TWENTY YEARS LATER. NOTABLE ACHIEVEMENTS AND ABANDONED AND POSTPONED PROJECTS IN THE FIELD OF COMMUNICATION AND INFORMATICS SYSTEMS OF ROMANIAN ARMED FORCES (1997-2017)

Major General (ret.) Associate Professor Constantin MINCU, Ph.D.[*]

Abstract: *The author briefly presents a series of recent aspects in the current geopolitical context on some strong points as well as internal vulnerabilities and external threats of the military communication and informatics systems and networks developed in the Romanian Armed Forces since 1997. The article exposes the evolutions in conditions of austerity and even hostility of the main operational and technical sequels of the Romanian Armed Forces Signal System - STAR (RTP/RMNC), as well the influences of new technologies in the C4I systems on the planning and conduct of operations (battle). Furthermore it presents some strong points of the achieved systems and principles taken into account in the modernization and transformation effort (regarding the NATO criteria and requirements), as well as their internal vulnerabilities and external threats identified after a thorough analysis. Unfortunately, we can see the projects have remained abandoned or postponed because of different reasons.*

Key words: *communications, RTP/RMNC, STAR, NATO.*

1. Introduction

We consider, on the grounds of a complex set of arguments at the hand of current civilian and military decision-makers from the Romanian

[*] Academy of Romanian Scientists, member of Honorary Council of Academy of Romanian Scientists, Scientific Secretary of Military Sciences Section, E-mail: mincu_constantin@yahoo.com.

Ministry of Defense that a critical revision of achievements and failures in the field of communications and information systems (CIS) over the last twenty years is of utmost relevance and usefulness in today's geopolitical global and areal context.

It is necessary to attentively observe and take act of the fact that in the areas of technical systems for command and control of forces and their use in real or almost real-time, the role of C4I systems increased exponentially due to some technological and operational progress made in the latest years in certain important armed forces of NATO and non-NATO countries, among which we can mention:

- Rapid technological developments in the production of communication and informatics equipment;
- Amazing growth of computers' performances, in the late 25-30 years;
- The development of microprocessors' performances[1] as basic element for operation speed and for decreasing efforts;
- Conceptual, technological and operational unity of equipment and digital communication networks with electronic computing and software applications;
- Increasing pressure on military command and control structures for the continuous shortening of operational conduct cycle and for the correct and rapid performance of a multi-criteria analysis of a huge volume of data needed for planning and conduct of operation;
- Perfecting optical-electronic sensors integrated in all the systems and platforms of weapons and equipment;
- Emergence and development of digital maps and their integration in GPS systems;
- Conceptual and acting emergence and development of "info-war", which nowadays has increasingly violent manifestations;
- Elaboration of new concepts on waging war, such as: "network based warfare", "asymmetric military conflicts", "cyber-war", "fight against terrorism", "hybrid warfare", etc.

[1] http://wikipedia.org/wiki/central_processing_unit

For all the aforementioned issues, developments and comparative analyses can be performed, including one between some systems in the modern armed forces and in the Romanian Armed Forces, with clear conclusions on the steps to follow if there is the necessary political and institutional will and if human and financial resources are allotted.

2. Some influences of the new scientific and technological developments on the communication and informatics systems and equipment with direct effects in planning and conducting modern military actions

Specialists and analysts in the military field[2] unanimously consider that the unprecedented development of techniques and technologies, the emergence of new products and services with accelerated development – we particularly refer to information technology, special technologies, digital communication systems, software applications designed for planning and conducting operations (battles), as well to the technologies implemented in weapon systems – have a major impact on all categories of forces, weapons, armaments systems and implicitly on the intended results of actions in crisis and war situations.

It is understandable that we will not be able – given the limited amount of space reserved – to identify and present all the possible influences (there are many and in permanent development). We will try to bring to the attention of the interested parties just a few of them which we consider to be more important and visible today.

Thus, in the field of military and civilian human resources and the performances expected from the military systems there can be identified:

•New and difficult requirements in professional, psychological training and in the development of moral qualities to be able to confront some increasingly complex and hard to manage systems;

•The need for everybody from the General to the soldier to understand the new “tools” of information age in all their technical and

[2] *Papers of Jubilee Symposium AFCEA,* Washington DC, June 18-19, 2006, with the interventions of: Admiral Edmund P. Giambastini Jr., Vice-president (on that date) of the Joint US Army Staff and General (Ret.) Colin L. Powell (former State Secretary).

operational complexity, in order to use them normally, naturally, without gaps caused by the technological stress (for all the combatants, no matter their position, rank, or category of armed forces);

•Just appreciation of C4ISR systems; limits (+ variables) under the conditions of a rough cyber warfare, led with all modern means. Therefore, the militaries should remain capable to act in need without these means, which can end up in congestion or collapse (this is understandable even in the most technologized armed forces, as those of the US);

•Testing, during exercises, under conditions as close as possible to realities of the modern battlefield, of the manner of relationship of fighters with systems of complex weapons assisted by computers or included in C4ISR-type of technical and operational systems;

•Specific training and taking necessary measures to protect fighters from the psychological war actions used by the enemy in peacetime, crisis and war situations.

In exercising command and control from the strategic level to the individual soldier, there are the following needs:

•Increasing the capacity of commanders, staff officers and combatants to know the enemy and his intentions in real (quasi-real) time by using the C4ISR system possibilities (where they exist);

•Rapid, multi-criteria analysis of complex situations by using computers and specific software programs and, by this, shortening the time allotted to all the commander and staff activities (conduct cycle);

•Detailed storage of data and information about all the aspects of operation (fight) in their chronology and depicting by analysis some lessons for the future actions;

•Automated replication and storage of data and information from the main base control point to its other 1-2 own control points, at some subordinate echelon control points and at the upper echelon control points;

•Appointing the high commanders following serious criteria such as professionalism, psycho-moral training and resilience in stress environments, under the conditions they exercise management of complex human and technical systems and have a wide spatial unfolding (is easy to understand from the situation itself that the increasing number of political appointments in recent years in Romania were destined, from the beginning, to destroying the cohesion and efficiency of military structures in any modern army);

•With the help of the new technologies, it was possible to reduce the number and the size of the communication and computer means, as well as the control cells, in some cases almost ten times. This has increased the mobility and protection of all control points.

In the field of ISR sensors sub-systems' integration in the C4ISR complex systems, we could mention the following points:

• We can clearly understand that communications and informatics systems cannot be a strong differentiator in complex military actions without an operational and technical integration of large classes of optical-electronic sensors (radar systems, infrared sensors, optical sensors, acoustical sensors, laser marking and sighting systems, etc.) as we now understand through highly integrated C4ISR (+ variants) systems;

• Conceiving, starting from all the information and data gathered through modern technical (including satellites) and human means, of a common image of the space of military actions and sending it to the entitled people in real or almost real time;

• Creating operational and technical possibilities to "see" further and faster than the enemy, through the combined performances of sensors, humans and computers;

• Taking technical and organizational measures to protect sensors from the potential countermeasures of the enemy;

• Creating a real possibility for each combatant to become himself a sensor integrated into a system by communication means, micro-computers and sensors he wears in battle, no matter the environment or place he is situated in a given time.

As a conclusion to this chapter we can state that the new technical means (communications, computers, software applications, sensors) directly determine increased efficiency and rapidity of command and control acts and concomitantly bring to the front new external risks and internal vulnerabilities which must be acknowledged and counteracted.

3. Evolution of communication and informatics systems in the Romanian Armed Forces between 1950-2017

We consider that the development of Romanian Armed Forces signal branch following World War II is very well synthesized in the Communication and Informatics chapter (pages 408 – 441), in Romanian Armed Forces Encyclopedia (*Enciclopedia Armatei României)*, published in 2009, chapter republished by the Signal Command in Communications and Informatics Journal no. 2 (10) in 2009 (*Revista Comunicaţiilor şi Informaticii nr. 2 (10), 2009*).

We think it is necessary to recall some main aspects with positive or negative effects in time (some prolonged until today):

•From 1950 until 1968 we can speak about signal in the lower limit of an European armed force, with exclusively analogue techniques imported from USSR, usually at least 10 years behind the endowment of the armed forces of our (then) ally;

•The events in August 1968 represented the wakeup call for the Romanian political and military decision-makers (but not for long time) that saw the quantitative and qualitative scarcity of technical structures and means in exercising troop leadership during that period of time. Therefore, the focus was on the design and manufacturing in our country of some types of technique and equipment with acceptable performances, adapted to the need of troops conduct on the national territory.

•In 1978, the Command of Signal Troops (CTT) established "The Study on the development of signal branch of service" and mainly proposed measures to improve armed forces' signal troops in order to avoid stagnation, material and moral obsolescence of the technique, diminished leadership response capacity in special situations.

•There was some progress, particularly in the production of techniques for tactical echelons but in the middle of the '80s the enthusiasm stopped. The excessive saving measures imposed on the armed forces by the political leadership of that time made the encouraging dynamics of efforts to improve the signal means and forces not to produce obvious improvements. 1989 found the armed signal system at the level of an analogue one, equipped with obsolete heterogeneous technique with a lot of technical risk elements, with no obvious forms of transit to digitization, computerization and automation.

•Since 1990, a new process of modernization of military signal has started, in all its aspects (human resources, organizational structures, technical systems and equipment), a process that has proven to be long and difficult, often carried out under hostile conditions, especially on the part of those who have the legal obligation to allocate a minimum of financial resources:

oAt the beginning of February 1993 in Signal, Informatics and Electronics Command (TIEC) the final form of *„The conception of organization and achievement of Romanian Armed Forces Signal System – STAR"* was defined;

o The mentioned conception was analyzed and approved in the Supreme Council for Countries' Defense meeting on 09.06.1993.

It is necessary to mention that the unitary conception approved by Decision no. 0031 from 09.06.1993 was based on the following:

o The own experience in the Romanian Armed Forces accumulated along the years in the field of designing, achievement and use of military signal systems;

oExperience and advanced technologies in some armed forces in NATO countries (US, UK, France, Italy, Germany, Belgium) transmitted to our armed forces by publications, special books in the field, studies, analyses, direct meetings, etc.;

o Projected structure of our armed forces in the perspective of 2005-2015 years;

o Organization of armed forces leadership on the whole hierarchic scale at peace, crisis and war;

oProvision on fully safety and technical accuracy of information relations, based on some rules agreed with other state institutions with duties in the field of national security, defense and public order by using existent and gradually implemented resources ("network of networks" concept, based on organizational and technical solutions of interoperability).

•**Starting with 1994** we passed to the conceptual and technical grounding of *STAR Project* (RTP and HF and VHF Radio Program with frequency hopping stations), on the bases of consolidation of knowledge and access to information on the experience and technologies of Western modern armed forces and following the lessons learned along the participation of some Romanian specialists to the "Combined endeavor" series of exercises and to activities organized by NATO General Headquarters (after January 1995) and of some activities of Alliance's armed forces (US, UK, Germany, Italy, Belgium, etc.). An important role was played by the effort to fulfill the interoperability goals in the field of communications and informatics set by NATO in the process of preparation for adhesion (1995-2002). The implementation of these goals' requirements was clearly and unequivocally the first step in inviting our country, in October 2002, to adhere to the alliance with full rights and obligations.

•Without many details[3], we can say that until now big steps have been taken in consolidating some modern communications and informatics systems without reaching yet the level of strongly integrated C4ISR (+variants) systems, particularly because of the lack of allotted financial resources.

•Military and civilian specialists familiarized with the evolutions in Romania in-between 1990-2017 appreciated almost unanimously the phenomena produced:

o the poor condition of whatever remained from the so-called „defense industry";

o the wrong policies applied between 1990-2017 in maintaining and consolidating some sub-fields with technological and scientific potential in Romania;

othe employment of poor and sometimes fraudulent management that fully contributed to the bankruptcy of some productive units;

o the existence of unlawful interests in obtaining the land on which the production units of the fighting equipment and machinery were situated (and these actions are still in progress);

othe discouragement of private companies that appeared in Romania with defense products and services, and resorting, sometimes without arguments, only to imports;

oThe lack of political factors' interest in army endowment and the under-financing of major projects, the making of negative budget rectifications and the establishment of strong bureaucratic and other nature barriers, leading to the beginning of tender procedures only in September-

[3] *Communication and Information Journal (Revista Comunicațiilor şi Informaticii),* no. 2 (10)/2009, pp. 30-36.

October of each year, with the loss of funding due to lack of time (this phenomenon even seems to be done on purpose);

○The loss of specialists of great value, some with unique specialized training who, due to lack of resources and prospects, were forced to leave in other areas or even emigrate;

○The complete indifference of the political factors with responsibilities in national security and defense for the export of equipment and services in the defense field to the markets that Romania had had and for those products that have remained or could be made competitive (the export has diminished from 800 million USD per year between 1985 and 1989 to 50 million USD per year at present). The explanations given by the decision-makers lack credible arguments and are, consequently, unconvincing.

•The transformation of the Armed Forces Planning process (the famous PAAP) into a real farce, as it can be clearly demonstrated in the following reasoning: let us assume that the military, having the right arguments, sets the endowment needs for the next year at 100 LEI. The government says it is a crisis and it only allocates 10 LEI, the Defense minister and the generals report that they are happy and they will make do with 8 LEI. The year passes and in December, it is found that they actually received (by deliberate action) only 2 LEI. It is clear that Romania will only have a Defense of 2 LEI worth.

•In the context of the above mentioned facts, we present a fragment from an interview given by George Friedman, the founder of STRATFOR to journalist Anne-Marie Blajar, hot_news.ro, November 16, 2010, regarding the situation of Romania (Romanian political and military decision-makers could study the whole Interview and take notes):

„[...]Another thing that (Romania) has to have is armed forces. You are not taken seriously in this world unless you have an army. You will say it is expensive. And I will tell you to look at the past century: 5% of GDP would be a colossal amount, but I am sure you would have paid much more to avoid the Russians and Germans. If you think there are no threats anymore and they will not exist, then you are in a very rational position. On the other hand, you have to think that in this part of the world there was no century without a tragedy. And under these circumstances 5% does not mean so much.

Poland believed in 1939 that it had a relationship with the Germans and the Russians, which made it unnecessary for the radical upgrading of its army.

There are two issues: firstly, you cannot help a country that collapses in a week. And secondly, in this world no one helps a country that cannot help itself. The idea that the Germans will send young people to fight and die in the interest of Romania is not rational. You can argue that Russia will not be aggressive, maybe it will not be, but in the past, every time an East European country had bet that another one would not be aggressive, it lost. If you build your Defense and they are not aggressive, you have wasted some money. If you build your Defense and therefore they are not aggressive, you will never know it. But if you build your Defense and enemies do come, then alliances mean something. No one will send their children to defend you. I have two children in the US Army: my daughter has been in Iraq for 25 months, my son is in the Air force. They do not come here to defend the Romanians.

If it is in our interest, then it is another problem. One thing that the Romanians, like a mature nation, must ask themselves is how to turn this into the interests of the Americans? ...”

4. Strengths of Romanian Armed Forces CIS based on the principles developed and applied in the NATO member countries’ armed forces

In the title of my article I refer to the latest twenty years (1997-2017) because in 1997 a series of important events took place for the army in general and especially for communications:

•On April 30, 1997 the Communication and Informatics Directorate is established in the General Staff (DCI/SMG);

•In the spring of same year the first three centers from the Permanent Signal Network (RTP) were created, as the main part of the new Signal System of the Romanian Armed Forces (STAR), following long theoretical and practical efforts undergone in an atmosphere of hostility and continuous attacks (1993-1997). In 2002, RTP was about 60% of what was specified in the provisions of the Project, and in 2010 it became 100%.

•HF and VHF with radio hopping frequencies reached 50% in 2002.

In addressing this point, a thorough and comprehensive analysis of strategic, operational and tactical issues is needed on the following: the structure of the forces, the peace arrangement and possible variants of war, the organization of command and control (human resources, state-of-the-art technology, layout of driving points on the entire hierarchical scale, management reservation, etc.).

Thus, the following principles were materialized which can be considered as strengths.

The system is military, with unique leadership achieved by the specialized bodies of General Staff (Communications and Informatics Directorate and Communications and Information Command). This system is based on military principles, on peace and war situations, different from other commercial or special systems. The predominance of the strategic, operational and tactical requirements with respect to the technical requirements can be defined as follows:

•It is automated, secret and multiple reserved.

•It is based on military standards and requirements, as a condition of interoperability with tactical mobile systems and with NATO and Allied armed forces.

•The system is permanently in readiness (combat) mood through the management and operation service provided by well-trained and motivated specialists.

•A complete secrecy of the structures of the existing system at peace and its development at war is ensured (or should be ensured).

•The STAR structure has the real capacity to provide some independence from the current and future layout of the control points and device elements.

•There has been and continues to be a radical change in the share of signal in the system - the percentage reduction of voice signal in favor of data transfers.

•The possibility of rapid reconfiguration of the broadcasting system is ensured in relation to the complex conditions of a possible war:

- Permanent signal network at peace RTP/RMNC;
- Strategic signal network at war, by adding new mobile and fixed centers in RTP/RMNC.

- An enhanced independence (now necessary) from the commercial networks (channels provided by these means become complementary).
- A high reliability (see books and studies on this subject) to ensure uninterrupted connection and in the event of permanent or temporary dismantling of up to 50% of its elements.
- RTP/RMNC elements are located in the territory so they can be defended by the army units in the area.
- Provision of radio-relay equipment and radio with frequency agility (the ability to “escape” from jamming and interception of the enemy).
- Ensuring interoperability without organizational and technical problems with NATO similar systems.
- Establishing an interconnection solution with other special systems on the basis of the arrangement of bidirectional access gates without a subordination relationship of the armed forces’ system and an exaggerated dependence on their administrators. The main issue here is the military principle whereby the commander of the operation (the battle) relies first of all on his own human and technical resources and does not have to ask for communications from others, no matter how good they are supposed to be.

These strengths (principles) present in the STAR conception, in the Technical Project and related documents (over five hundred thousand pages) which were approved by several CSAT decisions, orders of the Minister of Defense and the Chief of General Staff, cannot be the object of self will (without operational and technical arguments) of several officers from the Communications and Information Section and the Communications and Informatics Command, who after 2010 ignored them or destroyed them, for purely commercial reasons, by resorting to certain suppliers, “designated on purpose”, and who greatly contributed to transforming the systems into a mournful monk pot.

If they want to change everything, they must obtain approval from the same forums (CSAT, the Minister of Defense, Chief of General Staff). If not, they could face even criminal consequences in crisis or war situations.

We will see (obviously still briefly), in the following chapter related to vulnerability, the huge dangers these systems are exposed to primarily for internal and then external reasons.

5. Internal vulnerabilities, failures, abandoned and postponed projects

As justifiable as possible, with operational and technical arguments, military communications and information systems represent a vital part of Romania's critical infrastructures. On this topic, we published in 2010 an article[4], with some issues regarding the provision of their physical and information protection, in the context of ever-increasing threats. There are other authors who have published studies and articles on this subject, with a clear intention to raise awareness of political and military decision-makers, and to prompt the taking of concrete measures of development and protection[5].

Unfortunately, these measures are completely lacking, and planners, designers and users of military communications systems seem to serenely ignore this complex and difficult to manage issue.

In the following lines, we will not resume the ideas we wrote in 2010, but we will refer to some concrete issues that, on short and medium term, will create dangerous situations for the country's Defense capability.

We will mainly refer to the current state of RTP/RMNC because of the total dereliction of normal maintenance and repair work since 2010. As far as we are concerned, the situation is due to a mix of causes: sheer irresponsibility, lacking professionalism, precarious training in the field of strategic and operative knowledge, evil considerations and servility towards persons who issue aberrant orders, all of which result in the undermining of the country's Defense capacity, in a fully documented and qualified way including criminal intent. **Let us explain:**

- Between 2010-2017 minimal maintenance activities were not completed, except for 12 of the centers.
- Mending some equipment and modules was practically abandoned; in warehouses there are hundreds of dysfunctional elements.

[4] Constantin Mincu, *Sisteme şi Reţele de comunicaţii şi informatice militare şi speciale, ca parte vitală a infrastructurilor critice ale României, Asigurarea protecţiei fizice şi informaţionale a acestora,* Revista de Ştiinţe Militare a Academiei Oamenilor de Ştiinţă din România, nr. 2/2010.

[5] Gr. Alexandrescu, Ghe. Văduva, *Infrastructuri critice. Pericole, ameninţări la adresa acestora. Sisteme de protecţie,* Editura UNAp, Bucureşti, 2006.

- In the last four years, some maintenance works were attributed to clients on the basis of pressures by politicians and on a single criterion - the "dumping price" of companies with no operational and technical connection to such a complex national network which still is RTP/RMNC. The effect is the destruction of this national and military asset in the shortest possible time. **Let us explain the effects that are already taking place:**
  - Blocking telephone calls and data traffic for specific MoD applications generated by the disconnection of high-bandwidth interfaces, which determines traffic concentration on low-capacity connections (2 Mbps), a phenomenon that produces saturation thereof;
  - Anomalies in the operation of the bit synchronization processes that take place between communications equipment, with obvious repercussions in the quality of voice and data connections, anomalies caused by inadequate state of interconnected equipment (TDM and ATM switches, multiplexers, radio-relays, etc.):
    - Impossibility to extend or even implement the late software version;
    - The malfunctioning/non-compliance of ATM and TDM levels within RTP/RMNC, this situation being determined by the lack of modules, sub-modules, exchange sub-assemblies and related materials due to the failure to perform timely repairs in specialized laboratories.
- There were identified and diagnosed some causes in the low performance functioning of RTP/RMNC:
  - The existence of some incomplete configurations of equipment;
  - Repeated resets of equipment, which generate the alteration of software packages;
  - Failure of subscriber units due to accidental short-circuits, accidental touching of terminations, inappropriate use of line and/or channel terminals;
  - Damage to the bit synchronization network due to failure of the clock source modules.
- The low performance functioning of the RTP/RMNC management system leads to:
  - Impossibility to keep up-to-date the global network database;
  - Impossibility to update the communications centers in a centralized manner;

- Impossibility to manage the alarms generated by the equipment and on these grounds the impossibility to take necessary measures to correct the inadvertencies.

•The rapid and irreversible degradation of waveguides going through breaks of radio links, generated by the lack/failure of waveguide pressurization equipment, corroborated with destruction of the excitatory membrane.

•Output of the temperature parameters of all the equipment, due to the lack/failure of the indoor air conditioning systems.

•Poor operation of the power/earthling systems, which can lead to equipment failure in the centers.

• Inappropriate operation of radiant systems (one of the causes being the desalination of the antennas), which generates the interruption of high-capacity flows.

We have to state once more that, under the conditions of major malfunctions in RTP/RMNC, the communications support for data network systems and applications that are transiting the network will be seriously affected with respect to the following aspects:

•Voice and data communications for all the users;

•INTRAMAN;

•SCCAN (Air Police, FDEX, SIMIN, RAP, LAP etc.);

•MoD video-conference;

•CRONOS

•Communications connections with the theatres of operations;

•Communications connections with NATO and EU systems;

•CBRN Surveillance and Warning System.

Other threats and internal vulnerabilities can be added to the above:

•Lack of preoccupation to get and maintain information superiority;

•The often flagrant discrepancy between information requirements for decision-making and leadership of national security actions and the real possibilities of acquiring them;

•Inadequate design, organization or operation of information systems;

•Endowment of information systems with means of data collection, communication and poor performance computers that are difficult to exploit and to be ensured protection, their misuse (see the mix of non-performing commercial equipment introduced in RTP/RMNC in recent years);

•Lack of understanding of the internal and international security environment and its influence on the information processes of the military structures;

•Inappropriate organization of databases, the existence of non-performing software or intentional errors;

•Poor professional training and reduced experience of the personnel involved in organizing, operating and assuring the functioning of information systems (in our opinion, this phenomenon is found throughout the current hierarchical scale);

•Inappropriate classification of the categories of information and data on national security and erroneous certification of the right to access them;

•The disloyalty (increasingly obvious) of some people who exploit the technical equipment of information systems;

•Reduced security of data and information during the transmission of their storage, processing and display, unauthorized access of foreign persons.

We also consider it necessary and, at this stage, we have to ask for the civil and military officials who have a greater or lesser degree of involvement in military communications and information systems to perform a point-to-point surgical analysis to identify operative measures to put the systems back to work and to take appropriate physical and information protection measures due to the actual threats and vulnerabilities presented and others that may occur.

We should mention in this context the postponement or dereliction of vital systems for the Romanian Armed Forces, such as:

•C4I tactical systems for tactical echelons (company, battalion, brigade, division), under the command of Land Forces Staff;

•The achievement only of islands with insignificant role in leading the forces;

•Unreasonable delays for specific Air Force Staff and Navy Staff systems;

•The failure to carry out the automated management of the radio-electronic spectrum.

There is a persistent lack of financial resources, but if nobody asks (more decisively) the political factor and the government does not allocate any money, they have other „priorities”.

6. Vulnerabilities and external threats on C4I systems

External information threats comprise the specific actions executed by potential adversaries and hostile forces to our country in order to forbid or harden the execution of decisional and operational functions on national security.

According to the conclusions drawn in the specialized literature[6], the main vulnerabilities and threats are as follows:

•Physical attacks against data sources and means of information transmission, processing and display;

•Electronic attacks on means of collecting, transmitting and collecting information;

• Cyber-attacks against the information systems of information security structures for national security and those of economic, financial, diplomatic organizations etc.;

•Software piracy;

•Physical and electronic attacks on the decision-making bodies of our state (Presidency, Parliament, Government, Ministries, etc.) related to national security;

•Psychological attack on all decision-making and action structures of our country (political, economic, social, Defense, etc.).

These threats are not new, they are generated by the development of the information society itself, but we need to know, carefully study and precisely determine the appropriate measures to combat them.

It is well known that the purpose of collecting information for national security is to ensure accurate knowledge of the international situation, especially in the area of interest of Romania, the European Union and NATO, as well as the domestic situation in our country and in the

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

neighboring countries, thus realizing the anticipation of some aggressive actions of potential opponents or hostile groups and, consequently, preventing surprise.

Along with these threats and vulnerabilities presented above, many others can be identified by studying literature and by conducting case studies on events that have recently taken place in our area and around the world.

Prevention and protection measures must go beyond the declarative and academic phase and it is necessary for today's and tomorrow's decision-makers to take concrete, visible and verifiable measures, obviously providing the necessary human and financial resources. That if we still want to exist as a state, if not, no.

7. Some conclusions

The statements of General (Ret.) Colin L. Powell (AFCEA, 2006, Washington DC):

•Civilian and military statesman have political and moral responsibilities to the combatants sent in the operation fields;

•Soldiers (understood as fighters, no matter the rank) cannot be the subject of propagandistic and politician actions, crocodile tears, expressed in the media, after misfortunes have happened, resulting in loss of young lives;

•Endowment with weapons, IT & C equipment and military means of protection must be the zero priority of the US Army (author's note - and any other military);

•Modern wars and conflicts have unquestionably proven that the importance of C4ISR systems has grown exponentially, from strategic to soldier level, meaning real-time visualization of the space of operations, relevant information for fighters, aspect which saves lives more than the thickness of any armor.

The evolution of the field (CIS, C4ISR, etc.) continues at an alert pace in the NATO and non-NATO armed forces (Russia, China, India, etc.) in the tough competition for winning and maintaining information superiority.

The rapidity of change is evident in the field of computers and software applications, in the development of space technologies, the miniaturization of components and equipment, which directly contributes to increasing mobility and troops' protection.

Microelectronics, Informatics, Robotics, Nanotechnology are contributing to the development of new, increasingly sophisticated weapon systems.

The Romanian Armed Forces moved in the right direction (in the context of harsh financial constraints) in the period 1994-2006, but after that, practically, abandoned the C4ISR modernization programs and projects; the main structure affected because of that being Land Forces Staff, its large units and subordinate units. No real possibilities for good change in the future seems to be identified.

BIBLIOGRAPHY

*** *Classified Information Protection Act*, no. 182/2002, published in the Official Gazette no. 248/2002 (In Romanian: *Legea privind protecția informațiilor clasificate,* nr. 182/2002, publicată în Monitorul Oficial nr. 248/2002);

*** *Concept of organization and realization of STAR,* Command of Communications and Informatics, Bucharest, 1993 (In Romanian: *Concepția de organizare şi realizare a STAR,* Comandamentul Comunicațiilor şi Informaticii, Bucureşti, 1993);

*** *Doctrine of Intelligence, Counter-Intelligence and Security of the Armed Forces*, Bucharest, 2005 (In Romanian: *Doctrina pentru Informații, Contrainformații şi Securitate a Armatei*, Bucureşti, 2005);

*** ENISA Risk Management/Risk Assessment (European Network on Information Security Agency);

*** *General Technical Project of RTP / STAR*, General Staff, Bucharest, 1996 (In Romanian: *Proiectul tehnic general al RTP/STAR*, Statul Major General, Bucureşti, 1996);

*** *National Security Strategy of Romania*, Bucharest, 2014 (In Romanian: *Strategia de Securitate Națională a României*, Bucureşti, 2014);

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

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

ALEXANDRESCU G., VĂDUVA G., *Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție,* Editura Universității Naționale de Apărare „Carol I", Bucureşti, 2006.

ANDERSON H.R., *Physical Vulnerabilities of Critical US Information Systems* (Internet, IaverMay03.pdf);

GANSLER J.S., BINNENDJIC H., *Information Assurance, Trend in Vulnerabilities, Thret and Technologies.*

MINCU C., *Analiză privind realizarea Sistemului de Transmisiuni al Armatei României (STAR),* Comandamentul Comunicațiilor şi Informaticii, Bucureşti, februarie 1997;

MINCU C., *Sisteme şi Rețele de comunicații şi informatice militare şi speciale, ca parte vitală a infrastructurilor critice ale României, Asigurarea protecției fizice şi informaționale a acestora,* Revista de Ştiințe Militare a Academiei Oamenilor de Ştiință din România, nr. 2/2010.