NETWORK-CENTRIC WARFARE AND NETWORK ENABLED CAPABILITY IMPLICATIONS OVER THE C4ISR TYPE INFORMATION NETWORKS IN THE ROMANIAN ARMED FORCES

Ltc. Gen (ret) Professor Cristea DUMITRU, PhD
- Associate member of the Academy of Romanian Scientists,
Military Sciences Section and former Chief of Romanian J.6

The last two decades have been marked by the evolution of mankind toward the Information Age, a new stage of societal development where the modern society is affected, among other factors, by the explosive technological changes. Within the context, technology represents the main driver for change. To be more specific, small innovations emerged in the information technology and communications are considered responsible for global transformations in the economy, politics or culture structure. This assertion also extends its validity over the military phenomenon, which is just another form of human behavior. The large scale use of the information technology and communications led to a cybernetic battlefield and the change of the war waging philosophy, with the rise of new concepts that better describe the new reality: Network Centric Warfare, and Network Enabled Capabilities.

1. Introduction

In our opinion, the conflicts' physiognomy of the end of 20th century and beginning of 21st century have radically changed. The complex set of factors which personalize the conflicts include particular political, economic and strategic situations, new political and strategic goals, new objectives, specific action forces and means, a different conception and intensity, a new attitude against the opponent, different action spaces, a comprehensive variety of dominant action types, and ever more sophisticated and unexpected ways of violence outburst. The world of these conflicts is a world of asymmetric confrontations.

Out of the main features of the current and future military conflicts it is worth to mention the following[1]:

- Causal complex that results from the existing incompatibilities between dictatorial political or autocratic systems and democratic ones;

[1] *Cf.* **Frunzeti, T., Mureşan, M., Văduva, Gh.,** *Război şi haos, Editura Centrului Tehnic - Editorial al Armatei, Bucureşti, 2009, pp.27-29.*

- Distinct fingerprint of the new military conflicts determined by the huge disparity between the rich world and the poor world, between the civilization of high technology and the traditional civilizations, diversified, with ancestral values, customs and traditions;
- The technological effect given by the different technological development;
- Different conflict intensity, from extreme violence of the terrorist attacks to domination or imposition of a certain conduct;
- Continuous Nuclear, Radiological, Bacteriological and Chemical threat;
- Dissymmetry and asymmetry;
- Ubiquity of the action – reaction binome;
- Prevention and the primitive character or repression;
- The new terrorism – antiterrorism binomial implication;
- The patchwork character;
- Unpredictability.

These features could be supplemented with others like flexibility and confusion, indirect character, political and religious extremism, etc.

The typology of war is extremely diverse, but when we refer to the conflict dimension we should only take into account three types of war, namely the asymmetric warfare, the cognitive warfare and the high technology and information based warfare (network-centric warfare).

The essential principles of the Information Age warfare are:

- ✓ Information superiority;
- ✓ Common access to a high quality system of information;
- ✓ Dynamic self-synchronization – to increase the freedom of the small operational structures;
- ✓ Dispersed forces and discontinuous operations;
- ✓ Flexible forces – easy transfer from the massing forces approach to the effect based approach;
- ✓ Large scale use of sensors ensuring a higher information level;
- ✓ Compressed levels of warfare and operations driving prevalently to joint operations;
- ✓ High speed of the command procedures;
- ✓ Full spectrum dominance – the ability of forces, operating unilaterally or in combination with multinational partners to defeat any adversary and control any situation across the full range of military operations[2].

Information operations represent the integrated use of the electronic warfare actions, psychological operations, deceiving, security of operations, command and control operations, "information supremacy" operations, psychological actions, hackers' actions, economic information actions and virtual space actions[3]:

---

[2] *Cf. Joint Vision 2020, Department of Defence, Washington D.C., 2000, p. 4*

[3] *Cf.* **Topor, S.,** *Războiul informațional, Editura Universității Naționale de Apărare, București, 2005, pp. 25-27*

✓ Command and control operations – neutralize the command and the command-control systems of the adversary. These operations integrate psychological operations, deceiving, security of the operations, electronic warfare and actions of physical destruction;

✓ "Information supremacy" operations – projection, protection, and annihilation of the systems which contain enough information to dominate a conflict space;

✓ Electronic operations – equipment employed to reconnoiter, neutralize, and destroy the electronic systems that generates or convey information, as well as cryptographic techniques;

✓ Psychological operations – the information is used to change the attitudes or options of partners, neutrals or enemies;

✓ Hackers' actions (software piracy) – computers and communication networks are the target of the active and passive attacks with disruptive and destructive software;

✓ Economic information actions – blocking or acquiring information in order to gain economic supremacy;

✓ Virtual combat space actions – fundamental and technological research of the war games and futuristic scenarios.

Offensive information operations are intended to neutralize the information systems and actions of the adversaries, while the defensive information operations are designed to defend the own elements against similar offensive operations of the opponents.

One of the modern ways to conduct combat operations is the Network-Centric Warfare (NCW). It is a relatively new state-of-the-art technological and information concept, with global scope, easy to access only by entities equipped with performing information and analysis systems, cutting-edge technologies, modern information technology and communications, and the technical support structures needed.

From the perspective of conflict dimension, network-centric warfare could be perceived from at least three points of view:

✓ Theatre warfare representing a confrontation between two or more armed entities, in a well defined theatre of operations as geographical area and philosophy of the real actions;

✓ War extended in other areas than those specific to the armed combat, like cyber space, media, economic and financial dimensions;

✓ War in the theatre of concepts, which has as goal the knowledge dominance, with a scientific foundation of some systems of action and reaction allowing the intelligent and efficient use of existing forces and means, together with the innovation of new ones, more performing, and more difficult to be identified and discovered.

The concept and employment of NCW belong to the nations that possess high level of technology, and developed information technology and communications, especially the United States of America, the only nation which successfully used them in a direct military confrontation, in Iraq.

The NCW concept provides six essential capabilities[4]:

- Real and virtual networks equipped with C4ISR (similar) systems;
- Relational databases;
- Rapid, flexible, expeditionary and interoperable forces;
- Interconnected weapon systems;
- Projection of forces and means;
- Networked logistics.

Although during the war in Iraq NCW proved its effectiveness, it still has some limits in the post-war operations. Under these circumstances, although NCW is likely to dominate the combat space (generally, the armed confrontations), it is not largely available. According to all probabilities, NCW will not succeed, at least for the first two decades of the 21st century, to provide all the advantages it has been created for, unless the combat environment has a high level of certainty dynamic, thus a disproportioned warfare. NCW is not a chaotic warfare, but one that has a rapid development and a predictable end, and that could produce chaos, since disproportionality brings quite serious problems in the immediate dynamic of the political, economic, social, information, and military situation.

2. Employment of the C4ISR Systems in the New Operational Concepts: Network-Centric Warfare and NATO Network Enabled Capability

The concept of NCW describes the combination of emerging tactics, techniques and procedures that a networked force can employ to create a decisive warfighting advantage[5]. Although this concept is strictly related to the reality of American military forces, its evolution – NATO Network Enabled Capability (NEC) – extended the theory over entire North Atlantic Treaty Organization. NEC is the cognitive and technical ability of the Alliance to conduct different components of the operational environment, from the strategic level, including NATO Command, to below at the tactical level, using a unique integrated network information infrastructure[6].

The purpose of the employment of new concepts like NCW and NATO NEC in planning, organization and warfighting is providing all leaders from every subordinated level with near real time information necessary to understand the tactical situation and to act according to the commander's intent. This increased capacity of command generates new operational challenges. While the subordinates have broader access to the tactical situation, high level commanders have access to very detailed tactical plans. The high level commanders should resist the temptation to conduct minor military actions at the subordinates' level, because their intention could reduce the benefits of the modern information systems and could also alter the level of understanding of the situation they support. As a result, it is necessary to promote strong leaders at every level, and to build

---

[4] *Cf.* **Frunzeti, T., Mureşan,** *M., Văduva, Gh., Război şi haos, pp.35-36.*

[5] *Cf.* **Garstka, J.J.,** *Network Centric Warfare Offers Warfighting Advantage, Signal Magazine, USA, May 2003.*

[6] *NNEC Vision and Concept, MCM-0032-2006, Allied Command Transformation, Norfolk, Virginia, USA, 2006, p.2.*

troops' confidence and cohesion on complex and combined systems and equipments C4ISR type, put in practice by realistic training, drills and field exercises.

A robust force strongly connected in network improves the information exchange, cooperation, quality of information, and the situational awareness that generates a significant growth of the mission efficiency. It has been practically demonstrated that information networks have positive impact on the combat power, synchronization of the staff personnel and decision makers on the battlefield, casualties cut, amplification of the force agility and operational tempo.

The new sensors, extended connectivity and new information systems substantially concur to the efficiency of the troops' combat actions. Information distribution increased the situational awareness with the direct improvement of the perception of battlefield environmental elements, and growth of both maneuver speed and fire precision. Extended connection enables troops to conduct combat actions on larger distances and spaces than in the past. Information availability and reliability allow a quick reorganization of the tasks and a full integration of the military units new entered in the theatre of operations. The network's level of development determines synchronization and correlation in time and purpose of the dispersed troops.

Command of a robustly networked force improves information sharing, collaboration, high-quality information, and shared situational awareness resulting in significantly increased mission effectiveness. The networked information has impact on the application of combat power, battlespace synchronization, decision-makers and staffs, lethality and survivability, force agility, and operational tempo[7]. **Figure 1** presents this process in detail within the network enabled organizational context.

Nowadays, there is a trend for the extended use of the information technology and communications in defense systems in order to develop operational capabilities at minimum costs. In most of the situations, the main intention is oriented toward the network working, namely making networks of sources, information, execution level, commanders, etc. This trend has the advantage of the use of the great developments in the information technology and communications field. Concepts like NCW and NATO NEC are designed to develop and extend important capabilities as: information collection, processing and dissemination; decision quality and command efficiency; cooperation between different structures and levels of the same structure; flexible use of the military units and defense systems[8].

[7] *Cf.* ***Cammomns, D, Tisserand, J.B, Williams, D.E., Seize, A., Lindsay, D.,*** *Network Centric Warfare Case Study, Volume I- Operations, V Corps and the 3rd Infantry Division (Mechanized), 2003, p. 13.*

[8] *Cf.* ***Timofte, G., Vasile, R.V.,*** *Direcţiile de evoluţie a sistemelor C4ISR impuse de cerinţele rezultate din conflictele militare contemporane, Sesiunea de comunicări ştiinţifice „Strategii XXI", Universitatea Naţională de Apărare „Carol I", Bucureşti, 2008, p.2.*

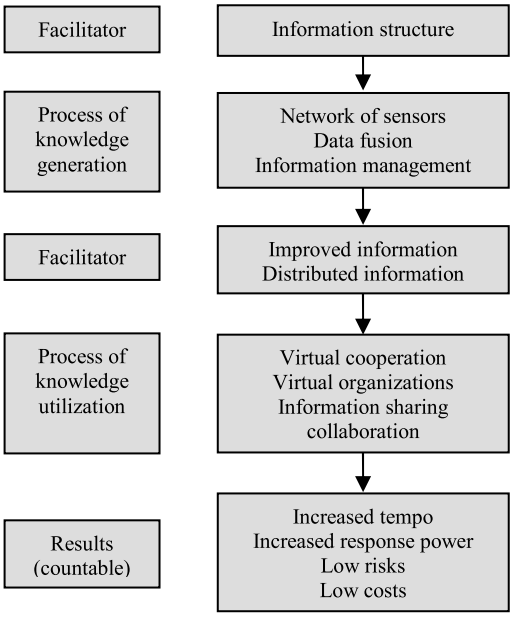

Figure 1: Command of the networked forces

These new concepts impose enhanced methods or even new methods of conducting operations. Introducing new capabilities could lead to radical changes in the defense organization, both from the point of view of technical system exploitation, and troop tactics and specific training. Concept development concurs, as well as with the efforts of adaptation to the global strategic and political environment established after the Cold War age, with its particular fragmented and sometimes unclear security threats. One of the main elements demanded by the NCW and NATO NEC concepts is achieving interoperability. Interoperability is a procedure used to strengthen equally the efficiency and effectiveness of the combined or joint forces, and the required capabilities for the whole operations range of the Alliance. Interoperability is an essential facilitator and an important force multiplier[9].

Several operational scenarios for operations or crisis management could be conceived in order to better understand the missions assigned to the C4ISR systems, and to observe major information needs and requirements. Information requirements include data, communications, capabilities, and cooperation tools that facilitate success in any scenario.

[9] *Enhancing Inteoperability, Executive Working Group, Brussels, 2008, p.1-1.*

The relationships between operational scenarios and information requirements assigned to the C4ISR systems could be represented like in **Figure 2**[10].

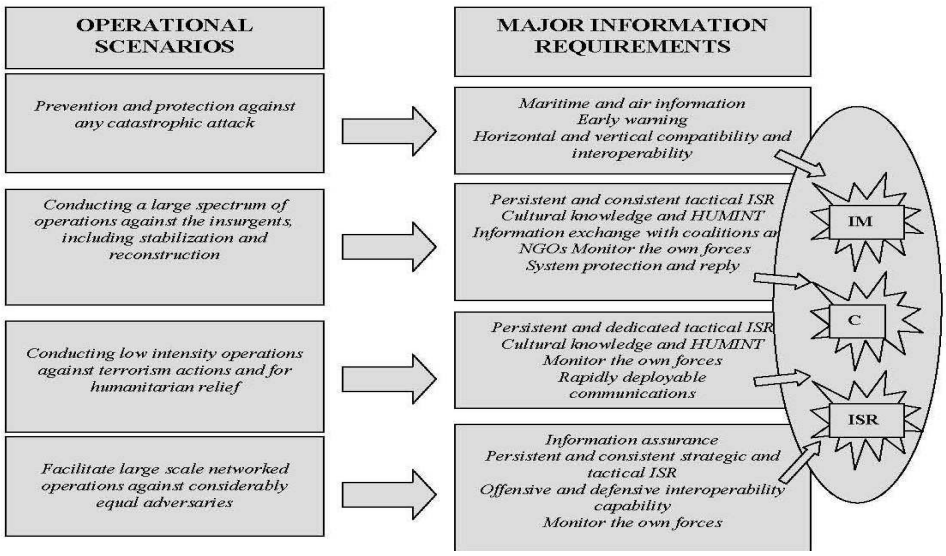

Figure 2: The relationships between operational scenarios and information requirements

Although after the scenario assessment a certain common line could be observed, this demands some particular information requirements out of which eventually three specific areas or domains will result as follows: information management (IM); command and control information capability (C2); information surveillance and reconnaissance (ISR). Taken as a whole, the three combined domains form a so-called information capability for combat/operations.

3. NCW and NATO NEC Implications Over C4ISR Type Information Networks

Military operations of the 21st century are characterized by a continuous growth of complexity due to the joint effort to accomplish the objectives, and to the interlaced nature of strategic, operational and tactical levels, as well as to the mixture of military and civilian objectives. Increasingly more, military commanders face the problem regarding the

[10] *Defense Science Board, Summer Study on Information Management for Net-Centric Operations, Vol. II, The Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington, D.C., 2006, p.10.*

conciliation of conducting traditional military operations with overall mission objectives, and the national policy goals.

Globalization, technological developments and the transition pace to the Information Age deeply affect the political, social and security environment, including NATO's ability to answer the new threats, demanding new deterrence, warning, and prevention strategies against terrorist attacks, with amendments in the proper application of the military and civilian powers, within the effect-based operations.

This kind of arguments determine the transformation of the Alliance and its members alike by enhancing the decision making processes based on information superiority and NEC. This approach aims at a deeper integration of political and military tools, adoption of new methods and organizational institutions able to generate rapid and decisive results at the tactical, operational and strategic levels, outside the traditional areas of responsibility. Resizing the decision making process, based on information superiority and implementation of the NCW and NATO NEC concepts represents essential parts of the armed forces transformation, with a decisive role for the information systems. The general framework of the Alliance transformation is presented in **Figure 3**.

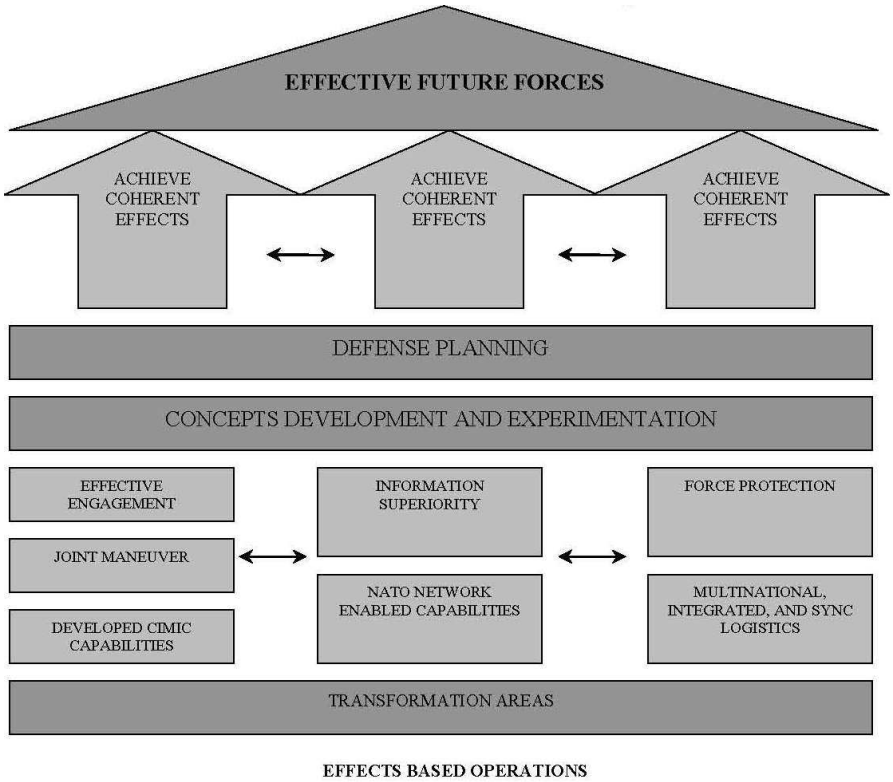

Figure 3: General framework of the Alliance transformation

This purpose is ensured in the military by developing the potential of the C4ISR systems that rationally encompasses the elements involved in the sensors interconnection (sources of information), performers/weapon systems (operational elements) and decision makers, together making possible the development of networking and effects based operational capabilities[11]. Providing information assurance, with direct influence on combat power and mission efficiency, drives the optimization of the deployment and support of joint forces.

The future combat space will include elements of the strategic concepts of NCW and NATO NEC that first will transform information in a power factor and increase the reaction capacity and precision of force commitment, and secondly will quickly include all the conceptual and technological innovations from the military. It is important to emphasize that if the new millennium conflicts will be conducted mainly in a coalition or alliance environment, then the most difficult obstacle is represented by the removal of the technological gap between the participant states.

The conceptual framework of NCW and NATO NEC and the way the integration of data collecting capabilities, decision making and transmitting the decision to the operational elements is conceived are synthetically presented in **Figure 4.**

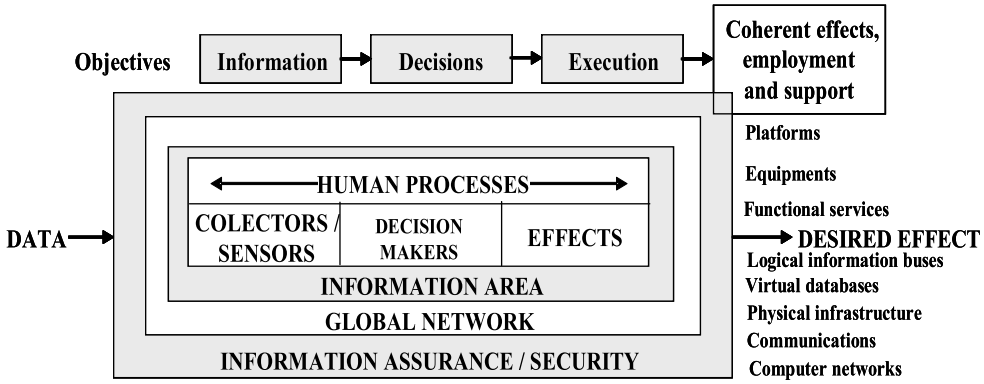

Figure 4: The conceptual framework of NCW and NATO NEC

The integration of these dimensions (elements) allow NATO structures and NATO nations to create a common picture of the battle space and consequently to enhance its level of situation awareness and the effectiveness of the common actions. The principle of making the common operational picture is shown in **Figure 5.**

[11] *NATO Network Enabled Capability Feasibility Study, v 2.0, Executive Summary, NC3A, Brussels, 2005, p.7.*

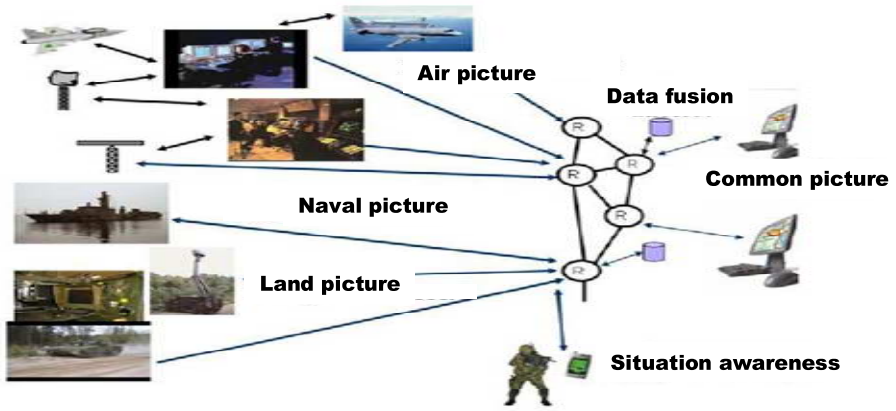

Figure 5. The principle of making the common operational picture

Concepts like NCW and NATO NEC will allow troops to be able to act within their structures or a coalition of forces in a way that should be redefined to match the present-day concepts regarding the military operations and architecture of the information systems. Conducting the forces demands integrated C4ISR systems at every echelon. Under the conditions of particular dynamism of the military actions and positions fluidity, the C4ISR systems have to ensure full cover with leadership alternatives of the entire area of responsibility, real time command and control of the available forces and means, as well as efficient logistic support. The implementation of the NCW and NATO NEC concept is seen as a force multiplier, a generator of information and decision superiority, granting substantial growth to the mission efficiency.

4. Assessment of the C4ISR Capabilities Development in the Romanian Armed Forces according to NATO NEC Environment

At this moment, transformation is the most important noticeable fact in the military. It is a key word in NATO and at the same time in the Romanian Armed Forces. Basically, transformation refers to:

- ✓ Reconsidering the nature of military operations, as well as doctrines, skills and assets.
- ✓ Influencing the C4ISR systems, with two general frameworks, namely Network Enabled Capability and Critical National Infrastructure.

The main purpose of the two frameworks is to obtain information superiority, which is one of the fundamental pillars of the NATO NEC concept.

Network Enabled Capability provides better and faster support of the entire operations spectrum. Its most important desired results are:

- Information and decision superiority (the first objective of NATO NEC);
- Information coherence and overall users' interoperability;
- Increased awareness;
- Increased flexibility.

These results become possible only contained by a Networking and Information Infrastructure that brings together sensors, command and control centers, and effectors, regardless they are on land, sea or air.

In our opinion, the basic criteria of NATO NEC are the following:

- Intelligent networks;
- Information management software included in network nodes;
- Distribution of broadband services;
- End-to-end Quality of Services;
- Security solutions distributed evenly in the entire system;
- Users' mobility.

The purpose of the NATO NEC concept is to create intelligent networks able to have an operational contribution to information management and dissemination. This service requires information software management applications included in network nodes, implemented command and control, and administrative applications (Intranet), and large-scale use of graphic and imagery tools.

For these applications broadband services are needed. These services require real time data, i.e., multimedia service with guaranteed end-to-end Quality-of-Service for streaming video, sensors management, effectors control, etc.

This whole environment demands security solutions distributed evenly throughout the system, in order to serve different user communities (information security, registration and authentication of the users, etc.).

And, last but not least, the NATO NEC concept requires the support of the users' mobility, specific systems and technologies that extend voice, data and multimedia services to the fielded units, down to soldier level.

Taking into consideration the second framework mentioned, it is important to emphasize that it started to be consistent after 9/11, having the following basic criteria:

- ✓ Proprietary or dedicated data flows;
- ✓ Network redundancy (grid systems) and different transmission media (radio relay, satellite, optic fiber);
- ✓ Automatic restoration of the users' connections through Multiple Priority and Preemption mechanisms;
- ✓ Operations System Support;
- ✓ Use of on-line certified encryption equipment;
- ✓ Control systems of the access to the public systems.

Network Information Infrastructure is made up of strategic Network Information Infrastructure – National Military Communications Network; tactical Network Information Infrastructure; Functional Area Services, as well as users and missions.

The first implemented element and one of utmost importance is the Permanent Telecommunications Network. This is the infrastructure of the National Military Communications Network.

The Strategic Radio Network is a single channel network based on performing radio equipment designed to provide communication capabilities for service staffs and deployable large units or for generation-regeneration of forces on maneuver, as well as a backup solution to the Permanent Telecommunications Network ensuring mainly data communications. In order to provide supplementary communications capabilities in some areas, there are deployable elements of the Permanent Telecommunications Network mounted on containers or special vehicles.

Each service (especially the Air Force and the Navy) can set up their own specific sub-networks.

To improve the performance of the Romanian National Defense Network, we consider an evolutionary strategy should be adopted. This strategy is basically founded on the following stages:

- ✓ Assessment of the existing systems;
- ✓ Projection of a national Overarching Architecture;
- ✓ Development of necessary Reference Architectures and Target Architectures;
- ✓ Design of the Roadmap for Target Architectures.

The stages already started to be approached according to the operational requirements and available funds.

Today, the Permanent Telecommunications Network represents the infrastructure of the National Defense Network that is used by all the structures of the Romanian Armed Forces. Over this communications system there were accomplished: the military INTRANET system (INTRAMAN), encrypted video-conference system, specific naval forces applications (ARGUS), environmental applications, etc. At the strategic level, these networks represent the pillars of the Network Information Infrastructure. The development concept of the National Defense Network will allow the evolution toward a component of the NATO network confederation. The current performances provide operational capabilities and interconnection with other networks with certain limitations. In our opinion, the most important fact is the permanent commitment for the improvement of these capabilities.

The strategic Network Information Infrastructure supply communications in support of a significant number of functional applications, such as: the National Air Command and Control System (including sensors connections – FPS117, GAP FILLER and radars and updated analogical vectors – air bases, Soil-Air Missiles, electronic warfare units), NBC Surveillance and Warning System, National Integrated Meteorological Information System, Maritime Complex Observation System (SCOMAR), Military INTRANET, etc.

Today, the Permanent Telecommunications Network is an enhanced EUROCOM system based network with EUROCOM, STANAG and commercial (ITU-T) gateways to other networks. All of these ensure a high level of interoperability with commercial (ITU-T), and tactical (STANAG and/or EUROCOM) networks. The Permanent Telecommunications Network is also interconnected with NATO General Communications System (NGCS), and with the Italian National Military Communications Network using the SICRAL satellite system. In the future, the Permanent Telecommunications Network will provide services to NATO users on Romanian territory. Furthermore, there is possible to interconnect the Permanent Telecommunications Network with other nations' tactical networks.

The Strategic Radio Network is intended to provide minimum voice, data and link capabilities for all tactical and operational units HQs, when other means of communication cannot be used. This network is employed at the level of the services' HQs, for tactical and operational units (mainly for the units made available for NATO operations). The communications provided are protected to interception and jamming with incorporated crypto devices and frequency hopping equipments. The Strategic Radio Network has integration capabilities with INTRAMAN messaging services.

Major services offered by the military INTRANET or INTRAMAN, as well as the information systems which use it as support infrastructure are:

- Basic information services (electronic mail, files and printing, WEB, hierarchical activity management, hierarchical documents flow management, etc.).
- Support for operational information systems:
  - Support Information System of the Military Actions (SISAM)
  - Defense Intelligence Information System (SIA)
  - Modeling and Simulation Information System (SISMIM)
  - Weapon Systems (SISARM)
  - Assisting Military Education Information System (SIMIL)
  - Integrated Logistic System (AILS)

There are Out Of Area extensions of the Romanian National Defense Network to support our deployed troops in overseas operations. There are also extensions for the Romanian Ministry of National Defense representations to NATO, ACO and EU. These extensions provide voice, data and VTC services.

5. Expansion of Romanian Armed Forces' Defense Capabilities by Implementing Integrated Technologies to Ensure Flexible and Multifunctional Capabilities

The operational needs that can be defined for a defence common network are:

- Connectivity for all involved segments: political level, military at all levels, international coalition like NATO, EU and others
- Access to the network to meet criteria like flexibility, simplicity and security, in-country or out-of-area, in order to allow the users to exploit the network:
  - From fixed sites through military, governmental or commercial infrastructure;

- From fixed sites via deployable CIS/CCIS assets;
- From mobile assets/commands/units via connections set up by means of remote access services.

One of the most important technical requirements for the National Defense Network is to comply with the most relevant standards to ensure interoperability. The network topology has also to grant suitable flexibility, survivability and streamlined services integration according to users' needs. The network should also support different services / applications / functions and the relevant information flows, granting both autonomous and common operations, integration and data exchange when required by specific services or applications.

No less important is the employment of the latest technologies such as Software Defined Radio, Secure Communication Interoperability Protocol, and TACOMS Post 2000, etc.

The National Defense Network should provide support for:

- Network interconnecting services
- Core services
- Functional areas services for human resources, reconnaissance, operations, logistics, planning, geo-meteorological, and simulation, etc.

This approach is similar to NATO's approaches used for the development of NATO Bi-Strategic Command Automated Information System, Deployable CIS, and NATO General Purpose Communication System.

Within the described scenario, an evolutionary process leading to a "network based" capability within an acceptable timeframe is of utmost importance. To this aim, actions should be concentrated on the implementation of a "Common Network" by taking advantage of the recent procurements and by optimizing and integrating systems, already in use or to be introduced in use in the near future. Under the assumptions on targets made, the following requirements will lead the process:

- Support of broadband services (multimedia integrated services);
- Optimization of the available transmission bandwidth;
- Upgrade / implementation of access networks;
- Increase of network security through NATO approved encryption systems, and NATO security concepts (i.e. multilevel security);
- Upgrade of existing or introducing new IT platforms to support core services;
- Increase of integration with the achievement of out of area seamless support through satellite bearers, and high capacity connectivity to mobile assets;
- Enhanced interoperability between National Defense Network and NGCS;
- Increase of automation and control functions to replace reduced manning.

These requirements lead to final objectives achievement:

- Building a secure and highly survivable network;
- Full integration of both strategic and tactical network components;

- Network architecture and adopted technologies able to optimize the capabilities regarding the efficiency and management;
- Evolution of services.

Starting from the present situation, a sequential action plan could be defined in order to build a common network for the Romanian Armed Forces. The services provided by the network are core services and functional area services, in accordance with the concept of Bi-Strategic Command Automated Information System. Core services are fairly well extended in the network, and in our opinion the main issue is represented by less developed services dissemination to all the users.

In the Functional Area Services, Romanian Armed Forces are in the stage of efforts and funds investments. These activities are driven by the need of real time information exchange between effectors and sensors, as well as by specific services for different missions. The services will be provided starting from core area toward specific areas as national users, NATO users, users from different coalitions, and participants to abroad missions.

For a short time perspective, we believe that Romanian Armed Forces will focus their efforts on integration of existing systems and introducing only integrated subsystems, or subsystems with integration capabilities into the existing network.

The Romanian Armed Forces are in the process of testing and finalizing the integration activities of new Electronic Warfare System - the program Azur, and Weapon System - Hawk XXI. Also, there are two main programs for services – SCOMAR – surveillance and reconnaissance system for the Naval Forces Staff and SCCAN – command and control system for the Air Force Staff.

For the near future ambitions are higher. Because of the highly demanding capacity of new information systems, the Romanian Armed Forces will concentrate efforts for up-grading the existing infrastructure by introducing high-rate supports. For some areas high capacity fiber optic area networks will be realized. In order to increase the processing capabilities, multi-protocol – multi-service switches will be introduced.

Furthermore, the efforts will be focused on:

- ✓ Integration of the legacy systems made through specific gateways that will not limit the performances.
- ✓ Use of software defined radio that will be extended for all services and all type of communications. Radios with these capabilities are already in use.
- ✓ Setting up a global network management system.
- ✓ INFOSEC area, protecting the information and the systems being another major task. IP encryption is to be used as a standard solution.
- ✓ Sensors integration and use of smart sensors.

Conclusions

The Romanian Ministry of National Defense has started different up-grade programs, many of them at lower echelons, due to the commitment level at the programs' initiation moment. Currently, this commitment involves higher echelons, because it became

obvious that because the lack of coordination these systems could be hardly integrated at brigade level.

Analyzing this situation, the Communications and Information Directorate from the General Staff, with the Land Forces Staff support, decided that the only way to solve all the aspects regarding integration is to start a process of defining the C4ISR system at brigade level. The reason for this decision is that a multilevel, flexible and operational C4ISR system is potentially the most important force multiplier for overall battle space.

In order to develop a competitive C4ISR system, we believe that the architecture recommended in NATO C3 Systems Architecture Framework is the best approach. As basic technology battle space digitization and fundamental idea is C4ISTAR concept are adopted. No less important is the coordination with interacting programs.

The development and use of operational, digital and mobile communications to provide reconnaissance, command and control data to the soldier are based on operational requirements, and technological, time and budgetary constraints.

The C4I system should provide command support for all levels. All weapon systems have to be integrated. Mobility is a basic feature for all tactical systems. Protection is the key behind which security, electronic countermeasures, and data encryption lie. Communications support should provide enough capacity for command and functional services' support. Nonetheless important, the system must ensure interoperability between national and international areas, within the North Atlantic Alliance or with the military structures of the member nations of the European Union.