STRONG POINTS AND INTERNAL AND EXTERNAL VULNERABILITIES OF THE MILITARY COMMUNICATIONS AND INFORMATICS SYSTEMS AND NETWORKS DEVELOPED IN THE ROMANIAN ARMED FORCES UNDER THE CIRCUMSTANCES OF THE CURRENT SECURITY CHALLENGES

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

Abstract: *The author briefly presents a series of recent aspects in the current geopolitical context regarding some strong points as well as internal and external vulnerabilities of the military communication and informatics systems and networks developed in the Romanian Armed Forces since 1997. In the second section we referred to the evolutions in austerity and hostility conditions of the main operational and technical sequels of Romanian Armed Forces Transmissions System - STAR (RTP/RMNC). Furthermore, we presented some strong points of the achieved systems and principles taken into account along the modernization and transformation effort (regarding the NATO criteria and requirements), as well as their internal and external vulnerabilities identified following a thorough analysis.*

Keywords: communications, RTP/RMNC, STAR, NATO.

1. Introduction

We consider, based on a complex set of arguments, within the reach of current civilian and military decision makers of the Ministry of Defense that the theme we are interested in is also topical in the current global and regional geopolitical context.

[*] Full member of Academy of Romanian Scientists, member of the Honorific Council of Academy of Romanian Scientists, scientific secretary of the Section of Military Sciences; phone: 0722.303.015, email: mincu_constantin@yahoo.com.

In this respect, we think it is appropriate to repeat what we published in the Journal of Military Sciences no. 1/2008, in order to explain my and other authors' approach in the field of defense:

„Starting from the reality that the country's defense, as well as its armed forces, are public not private, and that clear provisions of the Constitution and specific laws entitle every citizen of the country to directly or indirectly contribute to strengthening Romania's capacity to defend itself if needed, we felt it appropriate to suggest that specific actions and processes be analyzed and debated within the Section of Military Sciences of the Academy of Romanian Scientists (AOSR). Clarifications are needed to meet possible puzzling situations and states of anxiety among civilian and military officials of some state institutions, who consider that they are the only holders of the truth and sometimes ask: "Why stir reservists about our issues?" The answer is simple – they get involved because they are Romanian citizen with citizenship rights and duties and they surely care about it. As for the particular case of members of the Section of Military Sciences of the AOS-R at least one other reason is added: among its members they are three former chiefs of the General Staff, heads of departments, professors teaching in civilian and military universities and some former important officials who held leadership positions in the Romanian State (Ministry of National Defense, Ministry of Interior, the Romanian Presidency etc.). Adding the fact that they all have PhDs and have as experience a major professional activity and an impressive work (books, manuals, studies, articles), attributes that gives them the ability for critical analysis and expertise in national security and defense of the country, they can provide objective points, fully virus-free from the influence of cyclical political and economic interests of groups, more or less interested in the fate of the country".

We consider that since 2008 until today (2015), the autism and easy-going attitude of the civilian and military people holding certain significant positions have become more and more obvious. As for the special case of leaders in the field of communication and informatics, at least since 2010, it went over any limit of good sense.

2. Brief history

There have been over 25 years since the first theoretical approaches and practical realization of what we call **"Transmission system of the Romanian Armed Forces – STAR"** (with multiple components) and many of the people today no longer know or do not want to know the efforts and steps taken in conditions of extreme austerity and in an atmosphere of hostility (details will be provided in another occasion) in order to make it viable. Therefore, we will briefly refer to the main points we consider might be useful in order to outline the phenomenon:

- **Concrete preoccupations** (studies, reports) for the organizational, structural and basic technical modernization of the transmissions system were quite numerous starting from 1970, but because of the lack of understanding and resources there were no great achievements.
- **On July 17th, 1991,** the General Inspectorate of Transmissions – GIT (the unfortunate name since then of the actual Command of Communications and Informatics) submitted to the General Staff a complete and well documented study on the major modernization of transmissions system. The basic problems released concerned the achievement of a strategic network on the whole national territory (named until 2006 – the Permanent Transmissions Network – (*Rețeaua Permanentă de Transmisiuni* – RTP), and after 2006 The National Military Network of Communications (*Rețeaua Militară Națională de Comunicații* - RMNC). The study was returned without any action taken.
- **In-between August 1991 – January 30th, 1993,** a small group of transmission specialists from GIT with a special committee compiled in many successive forms "The concept of the organization and achievement of *Romanian Armed Forces Transmissions System* (STAR)" grounded on:

- The severe critical analysis of the existent transmissions system;
- The experience in the field of the modern armed forces (there were studied tens of relevant books, manuals, hundreds of articles and documentaries obtained from different sources);
- The real necessities (based on a mathematic calculus) of all the echelons and types of military units from our armed forces;
- Close and permanent consultation with the transmissions specialists from all the armed forces;

- Consultation with the specialists in the central bodies of MoD and military academies;
- Many other strategic, operative and tactical considerations.

- **The „Concept of the organization and achievement of Romanian Armed Forces System of Transmissions (STAR)"** in its final form was defined on January 30th, 1993 and presented to MoD leadership at the beginning of February 1993, with the proposition to be submitted for CSAT (Superior Council for Country's Defense) owing to the importance of the issue, the special financial needs and the poorness of the current system (totally technically and organizationally obsolete), situated at the level of 1960s.
- **The concept mentioned above** was appropriated by the MoD leadership and handed in to CSAT at the end of March 1993.
- The document was discussed in CSAT meeting in June 9, 1993, and a decision was made **to approve** the creation of the system.
- **After the meeting in June 1993** different attacks and interventions followed from some representatives of the defense, public order and national safety system's institutions and two armed forces' officers and this led to delays and to re-analyzing the issue in other CSAT meetings (we do not recall them here) and to the triggering of a virulent press campaign led by authors well-known for their interests meant to block the programs for various reasons.
- **Following the situation created** there was proposed and approved the creation of an "Interdepartmental Collective Team formed by specialists from MoD, Ministry of Interior, Romanian Intelligence Service, Foreign Intelligence Services, Communications Ministry and Special Transmissions Service (16.09.1993)". „The Collective Team" came up with the document entitled **„Conclusions on the working compatibility of RTP/STAR"**. This document was signed and assumed by all the representatives of the mentioned institutions. Nevertheless, the ungrounded attacks continued and therefore the first centers finally managed to be installed in the spring of 1997, and 50% of the network was configured in 2002 (strong argument for NATO integration), and the final steps of implementing it were prolonged until 2010 (from subjective and objective reasons among which there was the random financing without any responsibility).

- **There are also arguments and details** which from understandable reasons cannot be made public.

3. Strong points based on principles developed and applied in the armed forces of the NATO member countries

Addressing this point requires a thorough and extensive analysis on strategic, operational and tactical matters on: force structure, forces deployment to peace and possible alternatives to war, organizing command and control (human resources, appropriate technology, number and arrangement of leadership points in the entire hierarchical scale, reservation of leadership, etc.).

Thus, the following principles were materialized, which can be considered strong points:

- **The system is military,** with unique leadership ensured by Romanian General Staff through its specific bodies (Communication and Informatics Directorate and Communication and Informatics Command). This system functions at war and at peace following military principles different from the principles of the commercial or special systems. Primarily, the strategic, operative and tactical requirements have precedence over the technical requirements.
- **It is automatized,** secured and multiply reserved.
- **It is achieved in compliance with military standards and requirements,** as a condition of interoperability with the systems of NATO and allied countries.
- **The system is permanent and ready (for battle)** from the point of view of management and operation service provided by well trained and motivated specialists.
- **It provides (or it should provide) a faultless secrecy** of the structures of the system existent in peacetime and developed at war.
- **STAR structure** has the real capacity to provide a certain independence from the current and future layout of command posts and related elements.
- **It has prompted** furthermore the radical change of the share of transmissions in the system – the limitation of voice broadcast percentage in the favor of data broadcast.

- **It has provided** the possibility for quick reconfiguration of transmissions' system, related to the complex conditions of a presumed war:

- Permanent transmissions' network at peace RTP/RMNC;

- Strategic transmissions at peace by adding new mobile and fixed centers in RTP/RMNC.

- **Enhanced independence** (necessary now) related to the commercial networks (the channels provided by these become complementary).
- **High reliability** (see the books and studies on this topic) to provide the uninterrupted connection and also in situations of permanent or temporary shutdown of at most 50% of its elements.
- **RTP/RMNC elements** are arranged in territory so as to be able to be protected by the military units in the area.
- **Provision with radio relay and radio with agile frequency** (possibility to "escape" the jamming and interception of the enemy).
- **Provision of interoperability** without organizational and technical faults with systems similar to NATO.
- **Achievement** of a solution to interconnect with other special systems grounded on the convenience of some bidirectional access gates without any relation of subordination of the military system or exaggerated dependence on their administrators. Here, the main military principle functioning is that the operation (mission) commander should firstly rely on own human and technical resources and he should not beg to ask for communications from others, no matter how credible and trustworthy those are supposed to be.

These strong points (principles) presented in STAR concept in the Technical Project and in the annexed documents (over one hundred thousands of pages approved by many CSAT decisions, orders of Defense Minister and Chief of General Staff cannot be overlooked (without operational and technical reasons) at the free will of some officers from the Communications and Informatics Directorate and Communications and Informatics Command. Thus, after 2010, these principles were ignored or destroyed for purely commercial considerations in order to please some **"specifically assigned"** providers, resulting in the decay of the already poor condition of the systems.

If these want to change everything they must gain the approval of the same bodies (CSAT, Minister of Defense, and Chief of the General Staff). If not, in case of a possible outbreak of a crisis or war, some bad consequences may occur, even involving criminal penalties.

In the following section we will try to cover (obviously briefly) the dangers these systems are exposed to by internal and external considerations.

4. Internal vulnerabilities

As justified as it could with operational and technical arguments, military communications and informatics systems are a vital part of the critical infrastructure of Romania. On this subject we published an article[1] in 2010 in which we referred to some issues related to their physical and information protection in the context of the increasing threats. There are other authors who have published studies and articles on this subject, with the clear intention to sensitize policy and military decision makers so as to initiate concrete measures for their development and protection.[2]

Unfortunately these measures are totally lacking, and planners, makers, users of military communications systems calmly choose to ignore considering this issue which is so complex and difficult to manage.

In the next part of the paper we will not repeat what we wrote in 2010; instead, we will refer to some concrete issues, which, on short and medium term, will create a dangerous situation for the country's defense capacity.

We will refer mainly to the current situation of RTP/RMNC characterized by the total abandonment of regular maintenance and repair work since 2010. We think the situation is due to a mix of factors: utter irresponsibility, lack of professionalism, poor training in knowledge of strategic and operational level, sheer meanness and obedience to the superiors giving aberrant orders, all resulting in undermining the defense

[1] 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.

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

capacity of the country, which can be documented and stated as such, including according to the criminal law. Let us explain:

- **In-between 2010-2015** minimal maintenance activities were performed only for 12% of the centers.
- **The mending of some equipment** and modules was practically abandoned and in the warehouses there are hundreds of broken, dysfunctional elements.
- **In the last two years,** some maintenance work was customary attributed and based on a single criterion – the "dumping price" of some companies without any operational or technical relation with such complex national network which RTP/RMNC still is. The effect is the destruction of this national and military asset in very short time. Let us explain the effects which are already manifesting:

- **The blocking of telephone and data traffic** for specific MoD applications caused by the interruption of connections at the interfaces of large capacity which determines the concentration of traffic on low capacity links (2 Mbps), phenomenon that produces their saturation;
- **Faults** in the bit synchronization processes function taking place between communications equipment, with obvious repercussions in terms of voice and data connections quality, anomalies generated by the inadequate condition of interconnected equipment (TDM and ATM switches, multiplexers, radio links, etc.);
- **Failure** to extend the implementation of the latest software;
- **Malfunctioning**/improper use of ATM and TDM levels of the RTP/RMNC, this being determined by lack of modules, sub-modules, subassemblies parts and related materials, because of faulty or lack of timely repair works in specialized laboratories.

- **There were identified and diagnosed** some causes for the low performance function of RTP/RMNC:

- Existence of incomplete configurations of equipment;
- Repeated resets of equipment, generating the alteration of software packages;
- Damage of subscriber units caused by short accidental circuits, accidental touching of terminals, inappropriate use of line and/or channel terminals;

- Deterioration of the network due to failure of bit synchronization clock source modules;

- **The low performance functioning** of RTP/RMNC system of management leads to:

- The impossibility to update the global database of the network;

- The impossibility of communications' centers updating in a centralized manner;

- The impossibility to manage the alarms generated by equipment and on their basis, the impossibility to take the necessary measures to correct the emerging inadvertencies.

- The quick and irreversible decay of wave guides resulting even in interruptions of radio relay links generated by lack/ failure of pressurization wave guides equipment coupled with the damage of the exciter membrane.

- **Exiting the temperature parameters** of all equipment, which is determined by lack/ failure of enclosure climate control systems.

- **Failure of the power supply**/ground systems which can damage the equipment of the centers.

- **Malfunctioning of radio systems** (one of the reasons being the mis-alignment of the antennas) which generates the interruption of high capacity streams.

We have to state that given the appearance of major faults in RTP/RMNC some communications support for systems data and network applications will be seriously affected, such as:

- Voice and data communications for all the users;
- INTRAMAN;
- SCCAN (Air Police, FDEX, SIMIN, RAP, LAP, etc.);
- MoD video-conference
- CRONOS
- Communication links with theatres;
- Communication links with NATO and UE systems;
- CBRN Warning and Surveillance System.

To the list above, we may also add other threats and internal vulnerabilities:

- Lack of concern for acquiring and maintaining information superiority;

- Inconsistency - often blatant - between the demands of information for decision making and management of the activities of national security and possibilities of their acquisition;
- Design, organization or malfunction of information systems;
- Information systems equipped with means of data collection, bad communications and computers, difficult to exploit and to provide protection, their misuse (see the mix of non-performing commercial equipment introduced into RTP/RMNC in recent years);
- Lack of understanding of domestic and international security environment and its influence on the information processes of military structures;
- Inadequate organization of databases, the existence of non-performing software or software with intentional errors;
- Poor professional training and low staff expertise involved in the organization, operation and functioning of information systems (in our opinion this phenomenon is found on the entire current spectrum);
- Improper classification in categories of information and data on national security and erroneous certification of staff's right to access it;
- Disloyalty (increasingly more evident) of some persons who operate the technical equipment of information systems;
- Reduced data and information security during transmission, storing, processing and displaying to the unauthorized access by strangers.

We consider that and, at this stage, we ask the responsible civilian and military staff who have more or less tangency with the communication systems and military information that a surgical, point by point analysis should be performed in order to identify measures for restoring operational systems and take appropriate measures of physical protection and information as a result of present threats and vulnerabilities or others that may occur.

5. External vulnerabilities and threats

The external informational threats include the range of specific action executed by potential adversaries or hostile parties to our country in order to forbid or harden the execution of decisional and operational functions on national security.

According to the conclusions reached in the literature[3] in the field, the main vulnerabilities and threats are the following:

- Physical assault against data sources and means of transmission, processing and display of information;
- Electronic attack on the means of collection, transmission and sampling of information;
- Cyber-attacks against information systems of national security information structures and economic, financial, diplomatic organizations, etc.;
- Software piracy;
- Electronic and physical attack on our country's decision-making bodies (president, parliament, government, ministries, etc.) for 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 very development of information society, but they must be recognized and carefully studied and the corresponding measures for combating them have to be precisely set.

It is known that the purpose of collecting information for national security is to ensure precise knowledge of the international situation, especially in the interest of Romania, European Union and NATO, as well as the domestic situation in our country and neighboring countries, thus anticipating the aggressive actions of potential opponents or hostile groups and therefore preventing the possibility of being taken by surprise.

Compared to these, the threats and vulnerabilities listed above can be better identified by studying the literature and case studies on recent events that occurred in our region and globally.

Preventive and protective measures must go beyond academic and declaratory phase and require the decision making factors for today and tomorrow to take concrete, visible and verifiable steps in this direction, obviously ensuring the necessary human and financial resources. That is, if we want to keep on surviving as a state.

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

BIBLIOGRAPHY

*** *Concepţia de organizare şi realizare a STAR,* Comandamentul Comunicaţiilor şi Informaticii, Bucureşti, 1993;

*** *Constituţia României*, Monitorul Oficial al României, nr. 233/1999 (in English: Romanian Constitution, Official Monitory of Romania, no. 233/1999);

*** *Doctrina Naţională a Informaţiilor pentru Securitate*, Editura SRI, Bucureşti, 2004 (in English, National Doctrine of Security Intelligence, SRI Publishing House, Bucharest, 2004);

*** *Doctrina pentru Informaţii, Contrainformaţii şi Securitate a Armatei*, Bucureşti, 2005 (in English, Doctrine for Intelligence, Counter-Intelligence and Security of the Armed Forces, Bucharest, 2005);

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

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

*** FM 3-13, Information Operations: Doctrine, Tactics, Techniques and procedures, US Army, 2003;

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

*** ISO/IEC 27001 Information Technology. Security Technique, Information Security Management – Requirements;

*** *Legea privind protecţia informaţiilor clasificate,* nr. 182/2002, publicată în Monitorul Oficial nr. 248/2002 (Law on the protection of classified information no. 182/2002, published in the Official Monitory no. 248/2002);

*** *Proiectul tehnic general al RTP/STAR*, Statul Major General, Bucureşti, 1996;

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

*** *Sisteme informaţionale*, Sesiunea anuală de comunicări ştiinţifice cu participare internaţională, Editura UNAp „Carol I", Bucureşti, 2007;

*** *Strategia de Securitate Naţională a României*, Bucureşti, 2014 (National Security Strategy of Romania, Bucharest, 2014);

ALEXANDRESCU C şi alţii, *Supremaţie electromagnetică,* Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 1999;

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

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

ALEXANDRESCU Ghe., VĂDUVA Ghe., *Infrastructuri critice. Pericole, ameninţări la adresa acestora. Sisteme de protecţie,* Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2006.

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

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

BĂDĂLAN E., *Securitatea României, actualitate şi perspective,* Editura Militară, Bucureşti, 2001;

FRUNZETI T., *Securitatea naţională şi războiul modern*, Editura Militară, Bucureşti, 1999;

FRUNZETI T., ZODIAN V., (coordonatori), *LUMEA DE AZI 2015*, Editura RAO, Bucureşti, 2015;

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

HLIHOR C., *Geopolitica şi Geostrategia în analiza relaţiilor internaţionale contemporane,* Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2005;

ILIE Ghe., STOIAN I., CIOBANU V., *Securitatea Informaţiilor,* Editura Militară, Bucureşti, 1996;

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

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

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

MINCU C., *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.

MUREŞAN M., VĂDUVA Ghe., *Războiul viitorului, viitorul războiului,* Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2005;

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

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

Publications in the field:

1. Gândirea Militară Românească (Romanian Military Thinking);
2. Buletinul Universităţii Naţionale de Apărare „Carol I”, 2008-2015 (Bulletin of “Carol I” National Defense University);
3. Revista de Ştiinţe Militare, 2006-2015 (Military Science Journal);
4. Annals series on military sciences, 2005-2015.