistry and hazardous materials, as well as mail and navigation[4]."

At **NATO** and **European Union** level, there are also concrete preoccupations to define critical infrastructures and to advance concrete solutions for their protection against ample hostile attacks or natural calamities.

The problem of critical infrastructures has been and continues to be debated by numerous civil and military specialists from many industrialized countries, and it stays as an open issue, both for theoretical analysis and fundament, and for practical action, in the acts of good governing.

I have to make the remark that many Romanian specialists have also dedicated themselves with good scientific and practical results to define concepts, to make an accurate inventory of the critical infrastructures in Romania and to make the political administrative decision makers elaborate a legal framework (laws, Governmental Decisions, etc.), followed by the putting into practice of the main measures, as soon as possible, especially in the case of vital networks (energy, water, informational, transport, financial – banking systems)[5].

---

[1]http://en.wikipedia.org/wiki/critical_infrastructure_protection.
[2]http://www.whitehousegov/news/releases/2001/10/20011016-12.html
[3]Executive Order Critical Infrastructure Protection; http://www.fas.org/irp/offdocs/eo1301.htm
[4]The National Strategy to Secure Cyberspace, February, 2003
[5]Authors and paper works: •Dr. Grigore Alexandrescu, Dr. Gheroghe Văduva – *Infrastructuri critice, pericole, ameninţări la adresa acestora, sisteme de protecţie,* Editura U.N.Ap. Carol I, Bucureşti, 2006; •George Dediu, Alexandru Manafu – *Protecţia infrastructurilor critice – o nouă provocare,* Editura U.N.Ap. Carol I, Bucureşti, 2006; •Dr. Constantin-Gheorghe Balaban – *Infrastructurile critice, un domeniu care se cere investigat*, Revista Geopolitică, Anul VI – nr. 27, pag. 49-55.

Both Romanian and foreign specialists, military and civil, who analyzed the field of critical infrastructures have made special attention to the role and place of the complex informational systems (global, zonal, national, military, special, commercial, private, etc.) in providing the population with a normal life, normal operation of economies, finance – banking systems, of the security and defense and of the political and administrative functioning of a country, alliance or of a political-economic union.

I will further make reference only to the **military and special software systems existing in Romania,** to the aim of having a general idea about them, to their physical and informational protection in case of attacks, major natural calamities or other hazardous situations.

It is necessary to point out that this kind of communication and software systems and networks are being treated by many authors as an **informational war topic[1],** taking place all the times, weather it is peace, crisis or war, having serious effects on their secure operation, a fact that directly dysfunctional operation or total breakdown of other systems (sub systems) for: political and administrative management, national defense, national and population security, economic, finance and banking systems, and those regarding vital units (energy, water, food, etc.).

2. Place and role of military and special communication and software systems within the critical infrastructures framework

a. Military communications systems and software have been and continue to be vital elements in the exercise of command and control at all Army echelons from strategic level to the fighter. Many authors, mostly soldiers, have produced books, studies, tests, projects, books and articles have demonstrated the role and place of such complex C4I systems (+ variants) in a modern war, and shows, in addition to their technical skills real vulnerabilities and operational methods and procedures resulting from modern software war, but also those that are created by major natural disasters, serious accidents, design and implementation errors or human error.

In order to better understand, at the moment, which is the available „**wealth**" of our army which needs to be physically and informational protected against multiple vulnerabilities and threats, we have to remind a few aspects, let's call them theoretical and methodological:

[1]Authors and Works: •Radu Dan Septimiu Popa - *Războiul informaţional şi securitatea naţională*, Ed. Militară, Bucureşti, 2009; •Teodor Frunzeti - *Securitatea naţională şi războiul modern*, Ed. Militară, Bucureşti, 1999; •M. Mureşan, Gh. Văduva – *Războiul viitorului, viitorul războiului*, Editura U.N.Ap. Carol I, Bucureşti, 2006; •Robert H. Anderson – *Physical Vulnerabilities of Critical US Information Systems* (internet, Iaver May 03.pdf); •Adrian V. Gheorghe – *Analiza de risc şi de vulnerabilitate pentru infrastructurile critice ale societăţii informatice – societatea cunoaşterii.*

- **C4I systems (+ variants)** are not regarded as one system but more like a **system of systems** where each system produces and / or consumes services. C4ISR is the integration of a doctrine, procedures, organizational structures, personnel, technical equipment and software, facilities, communications and research to support the commander's ability to perform command and control over the entire range of military operations. C4ISR provides commanders with timely and accurate data and systems for planning, monitoring, management, performance monitoring and reporting operations.

- **Command and control subsystem** consists of facilities, equipment, procedures and personnel essential to a commander in planning, command and control of subordinate forces and received support for the mission.

- **Communications subsystem** is a set of equipment, methods, and procedures and staff (if needed), organized to perform the functions of information transfer. This includes transmission systems, and user switching. It may perform storage and processing functions to support the transfer of information.

- **Computer subsystem (for computers)** is a set of equipment, methods, and procedures and staff (if needed), organized to perform information processing functions. It may transfer information to support the processing functions (e.g. the local computer network);

- **Information System (R)** - equipment, methods, procedures and personnel to carry out product information by collecting, processing, integration, assessment, analysis and interpretation of available information on hostile or potentially hostile forces, current or potential areas for action.

- **ISR - information system** that collects and processes information about threats to making products and the environment during operations, as well as information for identifying, tracking and engaging targets.

- **C4ISR systems architecture** must be approached from three viewpoints *(operational, systems and techniques)* with their relationships. **From an operational point of view**, network architecture refers to the centers, missions and tasks performed, the information conveyed to the mission (type, frequency, tasks and activities supported their nature). **From a systemic point of view,** they are considered: the overall functionality and interconnection services provided to support operational activities through the exchange of information among network centers. **From a technical standpoint,** it is considered the minimum set of rules governing the organization, interactions and interdependencies between parts (elements) system to meet operational requirements. This includes a series of technical standards, implementation routines, selection standards, rules and criteria that can be organized to manage the system or elements of services for a given architecture.

- **The above mentioned systems**, with their duties summarized, are represented on the ground by a series of technical and operational networks and facilities incurred during the period 1990-2010, so as much as possible in difficult economic and political conditions. These infrastructures of paramount importance critical to national defense will be summarized in the next chapter.

b. Special communications and information systems.

Special Telecommunications is a segment of what it is called the state telecommunications for ensuring secure voice and data communications for public authorities of the Romanian State:

- The Romanian Parliament;
- Romanian Presidency;
- The Romanian Government;
- The institutions engaged in defense, national security and public order;
- Central and local government;
- Judicial Authority:
    - Supreme Court Justice;
    - Public Ministry;
    - Superior Council of Magistracy;
- Court of Auditors;
- Constitutional Court;
- Governing bodies within government agencies and nongovernmental organizations of national interest.

These special systems and networks are characterized by national coverage, a high degree of protection and confidentiality and by physical and information measures of protection against various risks and potentially dangerous situations.

The designation **"special telecommunications"** was adopted in 1993 with a view of delimitation these from public or private sphere of telecommunications, as well as in order to customize their status in the field of telecommunications.

Special telecommunications networks particularity is given by the organization of infrastructure and the organization of services. Government telecommunications network system performance has its own separate, if possible, from other networks, with a **high degree of reservation and reconfiguration**, which can perform a wide range of services through the use of the most high-technology networks superior to the majority of private and public networks.

It follows quite clearly that the systems and networks STS (Law no. 92/1996) have a vital role for political leadership, administrative, military, and in some cases – also the country's main economic institutions and in this respect, fully qualify as critical infrastructure to be protected against a full range of risks and threats.

3. Brief Presentation of certain special military communication and software networks and systems as vital part of the critical infrastructures in Romania

3.1. Ministry of National Defense IT&C infrastructure

From 1991 until 2010, the Romanian Army designed, realized and developed a **Permanent Communications Network (PCN)** which is a distributed network, incorporating, in terms of operational and technical communications 253 with different development centers from the nodal main modules deployed to theaters of operations and communications with external extensions to NATO and the EU. This network, the main part of the Romanian Armed Forces Communications System (STAR) provides basic infrastructure (stationary) for multi-channel communications (voice, data, and video) for operational and administrative management of all military structures during periods of peace, crisis and war. It has a national geographical development, being extended in almost all towns of the county and numerous other locations where military units and interests. The role of this **critical infrastructure** networks for the benefit derived from its function of strategic management, operational and tactical information and resources available for inter-category and inter-forces, and also for projects with high military value of defense (e.g. for SCCAN and SCOMAR). In addition to these operational and technical skills and the network has some vulnerabilities in terms of ensuring safe and uninterrupted operation in conditions that could be subject to physical attack or hostile action Radio electronic by known means of information war (with all its assets and liabilities). General and punctual risk analysis may be carried out and concrete measures proposed:

- **Communication Network Support Campaign** (CNSC) provides infrastructure for mobile multi-channel communications, designed to restore some sections RTP destroyed or temporarily decommissioned and / or to expand into areas not yet covered by RTP Control Point.
- **Integrated Services Network Radio** (ISBR) provides communications equipment and procedures for Single Channel HF and VHF radio stations using hopping frequency, encryption devices for voice and data;
- **The encrypted Videoconferencing** (VTC) provides video conferencing services that support encrypted communications using RTP / RMNC. The beneficiaries are the principal structures and leadership of the Ministry of National Defense General Staff;
- **Satellite communication system** (SCS) provides communications support in inaccessible locations, remote or removed (in foreign theaters of operations - Iraq, Afghanistan, etc.).
- **Deployable communications and information system** (DCIS) provides voice and data services for deployable forces in theaters of operations, and connecting them to NATO General Communications System (NGCS).

- Tetra Dimetra mobile communications systems designed to provide mobile communications for some of the central structures and the Ministry of National Defense General Staff, the categories of military forces and operational headquarters and weapons as well as cooperation with the national system of defense structures, particularly in emergency situations, based on provisions of Law no. 363/2004.

All the above mentioned systems and networks are part of the Ministry of National Defense critical infrastructure and consequently, physical and informational measures have to be taken, according to NATO and EU present standards.

3.2. Special communications infrastructure management and cooperation in STS administration

- High Redundant Capacity Telecommunication Infrastructure, existing in the capital and in county residences.

This is based on professional equipment using modern technologies making use of optical fiber and radio relays.

Transport capacities are sufficient for communication between county residences and Bucharest in the upcoming years and cover all the needs expressed by the authorities. This integrated telecommunications infrastructure networks provide communications services for voice, data and video. In a short-term radio relay facilities will be extended for the use of each municipality, city and town having public authority bodies.

- Mobile radio communications infrastructure consists of local conventional professional systems and networks using TETRA-Dimetra TETRAPOL technologies and provides mobility services for public authorities responsible for their citizens' safety and for the national security. Currently, users of TETRA-Dimetra common platform are the Ministry of Administration and Interior (the Romanian Police, the Border Police, General Inspectorate for Emergency Situations, the Romanian Gendarmerie, Prefecture), the Romanian Intelligence Service, Ministry of Health - Emergency Medical Services (ambulance service, SMURD), Ministry of Finance (Customs Authority), municipalities (Community Police), Ministry of National Defense and Protection and Guard Service.

- Infrastructure for data communication services

This integrated high-capacity network infrastructure enables realization of extended area secure national network for the authorities. Major beneficiaries: Ministry of Finance, Ministry of Justice and Civil Liberties, Ministry of Interior, Ministry of National Defense, Ministry of Agriculture and Rural Development, Ministry of Environment, Ministry of Foreign Affairs and Ministry of Labor, Family and Social Welfare. The network is secure and encrypted according to NATO standards.

- Internet Infrastructure Services

Is developed from the express needs of public institutions and components NSDPONS (National System of Defense, Public Order and National Security) by given conditions that Internet services have become a main component of the functioning of all state entities.

- Infrastructure for satellite services

It was developed as alternative to land and infrastructure services to provide communications services for temporary missions in places where terrestrial infrastructure does not provide services. Through this infrastructure is provided operatively telecommunications services for emergency management authorities and wherever the situation requires the presence of intervention forces, and terrestrial network services are not available. Through the satellite infrastructure to ensure continuity of leadership in the state of calamity or disaster situations, in situations where terrestrial networks are no longer functional, as well as during the official activities of the state's leadership abroad needs. Infrastructure is available for emergency use by the components of the public authorities.

- Infrastructure for telephone services include telephone switches and telephone cords network, offering special "S" and "TO" telephone services and also IC cooperation services.

Issues that require special attention are those involving the infrastructure technologies resulting from the change in operators' access networks that provide related services to ensure protection of public communications in this environment, and the high costs of this type.

- Video services infrastructure works on the infrastructure of integrated communications and provide secure video conferencing for the Romanian Government and Prefectures.

- TESTA Infrastructure was developed as a result of Decision no. 387/2004 of the European Commission as a network to support projects of common interest and offer a protected and reliable communications platform for data exchange between European public administrations.

- Public Key Infrastructure (PKI) undertaken by STS is directed SNAOPSN components and public authorities.

- Special protection telecommunications infrastructure provides protection for telecommunications services and special security cooperation by:

☐ Finding, identifying, locating and removing sources of accidental disturbance (analysis of interference problems) or intentional (unauthorized emissions) and ensure availability of radio spectrum management STS.

☐ Execution of engineering controls special telecommunications networks to ensure confidentiality of special communications.

☐ Zoning locations to prevent leaks of classified state secrets compromising electromagnetic radiation emitted by the equipment STS.

- The single national emergency number - 112 extended to all municipalities and cities in Romania.

All these systems require a thorough analysis process of their physical and information vulnerability in order to identify effective measures of protection.

4. Physical protection of special military communication and software networks and systems in the event of war situation, occurrence of natural disasters and other negative phenomena.

Vulnerabilities and threats to national information security:

☐ As in any field, in the information systems for national security field, there are also certain vulnerabilities, i.e. less studied aspects and weaknesses of the system, infrastructure, environmental control or design of networks which are not caused by enemy actions but by nationally adopted solutions that can be attacked and exploited relatively easy to damage the integrity of the State.

☐ Software vulnerabilities are a component of the **security vulnerability**[1] caused by the state of affairs, processes or phenomena in the internal life of national community, which diminishes the society's reaction capacity against an existing or potential risk of any kind, including information, enabling their occurrence and development, affecting the realization of national security.

In general, information vulnerabilities are even greater, as information networks and information structures are more complex, being difficult to optimize, manage and protect. Equally, vulnerabilities increase in direct proportion to the technology implemented in their construction and operation equipment (especially digital) of software systems. It follows that the main aim of contemporary military conflicts should not consist, mainly, in the total destruction of equipment, weapons or force the opponent alive, but especially in neutralization and decay of its complex systems, mainly the software systems. In this context, the concept of the **country critical infrastructure** has become increasingly important because of the country's stability, safety and security systems and processes depend on it[2]. However, it is not mandatory that all the existing infrastructures or that can become critical at a certain point in time to be part of this category of infrastructure. Critical infrastructures are those facilities

[1]Doctrina naţională a informaţiilor pentru securitate (*National doctrine of security information)*, Editura SRI, Bucureşti, 2004.
[2]Gr. Alexandrescu, Gh. Văduva, *Infrastructuri critice. Pericole, ameninţări la adresa acestora. Sisteme de protecţie*. Editura UNAp, Bucureşti, 2006.

with an important role in ensuring security in the functioning and development of economic, social, political, informational and military systems.

The critical character of infrastructure, mainly of the information infrastructure is determined, especially, by the uniqueness of a system or process, by its role in the stability of operation of infrastructure and its vulnerabilities.

National security, defense and public order are important areas of critical infrastructure and its vulnerability where there to be found the structures related to information technology and communication networks of governmental, diplomatic networks, energy, transport, water supply, the financial and medical systems.

The main vulnerabilities of information infrastructures concerning national security, we appreciate that are the following:

- Possibility of interception of information from telecommunications network and computers used both by users and their opponents;

- Large volume of information produced, used and processed within the information systems, which may be subject to the attack or research of the existing or potential opponents, destroyed, counterfeit or stolen;

- Information infrastructure damage, which causes difficulties in its management, taxation, impossibility to detect fraudulent access to information and promoting cyber-attacks;

- Use of the same frequency bands and modulation schemes based on work equipment electromagnetic wave propagation, both in their own communications networks as well as those of potential adversaries;

- The use of machinery, components, and software database structures and standard operating (commercial) in all computer networks of organizations involved in national security and possibly their communications networks, enabling terrorist activities and organized crime in our country;

- Dependence informational infrastructure systems for national security infrastructure information of the country's trade, which creates a fraudulent access and misinformation;

- Can be incorporated (hide) the time, computers and communications equipment, the companies supplying equipment to software modules that can be activated by opponents at times determined by them, creating disorder and chaos in decision-making and information networks;

- By connecting to the Internet, Intranet or Extranet, which depends on national security organizations are vulnerable to unauthorized intrusion (maliciously or inadvertently);

- The existence of information networks with large numbers of nodes and wide interconnectivity, hard synchronization and managed, allowing penetration of unauthorized access, fully physical capture of some equipment or nodes (centers) communications, interception or interruption of important information flows and/or entry of false information to affect decision-making processes;

- Comprehensive digitization of national security information structure has a contradictory impact: on the one hand mix, synchronize and increases the degree of compatibility and interoperability of networks, of informational national security system, and on the other hand determines difficulty in managing the complexity and particularly high level of technicality of these, providing conditions for remote or internal cyber-attacks.

- Failure to follow the requirements and standards of the European Union and NATO compatibility and interoperability of information systems, especially in terms of information exchange (message format), access to databases, automatic encryption of communications and link-channels features;

- The possibility of using the electronic warfare against potential adversaries means radio electronics of the major information and communication systems, especially on the channel which connects the central source of information fusion and data processing;

- The interception of radio-communications by the enemy (hostile forces), timely their decryption - if unsatisfying cryptographer-systems were used - and using of this information for their own, to obtain informational superiority on the Romanian state;

- Current technical means informational systems have ensured full protection against physical, electromagnetic and cyberspace attacks, they can be destroyed, damaged or extracted information stored;

- Ordering the wrong place, in terms of functional and physical security and technical electromagnetic equipment information systems, mainly the means of communication and software, increases information interception vulnerability and physical attack;

- Use for the operation of information concerning national security of persons insufficiently checked and unfair, likely to be recruited by potential adversaries and determined to perform their sabotage or to provide information obtained fraudulently;

- Neutralizing shortwave radio link, especially at large distances, based on electromagnetic wave propagation through the ionosphere by changing its electrical characteristics, resulting in attenuation, random changes of direction of propagation and partial electromagnetic waves propagation;

- Existence at potential opponents, the electronic radiation weapons infra acoustic based on subsonic wave propagation in space, acting on personnel recruitment, leading to its inactivation periods some time and hence interruption of information systems;

- Means of communication antennas installed in the open or in buildings without natural protective properties, allowing their easy removal from office-stop operation and liaison, especially the one with radio stations and high power radio relay;

- Removal of Internet access information systems for national security isolating them to prevent the use of their documentation sources, including unclassified data by unauthorized persons, and opponents;

- Use of the Internet for terrorist[1] disinformation and cyber attack on critical information infrastructure of national security;

- Inappropriate design of infrastructure, with reduced redundant information, excessively centralized having low possibilities of replicating the existing information in databases;

- Insufficient concern for hiding and concealing elements of information infrastructures, inadequate security and protection measures;

The presentation made clear that there are numerous vulnerabilities, however the essential ones are the following: an optimum organization of information systems, choosing technical equipment and commercial software products with high performance, realization of qualitative implementation of (software) programs and applications of data sources by experts of organizations specialized on national security and safe automated, encryption of information systems and adopted security measures adopted.

Optimal organization of information systems represents a fundamental prerequisite for information efficient operation in wartime and their real-time reconfiguration, mobility and adaptability to revolving information environment and standard situations, as European Union and NATO member state, must be fully respected and vigorously applied to meet the conditions of compatibility and interoperability.

The standard format of documents bearing information must be unified with the European Union and NATO, and their completion has to be carried out both in Romanian and in English or French.

[1]Contemporary terrorism has already got a global character. It is based on religious, violent extremism, political extremism and on the effects of derooting [Vasile Marin, Elemente de analiză geopolitică a ordinii internaţionale contemporane (*Elements of geopolitical analysis of international contemporary order*), Bucharest, 2003].

Information systems adjusting to the environment, especially in situations of crisis and military conflict, imposes their being equipped with technical information streams capable of handling information flux which is 2-3 times higher than in normal peacetime operation. Reliability of information systems must be designed so that the probability of functioning without fault information and technical structures to be greater than 0.95, while ensuring a low probability of detection and interception of communications. Particular attention will be given to the organization and optimal use of computer networks database.

Internal information threats

The analysis carried out highlights the following internal factors, which may become threats against national security information system:

- Lack of concern for acquiring superiority of information on potentially hostile states and forces;

- Discrepancy between the information requirements for decision making and management actions on national security and the real possibilities;

- Design, organization, or improper operation of corresponding information systems;

- Acquisition of inappropriate data collection systems, communications and computers, difficult to exploit and protect;

- The influence of domestic and international environment on information processes of the state's specialized data structures and their cooperation with similar bodies in other European Union and NATO countries;

- Improper organization of database, the presence of some unsatisfying software products or with intentional errors for bad management, processing and display information, lack of concern for the use of artificial intelligence to carry out the information and management activities;

- Poor training and limited experience of staff involved in the organization, operation and insurance information systems;

- Improper classification of the categories of information and data regarding on national security and erroneous certification of the personnel’s right to access them.

- Disloyalty to equipment disposal of persons operating technical information systems;

- Reduced security of data and information during transmission, memorizing, processing and display, the unauthorized access of foreigners or nationals.

Responsibility for ensuring information superiority over potential adversaries and other hostile forces it must be pursued consistently both in peacetime and in times of crisis or military conflict.

Fragility of information superiority is the high-quality information to be obtained in real time, with the forces and means specialized information structures up and open sources or from their cooperating with them. Nonlinear nature of its low input causes the information to be able disproportionate effect in times of peace or crisis, especially during the military conflict.

An important role in peacetime is to establish, through laws and instructions, the requirements of national security information, differentiated active areas of health and hierarchical echelons of management, procedures and responsibilities for achieving them and their contents informational presentation and processing operations to which they are subjected. In this regard, it has to be born in mind that badly implemented modern information and communication technology and modern management methods shall constitute an essential component of the definition of force.

Experience on national security has proved that failure of information systems, lack of concern for their operation and removing defects that may occur represent the main cause of lack of relevant information and of impossibility of acquiring informational superiority. It is also important to bear in mind that informatics and modern communication, although they play a crucial role, present a number of technological vulnerabilities that have to be diminished or reduced using adequate organizational and technological measures.

Even if they are not exposed to potential opponents' informational attack, databases and software can create serious problems in situations when they are not properly organized and run. The main responsibility for their efficient operation lies with specialists in the informational systems, especially with engineers, analysts and programmers, equally to communication operators. Related to this, a major impact on information is realization of a reduced security of information at all stages of informational systems, thus creating the possibility of unauthorized access and data transmission to the opponent, because of the lack of loyalty of certain members of staff involved in the information flow.

At the same time, there are technical motives which can be external international threats, as a consequence of improper endowment with modern data collecting, transmission and information analyses equipment, as well as of some spare lots for these.

In conclusion, it is imperiously necessary to allocate important funding for equipping the information systems with modern technology, because the success in realization of national security can be obtained at high cost.

External Information Threats

External information threats consist in the assembly of specific action carried out by potential opponents and hostile forces for our country to forbid or make difficult the execution of decision making or operational processes regarding national security. These aim at limiting or excluding data collection, deteriorating or breaking down sensors or other data sources and preventing informational operating concerning national security. According to the conclusions drawn in the field literature[1], the main external information threats against decision making and operation regarding national security are the following structures:

- Physical attack against data sources and information transmission, analysis and display;
- Electronic attack against means for data collection, information transmission and analyses;
- Cybernetic attack against software systems of informational structures for national security and for the security of economic, financial, diplomatic structures, etc.;
- Software pirating;
- Physical and electronic attack against our state decision-making institutions (president, parliament, govern etc.) regarding national security;
- Psychological attack against all decision making and operational (political, economic, social, defense, etc.) structures in our country.

These threats are not new, they are generated by the evolution of the informational society, but they have to be known, carefully studied and adequate measures should be taken for their counteraction.

It is known that the object of data collection for national security consists in providing exact knowledge of the international situation, especially in a zone of interest of Romania, European Union and NATO, as well as the internal situation in our country and neighbor countries, thus realizing an anticipation of aggressive actions of potential opponents or hostile groups and preventative action.

At present[2] security is identified with the protection of everything that affects the basis of the state and international organizations we joined and with whom we have joint actions. This evolution has also changed the objectives of intelligence services which do not focus so much on information on military and strategic parameters, but mainly on aspects and economic, social, and political phenomena whose logic of action responds to certain models and different conditions and especially, more unpredictable than in the past.

---

[1]J. S. Gansler, H. Binnendjic, *Information Assurance, Trend in Vulnerabilities, Threat and Technologies*.

[2]Doctrina naţională a informaţiilor pentru securitate *(National doctrine of security information)*, Editura SRI, Bucharest, 2004.

It is proved that the existence of certain, full and useful information is the main support of management and coherence of decision making process on national security. That is why, physical attack of potential opponents and hostile groups against sources and means of obtaining information is, probably, the main vulnerability for informational systems of any nature in our country.

Electronic attack against the means for information collecting, transmitting and analysis is based on the use of high electromagnetic energies (lasers, radio band weapons, microwave weapons etc.) to neutralize or destroy the electronic devices (radars, sensors, radio stations, radio relays, computers etc.) used in informational systems and in biological attacks against members of staff.

We appreciate that this attack represents the main physical threat against the existing technical means and information systems of information structures regarding national security. Protection against these weapons attacking technical equipment and members of staff working in informational systems, have an outstanding decision role for the continuous operation of electronic devices used for information collection, transmission analysis and dissemination.

Cybernetic attack against information structure of national security represents an extremely important threat, aiming at the „virtual space" especially software and firmware products, protocols and databases of software systems used in computer and communication networks. The external actions specific to cyber-attacks aim at significantly reducing the possibilities to correctly use of services within the software system, software deterioration from its applications having a confidential or secret character in order to generate wrong information from the processed data.

These external threats are enabled by lack of implementation safe protection and securing rules for information during their transmission and processing of data collected by sources. They fructify gaps and/or weaknesses existing in the structure of our own communications and computers networks security system.

Cybernetic attacks are linked with software piracy[1], which can be done by local hackers or placed in any point of the interconnected space of information and aim at, depending on case, the complete paralysis of software systems or their intermittent decay, at moments established beforehand.

Cybernetic attacks are also targeting expert systems decay used in decision making and operating processes concerning national security, which is way beyond the information sphere in itself and can generate wrong decisions which will, one way or another, work in the advantage of the potential opponents.

[1]J. S. Gansler, H. Binnendjic, Infromation Assurance, Trend in Vulnerabilities, Threat and Technologies.

The attack directed against the leading capacity of central and local bodies in this country aim at neutering decision making systems, personnel and techniques, as well as the subordinated operational command structures, in order to paralyze the activities regarding national security (citizens' security, public order, defense, emergency situations, etc.) of economic, financial, social, etc. It is targeting physical and intellectual capacities of the leaders, public servants from central and local administration, staff in the public order, defense, and emergency situation interventions.

As action method, potential opponents or hostile groups can use abduction of one of the leaders, members of the parliament, highly ranked officers, etc. In order to disorganize various fields of activity and/or the attack against for influencing biophysical condition of the entire personnel to temporarily or permanently remove them from their activities.

This threat is enhanced by psychological attack, which is based on the use of information against human mind, to modify or cancel perceptions, attitudes or human behavior. Consequently, it is possible to trigger human errors in decision making or command – control processes, diminishing the managing capacity of the state and various fields of activity.

For connecting the state central bodies to those belonging to the European Union, NATO and other international bodies as well as for diplomatic connections, etc, an important role is played by low wave radio which can be neutered by changing the electric characteristics of ionosphere.

Existence of information security systems and communications concerning national security information systems of radar, radio and radio relay stations operating with high energy spectrum energy and using high gain antennae may represent an important risk for operational staff and some categories of electronic equipment, mainly computers, their composition. It follows that information structures on the state security, may have some vulnerabilities that can be exploited by adversaries or hostile groups, but also by ill-intentioned people from inside. Knowing the information vulnerabilities and threats allows taking severe measures, technical and organizational, for their reducing or complete removal.

Special military systems and networks protection

Protection of information systems refers to taking special defense measures to protect data transmitted through those, through data processing automatic systems, system and application as well as communication systems.

Five patrimony values of information systems (equipment, software, materials, data, and services) can represent a target for the following threats: losing, rejection (not recognizing), compromising and corruption.

Informational system security for national security depends on its dynamics and threats against it are directed against organizational structures, equipment, program application and operational system, materials used in the computer networks, memorized information on various magnetic supports, valuable papers existing in the system or services delivered by components.

Enumeration of the main protection measures[1] for information systems is presented in the figure of next page.

In general[2], threats regarding security of information systems and information circulated through those can be grouped as follows:

- Loss of equipment or physical components;
- Rejection of services;
- Unauthorized use of equipment;
- Accessing classified information;
- Unauthorized modification of information;
- Loss of information;
- Unauthorized use of information;
- Unauthorized finding of secrets regarding software products used;
- Unauthorized modification of users programs;
- Loss or unauthorized use of software products.

The information systems perimeter, where classified information is stored and transmitted, has to be zoned, in principle there are three security zones, namely: class I, class II and administrative zone.

Strict registration and continuous, uninterrupted of classified documents and authorized personnel who had access to those will be organized, to avoid accidental or intended deterioration of information.

Preoccupation for protection of classified information in software systems have increased considerably with the switch to automatic data processing[1], because:

- information density is much greater than in classic systems based on paper work, and the present magnetic supports (especially memory sticks) having capacities of tens of gigabytes can memorize large quantities of information which can be stolen quite easily;

- Transparency of documents disappears;

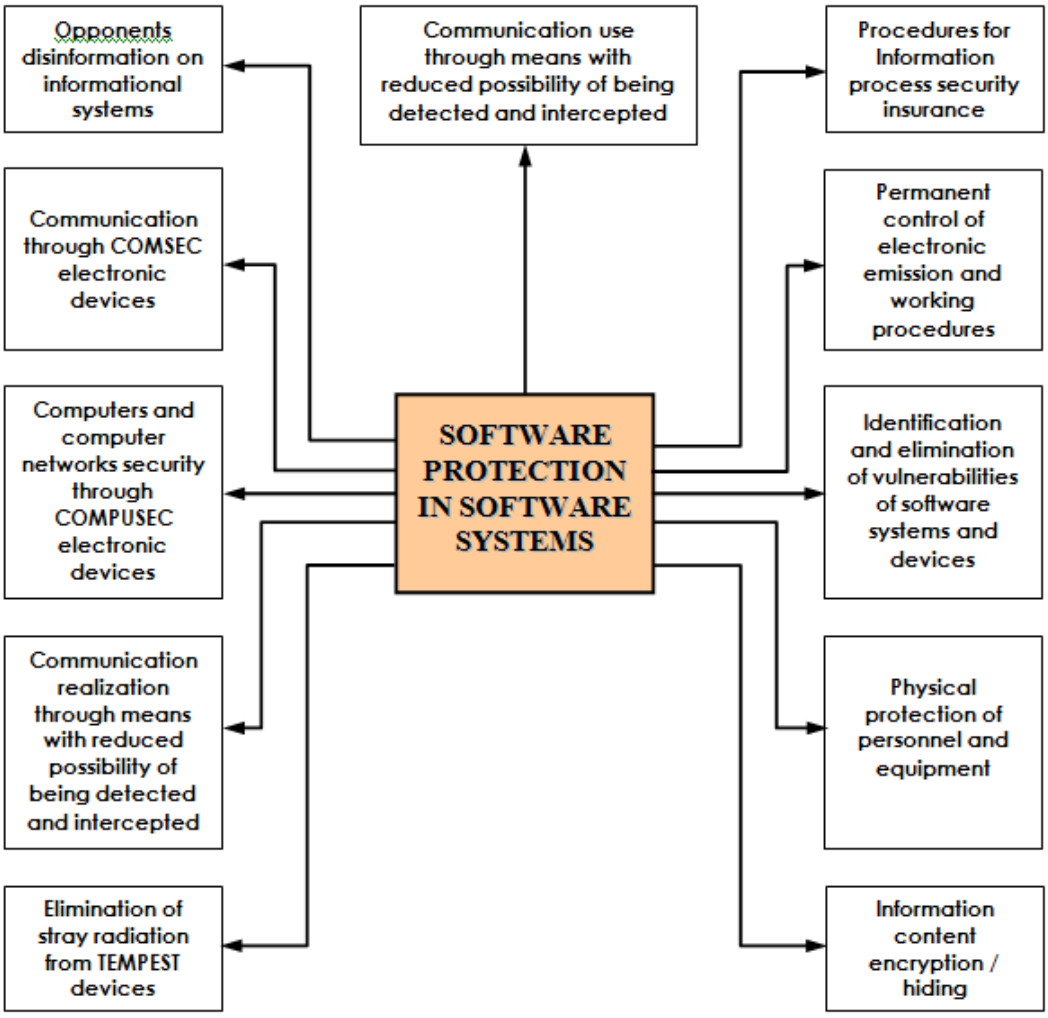
- accessing data in modern computer systems can be carried out with great easiness through unauthorized access of external or internal personnel regarding national security issues;

[1]Information Protection Capabilities, Joint Doctrine Encyclopedia, US Army, 1997.
[2]D. Oprea, op. cit. p. 38.

- Potential cybernetic attacks on computer systems storing information are difficult to be detected;

- Magnetic support persistence after having been removed can be a sure way to restore previously recorded information;

- Existence in computer memories of aggregated information with high decision making value allows obtaining of data that can be used directly or indirectly by the opponents for criminal activities;



- computer and communication networks have become more and more performing, but they also present significant vulnerabilities, enabling information attacks against them to be carried out mainly through cyber-attacks from anywhere in the world;

- existing security standards for information in software systems do not provide secure protection of those and require large expenses and highly qualified specialists, measures difficult to realize.

Protective mechanisms for information systems should be as simple as possible, easy to use, to provide a minimum number of errors or false alarms and to prove completeness, characterized by normal operation of any and fairness, anti-collated by providing answers to the registration of fraudulent intent. The protection mechanism should have a longer period to ensure permanent survival and determinate a level of protection. You also need to provide solutions to normal operating of technologies information system equipment when electric power cut their communications due to system failure and sudden temperature changes.

We appreciate that protecting the information system components of national security against information attacks identified earlier, especially against the electronic and cyber-attacks, it is supposed to be the main concern of all specialists in the fields of information, communications and informatics, as a globalization of threats and can produce disastrous effects, seriously affecting national security.

Therefore, the design of national security information systems must consider all technical means and their three main components, namely:

- Information collecting subsystem;
- Communication subsystems;
- Computer network (informatics) subsystems.

The information collecting subsystem is the one giving the significance and importance of informational systems, as they provide the raw material (information and data) regarding national security.

Modern technical means used for collecting information are numerous and are based on the use of the highest technology resulted from the symbioses between electronics, modern communication and informatics.

Consequently, they present certain vulnerabilities that can be exploited within the information war of potential (real) opponents, through their physical, electromagnetic or cybernetic attack.

Removal of some of those can cause interruption of some information flows, as a result of prevention of operation of sources information, namely of sensors, listening and monitoring means, goniometric and imaging equipment, etc.

The main means of protection of those lies in their continuous and interrupted guarding and defense as well as equipment display in protected areas (spaces) against electromagnetic impulses and high power energies.

Protection against interception of stray radiations

Radiation (programs) are formed from signals unintentionally compromising that, if intercepted and analyzed, provide disclosure of the information sent, received, processing or other operations under equipment communications and computing systems. The study said the area is known as TEMPEST (Transient Electro Magnetic Pulse Emanation Standardizing), which defines all investigations, studies and control of compromising radiation of electronic equipment.

Protection[1] against interception and analysis of stray radiation during their operation is achieved by:

- The reduction of parasitic radiation to the levels required by professional standards and rules;

- Limiting access to authorized personnel in the districts of installing communications and computing equipment and disposal of any devices capable of recording and retransmission of stray radiations at enemies' convenient distances;

- Continuous measurement of spurious radiation level in the working ranges of communications equipment and organizational and technical measures to eliminate or severely reduce their opportunities to be intercepted;

- Thorough training of operating personnel on protection measures of communications and computing equipment.

Physical protection of personnel and technical equipment

Physical protection is an important component of management information system and is realized by human and/or electronic monitoring of protected area, use of barriers and standardized procedures, control keys, access specialized documents, lighting and other solutions that prohibit unauthorized access.

In general, physical protection must provide:

- Security of personnel and strict delimitation of access to communications and computer equipment;
- Protection against espionage, sabotage, damage and theft;
- Reducing exposure to threats that can cause denial of service or unauthorized alteration of information;
- Continuous monitoring and surveillance of equipment and places of work of the staff (video monitoring);
- Re-encryption key after each switch off of cryptographic equipment;
- Providing security and defense unbroken key points of communication systems and computer networks.

[1]AR 381-14(S), Technical Surveillance Countermeasures and TEMPEST, SUA, 1998.

Security, in terms of staff should consider the following activities:

- selection;
- through the security check;
- continuous surveillance;
- training and awareness.

It follows that the protection of information and national security information systems against potential enemy offensive information operations is a defensive measure is absolutely necessary in all situations.

5. Conclusions and suggestions

From the theoretic approach of the problem regarding the information war from a doctrine and operational point of view, according to the vision of the North-Atlantic Alliance and implicitly to the conception of transforming the Romanian Army, as well as that regarding the information security of national security, result, obviously, a number of conclusions, their essentiality enabling us to appreciate the following:

- information is, without any doubt, an essential element of the factor of power, regardless the manifesting domain, however its possession is not sufficient, its wise use confirm, in fact, the efficiency and power of the information user;

- in the extremely alert of the new information revolution, practically determining the unlimited liberty of knowledge in the geopolitics of globalization, the informational war represents the component or, depending on the situation, the dominant element of any confrontation, regardless the domain where it operates: social, military, economic, physical etc.;

- in the present context of global information, but also of a fierce competition taking place at the level of all subsystems of the global social system, including, of course, the military one, informational war is equally, omnipresent, unavoidable and continuous;

- the organic scope of the informational war, in any of its forms it can be carried out, operational offensive or defensive, consists in acquiring informational superiority, with consequences in affirming superiority/victory in the field where it is sub summed up, in our case, the one regarding national security;

- practical impossibility to limit it in any ways, in point of area of manifestation, space or aimed objectives, regardless the domain where it operates or where it is used, confers the informational war the spatial attributes of globalization, enabling us to consider that, quite rightly, that it is both a vector and its consequences;

- as far as armies and the used techniques in the information war, they do not have an immutable character, beyond those already consecrated, as being possible

under unpredictable circumstances, the occurrence of „weapons", instruments and techniques unknown yet by the carrying out of informational war, including by the use of new principles in physics:

- from the perspective of postmodern technical achievements, the information war highlights both the uncontestable virtues of the informational revolution but also its limits in the context of contests that equally express it;

- the informational war and information, in the cognitive sense of human practice, are some of the most influential vectors of the new revolution in military affairs;

- in providing information security in national security, information resources play a crucial role, their quality and opportunity highlighting the capacity of intelligence structures in the country, as well as the level of institutional adjusting to the applied rigors of the informational revolution;

- the content of information feeding the complex affirmation of national security is extremely heterogeneous, practically undefined and without doctrine principles, a reason for which, from the perspective of systemic coagulation of this problem, we appreciate that it is useful to proceed to their systematization based on coherent criteria;

- national security efficient provision with information depends, decisively, on the decision making capabilities of the institutional structures assigned with such responsibilities;

- informational explosion, without precedent, as breadth and scope, in the history of humankind, makes it difficult to obtain the useful content of information designated to ensure national security, a reality that imposes the educated users of acquired information, a totally professional decision making process;

Based on the conclusions formulated as a result of a multilateral study of the specialized literature we consider that we may formulate the following suggestions:

- Breakdown of informational war concept, in the acceptance of its use to provide national security, depending on the three major situations where it can be used: peace, in situations of crises in case of war;

- The systemic study of content providing information for national security, taking into consideration all the fields contributing to these and of the information necessities, command and control, as well as the protection measures of communication measures of communication networks and related computers;

- Including of information security amongst national priorities;

- The problem of informational war should become compulsory subject in all education structures responsible for national security;

- Measures regarding country preparedness for defense (exercises, applications, etc.) should include the discovering and counteracting activities of informational threats involving national security;

- Advanced study of NATO norms and instructions on informational war by all the structures having responsibilities in national security in their concerned departments;

- Training of staff working in IT using computer networks of the structures in the national security system for the prevention and termination of cyber-attacks;

- Policy and operational correlation of the information war, as form of the armed war, with the main fighting forms used nowadays, but also with the laws and principles of armed fight, taking also into account the possibility of its independent use;

- Protection against informational threats should constitute a continuous preoccupation of all the structures with responsibilities in national security, but also of other organizations, both in times of peace and especially in times of crisis and military conflict;

- Procurement and endowment with modern means of defensive but also offensive information war of the main state structures responsible for national security

R E F E R E N C E S

[1] *** *Doctrina naţională a informaţiilor pentru securitate (National doctrine of security information*), Editura SRI, Bucharest, 2004.

[2] *** *Doctrina pentru informaţii, contrainformaţii şi securitate a armatei (Doctrine for information, counter intelligence and army security*), Bucharest, 2005.

[3] *** *Legea privind protecţia informaţiilor clasificate (Law of classified information*), issue 182/2002, published in O.M. issue 248/2002.

[4] *** *Legea privind securitatea naţională a României nr. 51/1991 (Law regarding Romania's national security issue 51/1991*), published in O.M. issue 163/1991.

[5] *** *Securitatea informaţiilor (Information Security*), Center of Expertise in the field of Security, 2008.

[6] *** *Sisteme informaţionale (Informational Systems*) – Annual Session of Scientific Communications with international participation, Editura UNAp, Bucharest, 2007.

[7] *** *Strategia de securitate naţională a României (Romania's national security strategy*), Bucharest, 2007.

[8] Alexandrescu C. and others - *Supremaţia electromagnetică (Electromagnetic Supremacy*), Editura UNAp, Bucharest, 1999.

[9] Alexandrescu C. - *Ameninţări informaţionale asupra sistemelor de comandă şi control în acţiunile militare moderne "SI-2007" (Informational threats against command and control systems in moderrn military operations "SI-2007*").

[10] Alexandrescu C., Teodorescu C., *Războiul electronic contemporan (Contemporary electronic war*), Editura Sylvi, 1999

[11] Alexandrescu Gr., Văduva Gh., *Infrastructuri critice: Pericole, ameninţări la adresa acestora: Sisiteme de protecţie (Critical Infrastructures: Hazards and Threats against them: Protection systems*), Editura UNAp, Bucharest, 2006.

[12] Bădălan Eugen, *Securitatea României, actualitate şi perspective (Romania's security, present and perspectives*), Editura Militară, Bucharest, 2001.

[13] Constantin Alexandrescu, Decebal Ilina, Constantin Mincu - *Bazele matematice ale organizării sistemelor de transmisiuni (Mathematic basis of transmission systems organization*), Ed. Militară, Bucharest, 1994.

[14] Dr. Constantin Mincu, Dr. Gruia Timofte - *Compatibilitatea Sistemelor Radioelectronice (Compatibility of radioelectronic systems*), Ed. Olimp, Bucureşti, 1999

[15] Dr. Constantin Mincu, dr. Victor Greu, Ing. Costel Rotariu - *Salt de frecvenţă şi contrasalt de frecvenţă (Frequancy hopping and frequency counter hoping)*, Ed. Militară, Bucharest, 1998.

[16] *ENSA Risk Management / Risk Assesment* (European Network and Software Security Agency).

[17] *EUROCOM D/1* Tactical Communications Systems. Basic Parametersm 1986.

[18] *FM 3-13 software Operations: Doctrine, Tactics, Techniques and Procedures*, US Army, 2003.

[19] *FM 34-1 Intelligence and Electronic Warfare Operations*, Headquarters Department of the Army, Washington DC.

[20] Frunzeti Teodor - *Securitatea naţională şi războiul modern (National Security and Modern War)*, Editura Militară, Bucharest, 1999.

[21] Hlihor C. - *Geopolitica şi geostrategia în analiza relaţiilor internaţionale contemporane (Geopolitics and geostrategy in the analysis of contemporary international relations)*, Editura UNAp, Bucharest, 2005.

[22] Ilie Gh., Stoian I., Ciobanu V. - *Securitatea informaţiilor (Information Security)*, Editura Militară, Bucharest, 1996.

[23] *ISO/IEC 27001 Software Technology. Security Technique*. Software Security Management Systems – Requirements.

[24] Mureşan M., Văduva Gh. - *Războiul viitorului, viitorul războiului (The War of the Future, the Future of the War)*, Editura UNAp, Bucharest, 2005.

[25] Robert H. Anderson – *Physical Vulnerabilities of Critical US SoftwareSystems* (internet, Iaver May 03.pdf).

[26] Toffler Alvin, Toffler Heidi - *Război şi anti-război (War and Anti-War),* Editura Antet, Bucharest, 1995.

[27] Toffler Alvin - *Puterea în acţiune (Powershift)*, Editura Antet, Bucharest, 1995.

Magazines

[28] *Gândirea Militară Românească (The Military Romanian Thinking),* Years 2001-2010.

[29] *Buletinul Universităţii Naţionale de Apărare "Carol I" ("Carol I" National Defense University Bulletin),* 2008-2010.

[30] *Revista Forţelor Terestre (Terrestrial Forces Magazine)*, years 2005-2010.

[31] *Impact Strategic (Strategic Impact),* years 2006-2010.

[32] *Revista de ştiinţe militare (The Military Sciences Magazine*), years 2006 – 2009.

[33] *Romanian Military Thinking Journa*l, years 2005 – 2010.