COMMUNICATION AND INFORMATION SYSTEMS ORGANIZATION FOR CRISIS MANAGEMENT AND CRITICAL INFRASTRUCTURES' PROTECTION WITHIN THE FRAMEWORK OF THE EUROPEAN UNION'S COMMON SECURITY AND DEFENSE POLICY

Major General (ret) Professor Constantin MINCU, PhD [*]
Dănuț ȚIGĂNUŞ [**]

This paper briefly presents the study of operational planning processes within the European Union institutions' framework, the analysis of undergoing projects on Communication and Information Systems; the Romanian army's contribution in the EU-led missions and national projects for C2 support; the experience of national detachments and expert groups in EU. Also, we will try to draw an inventory of lacks and constraints of interoperability inside and between the European and national systems and to analyze the lessons learned on the missions taking place under the European Union aegis.

Keywords: *European Union; CIS; C2; crisis management.*

Introduction

The European Union's concerns in order to vividly confront the multiplication of risk factors and some new and violent threats have intensified in the last few years.

As beneficiaries of some developed countries' experience (multiple lessons learned from previous political, economic-financial and military actions), the USA, and NATO as well, are trying to organize their institutions and systems for intricate situations likely to appear in the European space as well as in the neighboring areas.

[*] Full member of the Romanian Scientists' Academy, scientific secretary of the Military Sciences Section, member of the Romanian Scientists' Academy Honor Council (mincu_constantin@yahoo.com)

[**] Chief of CIS Resource Planning Bureau in Communication and Information Technology Directorate of the General Staff

Special attention is given to **"Communication and Information Systems for Crisis Management and Critical Infrastructures' Protection".**

Our paper tries to synthetically present some main aspects of planning, accomplishment and use of communication and information systems for the support of institutional and operational framework to put into practice the **Common Defense Security Policy (CSDP)** in the European Union, consequent to the introduction of stability and security for those systems' elements under the information era challenges.

1. Crises and their management within the European Union's Common Security and Defense Policy framework

Many experts willingly **consider** EU is not anymore an exclusively economic organization, as it increasingly plays its role as local and regional crisis' manager, develops procedures, rules and means for the identification, classification and protection of critical infrastructures on its territory.

Institutional and operational process of action in crisis situations is undergoing and, against this background, the estimation of information flows and architectural framework for support systems as the communication and information systems (CIS) for the complex processes of command & control (C2).

EU structures' specialists, as the ones from the member-states, intensively and carefully analyze (owing to the present day context as regards its political, economic, financial, juridical, diplomatic and military issues) the following areas:

- **Contemporary crises in the security field:**

- Contemporary crises and types of crises;
- Common Foreign and Security Policy as well as the long term development trends;
- Implementation of the European Security Strategy in the field of common and national crisis management and critical infrastructures' protection;

- **Crisis management by EU-led missions in the CSDP framework, by the participation and engagement of the member-states on military and civilian capabilities and forces issues:**

-Development of EU crisis response capacity and settlement of this organization's missions set as well as of the needed forces for them;

-Clarifying and gradual implementation of planning process and decisional mechanism at European strategic level for crisis management and critical infrastructures' protection (i.e., institutions, bodies, procedures, rules, commitments, etc.);

- **Command and control of forces used by EU for crisis management:**

-Crystallization and implementation of EU Conception regarding the military and civilian actions' command and control (political control, strategic guidance, comprehensive approach, *ad-hoc* chain of command, multi-nationality, unity of command, unity of effort and flexibility);

-Organization and functioning of military HQs for EU operations command, inclusively resources for Communication and Information System (who, with what and to which level it needs to provide specific personnel and equipment).

- **Clarification of some aspects concerning the national contributions to the crisis management and critical infrastructures' protection:**

- NATO's efforts to remain unduplicated;

- Correct and complete understanding and processing of trends regarding France, Germany and Great Britain's contributions to CSDP and Romania's positioning along this process;

- Settlement on real bases of human, material, financial or other nature potential of Romania's contribution to the implementation of the Common Security and Defense Policy and to possible actions.

2. Requests and principles regarding communication and information systems' planning and accomplishment for crisis management:

- **factors influencing communication and information systems' planning and accomplishment are identified and analyzed,** such as:

- Robust connection of participants, military and/or civilian forces;
- data and information collection, processing and dissemination;
- Fulfillment of the capability for a common understanding of the real situation;
- Growth of operational efficacy by information efficiency.

Area specialists consider the previously mentioned desiderata fulfillment depends on some factors influencing the process of CIS planning, projection, accomplishment, implementation, deployment on the theatre of operations and use in the support of EU missions (Annex no. 1), as follows: command and control systems' interoperability, including the supporting CIS; researche results and EU projects for Common Security and Defense Policy support; Lisbon structural transformations; EU – NATO relation as regards cooperation in the CIS projection, fulfillment and implementation field for the support of crisis management operations; operational factors.

- **CIS planning for crisis management and critical infrastructures protection within the SCDP framework:**

- Existence of an integrated architecture of communication and information systems is considered mandatory to assess the information superiority throughout the mission fulfillment;

- Definition of information exchange requests at strategic, operational and tactical levels within the EU missions' framework;

- Crystallization and application of a set of requests and principles regarding the operational planning process (selection of the option, Initial Military Directive elaboration, elaboration of chapters concerning CIS and adjacent annexes, etc.).

• **Organizational and architectural framework to accomplish CIS in support of EU missions for crisis management:**

- CIS architectural framework in EU is identified as the same as the one defined by NATO as NAF (NATO Architecture for C.3 and V.3 systems)[1], this being a major advantage for national CIS projection submitted to the forces' disposition able to act alternatively under both organizations' aegis.

• **EU and member-states CIS structure and functions:**

- The structure comprises: Communication and Information System with fixed infrastructure, Communication and Information System for surveillance and early warning; deployable Communication and Information System and Communication and member-states' Information Systems;

- Structurally speaking, CIS is set up as seen in Fig. 1. EU specialists and decision-makers consider it will have a modular and scalable composition, being organized in communication and information permanent centers (CIPC), located in Brussels and member-states' capitals, communication and information operational centers (CIOC), both fixed and deployable, supporting or terminal, from the level of operational HQs (OHQ, FHQ; forces' components or GTL), lines of communication (LC) on various information transportation media;

- All above-mentioned elements will be integrated in the information transport infrastructure by two levels of classification: EU SECRET and EU RESTRICTED (EU extended area secured network), which will have as basic application the secret level mail system – CAMEO (software application of collaboration in the crisis management network).

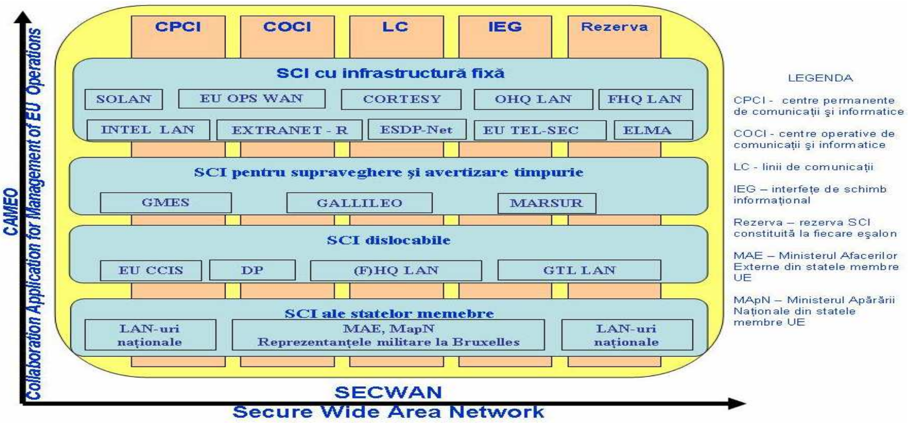

CAMEO
Collaboration Application for Management of EU Operations
CPCI
COCI
LC
IEG
Rezerva
SCI cu infrastructură fixă
SOLAN
EU OPS WAN
CORTESY
OHQ LAN
FHQ LAN
INTEL LAN
EXTRANET - R
ESDP-Net
EU TEL-SEC
ELMA
SCI pentru supraveghere şi avertizare timpurie
GMES
GALLILEO
MARSUR
SCI dislocabile
EU CCIS
DP
(F)HQ LAN
GTL LAN
SCI ale statelor memebre
LAN-uri naţionale
MAE, MapN
Reprezentanţele militare la Bruxelles
LAN-uri naţionale
SECWAN
Secure Wide Area Network
LEGENDA
CPCI - centre permanente de comunicaţii şi informatice
COCI - centre operative de comunicaţii şi informatice
LC - linii de comunicaţii
IEG – interfeţe de schimb informaţional
Rezerva – rezerva SCI constituită la fiecare eşalon
MAE – Ministerul Afacerilor Externe din statele membre UE
MApN – Ministerul Apărării Naţionale din statele membre UE

Fig. Main Document Only. Components of communication and information system for crisis management (structural approach)

nto account the mission's specific and extended, information exchange requests for command,

[1] European Defence Agency, *Network Enabled Capability Implementation Study*, EU NEC Vision third report, Brussels, 09.02.2010, p. 23.

control, information, surveillance and reconnaissance, cooperation needs in the theatre of operations, as well as the HQs emplacement in the field. Basic services are main network services, interoperability services, security services, management services, communications services;

- **Functional services** can be provided for: joint forces' command and control; land, air and naval forces' command and control; logistics; information; other functional services;

- Taking as a basis the functional analysis of a CIS generic system, the following functions are identified: interface with the user; conference facilities; regional radio coverage; public notice or announcing; information provision; circuits commutation; packages commutation; transport in the local network; data transfer capacity management, interface with dispersed users, external transmissions, of security, ambient infrastructure, network management, of interconnection.

3. CIS use along the EU-led missions for crisis management and critical infrastructures protection:

• CIS for early warning and strategic planning:

- There are ideas, that, in order to fulfill CIS for early warning, three types of information flows will be analyzed and considered by taking into account the command and control options for the mission: basic information law for routine information, information flow for information in EU-led autonomous operations, information flow for information in Berlin Plus (the existent situation regarding CIS for CSDP application is generically presented in Annex 2);

- From the analysis of the actual systems of communication and information available in the EU, we can draw the conclusion that at present they have a low level of interconnectivity, many breeches making necessary the information manual transfer and a much too high level of classification which, not at all times meets users' requests and, more importantly, there is no unique infrastructure for the automatic interconnection of CSDP institutions with the operational decision-makers from member-states' capitals.

• Deployable CIS use for crisis management support within CSDP framework:

- Accomplishment of a common infrastructure of network for information exchanges at all levels and implementation of some specific measures to increase the systems and services' viability throughout the EU-led missions;

- This common infrastructure of network presumes LANs interconnection of strategic level military structures (OHQ) with the operational (FHQ) and tactical level ones;

- Many experts regard deployable CIS viability and structure elements as dependant on their structure, on how dispersed are the component elements, how much is provided of the reserve and technical solutions adopted for information flow transport. Another influence factor specific for EU predictable mission is the level of dependency, at the operational and tactical levels, by the telecommunication infrastructure provided by host nation's public operators.

- **Aspects concerning CIS missions under the conditions of Network Eased Capabilities (NEC):**

- EU considers NEC represents „the ability to set up a unitary environment for a comprehensive approach and the efforts' unification of military, civilian and all the actors, at all levels, in the EU-led operations for crisis management"[2];

- Some estimate NEC will be implemented as soon as the premises for the implementation of a federalized infrastructure for exchange of data, information and information services in the support of EU-led missions has been created.

- **Use of communication and information systems to support operations in computer networks and cyberspace defense:**

- Operations in computer network are defined as "deliberate actions performed for IT network, computers and other electronic equipment optimization aiming to gain and maintain information supremacy concomitantly with the decrease of the adversary's capacity to act in this regard";

- At EU level, the Computer Network Operations (CNO) is under CSDP control but it has not yet been fully legally settled although there some specific measures have been taken in EC framework by the introduction of Directive 2006/24/EC regarding the abstention of data generated or performed by electronic communication services dished to the public[3].

- **Harmonization of national efforts to use the communication and information systems in support of crisis management:**

- It is considered necessary to appoint, on hierarchical levels, an **Officer Coordinator for Information Management (OCIM);**

- Improvement of EU military and special development organizational framework;

- Identification of some opportunities concerning the Romanian Armed Forces participation in CIS development for EU needs (the Romanian experience in Afghanistan SEEBRIG mission and also some Romanian specialists' value proved in NATO, UN, EU missions should be considered in this respect).

4. Stability in communication and information systems functioning and security throughout EU-led missions:

➢From the civilian authorities' perspective, any international confrontation, on different levels and causes, attracts a multiplication of the force balance while on the military level there is an apparent limitation of those (military power restriction due to the decrease of the violent character of confrontations). These principles practically manifest under the context of the missions undergone for crisis management as vulnerabilities damaging own

[2] EDA, EU NEC Concept for NEC in support of ESCD (12737/08 + COR1), Brussels, 2008, p. 3.

[3] Comisia Europeană, Directiva UE 2006/24/CE, publicată în Jurnalul oficial al UE (JOUE), nr. L.105, din 13.04.2006.

communication and information system's stability and security, as a whole, and, to a certain extent, the stability of its functioning elements.

- **Communication and information systems' stability during the EU-led crisis management missions:**

- Stable functioning presupposes some multilateral measures' adoption to provide stability under the conditions of a multitude of random factors able to be estimated but not exactly found out and the presence of disturbing actions by destructive factors performed by the enemy;
- Communication and information systems' analysis mainly means to respect the basic rules such as: modular global approach; profitability; orientation toward users; assessment of the unique process of data introduction; general and independent solution for the system's configuration; possibility of further development;
- Calculation by complex mathematical means of CIS stability;
- Calculation on statistical and probabilistic bases of CIS availability (availability is defined as the probability of a CIS element to be able to provide the functional capacity requested by users);
- Organizational structures and information flow stability presupposes identification of specific measures to provide organizational structures' stability by enforcing the approach of many relatively distinctive fields such as: continuity of command and control processes and leadership capacity; use of technical means and functional structures' liability; stability to jamming and electromagnetic disturbances; mobility of equipment and of structural elements;
- Settlement of principles and requests on information provision;
- Identification and putting into practice of solutions for the harmonization of national efforts to assess information traffic during EU-led missions;
- Insurance of CIS security by organizational and technical measures during EU missions' preparation and development;
- Elaboration and strict observance of some principles concerning CIS security ;
- Accreditation on scientific principles of CIS security standards;
- Careful multi-criterion study of some challenges against CIS security under the network eased environment.

5. The authors propose some measures for EU and national authorities:

- Crisis management missions' command and control by setting up a permanent C2 structure and a unique strategic military command in Brussels;
- Provision of support systems by the unitary approach of CIS problems in EU;
- CIS stability and security by applying unique standards of functioning and security;
- Efficient exercise of information security risk management;
- Implementation, with more force and efficiency, in the Romanian Armed Forces, of NATO and EU CIS procedures;

- Identification of some organizational and technical measures to increase CIS deployable operational and tactical efficiency;
- Information management implementation in all EU systems, networks and services.

* * *

In conclusion, we propose the following major guidelines of development as concerns CIS field designed to support EU-led missions for crisis management and critical infrastructures protection:

- To revise the operations' concept and their proper particularization to increase the straightforwardness and to avoid the misunderstandings on their implementation during the missions;
- To standardize processes and rules at all the operational levels;
- To develop and implement CIS in conformity to operational scenarios;
- To define interconnection architectures for the existent networks and to create common infrastructure for C2 chain;
- To revise levels of classification of networks and to define some common compulsory requests as CIS concerns for EU and member-states.

NOTES

A. Official documents

[1] Council of the EU, *Suggestions for procedures for coherent, comprehensive EU crisis management*, No. 11127/03, Brussels, 2003.

[2] European Defence Agency, *Draft technical Specifications for C4I Reference Architecture EU Battle Group (C4I RA EU BG)*, version 4, PROV 10-CAP-012, Brussels, 2010.

[3] *NATO Network Enabled Capability – Feasibility Study*, Vol II, Detailed Report Covering a Strategy and Roadmap for Realizing an NNEC Networking and Information Infrastructure (NII) v.2.0, NC3A, Brussels, 2005.

B. Author works

[4] Alberts S.D., Gartska J.J, *Network Centric Warfare – Developing and Leveraging Information Superiority,* Centre for Advanced Concepts and Technology C4ISR, Washington, D.C., 1999.

[5] Alexandrescu C-tin, Ilina D., Mincu C-tin, *Bazele matematice ale orgaizării sistemelor de transmisiuni*, Editura Militară, Bucureşti, 1994.

[6] Frunzeti T., *Considerații asupra participării Armatei României la acțiuni colective*, Editura Universității Naționale de Apărare „Carol I", Bucureşti, 2006.

[7] Gya G., *ESDP and EU Mission Update,* European Security, Brussels, 2007.

[8] Merlingen M., Ostrauskaité R. (ed.), *European Security and Defence Policy – An Implementation Perspective*, Routledge, Abington, 2008.

[9] Timofte G, Tudose E., Constantin G., *Protecția informațiilor în sistemele de comunicații militare moderne*, Editura Inedit, Bucureşti 2006.

C. Publications

[10] Bomqvist P., *CIO Target document for Networking and Information Infrastructure (NII)*, Swedish Armed Forces, Stockholm, 2009.

[11] Domingo A., Wietgrefe H., *TN-1009, NATO Deployable CIS Target Architecture Document*, Edition 2.0, NC3A, The Hague, 2004.

[12] Frunzeti T., *Gestionarea crizelor în războiul rece*, Lumea Militară, nr. 1, Bucureşti, 2006.

[13] G. Gamow, Z. Phys. **51**, 204 (1928).

[14] D. Forster, *Hydrodynamic Fluctuations* (Benjamin, New York, 1975) Vol. I, p. 25.

[15] P. Ring and P. Schuck, *The Nuclear Many-Body Problem* (Springer-Verlag, Berlin, 1980).

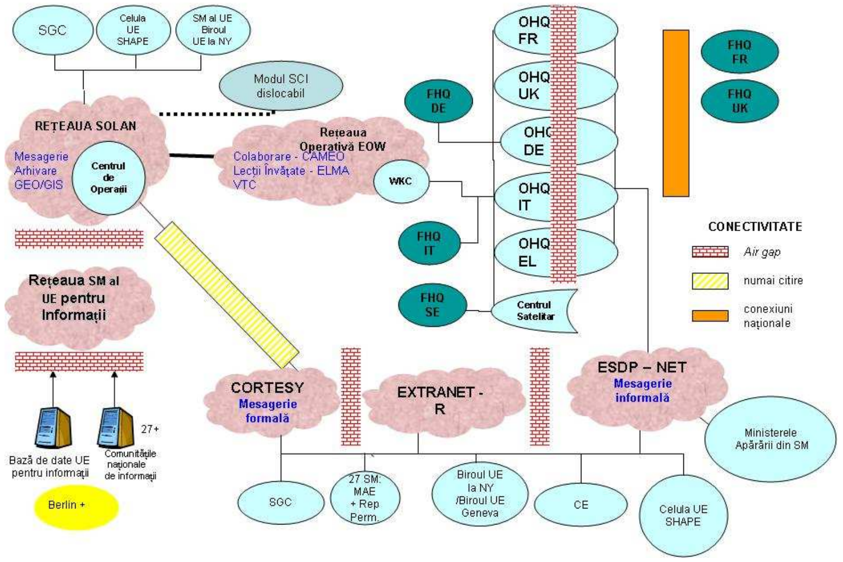
[16] A. Sandulescu and O. Dumitrescu, Phys. Lett. B **24**, 212 (1967).

[17] E. S. Paul *et al.*, Phys. Rev. C **61**, 064320 (2000).

[18] V. G. Soloviev, *Theory of Atomic Nuclei* (Institute of Physics Publishing, Bristol, 1992) pp. 123-125.

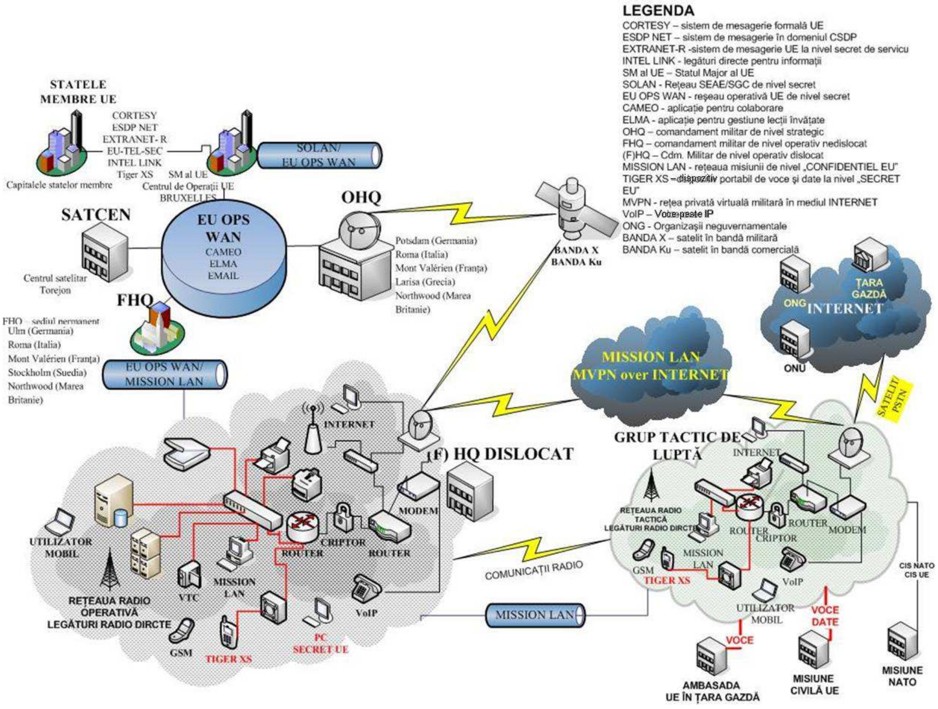
Annex 1

COMMUNICATIONS AND INFORMATION SYSTEMS AT THE STRATEGIC POLITICAL-MILITARY LEVEL FOR PSAC MISSION SUPPORT



Annex 2

UTILIZATION OF THE COMMUNICATIONS AND INFORMATION SYSTEM FOR EU MISSION SUPPORT AT THE THEATER OF OPERATIONS LEVEL



LEGENDA

CORTESY – sistem de mesagerie formală UE
ESDP NET – sistem de mesagerie în domeniul CSDP
EXTRANET-R -sistem de mesagerie UE la nivel secret de servicu
INTEL LINK - legături directe pentru informații
SM al UE – Statul Major al UE
SOLAN - Rețeau SEAE/SGC de nivel secret
EU OPS WAN - reşeau operativă UE de nivel secret
CAMEO - aplicație pentru colaborare
ELMA - aplicație pentru gestiune lecții învățate
OHQ – comandament militar de nivel strategic
FHQ – comandament militar de nivel operativ nedislocat
(F)HQ – Cdm. Militar de nivel operativ dislocat
MISSION LAN - rețeaua misiunii de nivel „CONFIDENTIEL EU"
TIGER XS – dispozitiv portabil de voce şi date la nivel „SECRET EU"
MVPN - rețea privată virtuală militară în mediul INTERNET
VoIP – Voce peste IP
ONG - Organizaşii neguvernamentale
BANDA X – satelit în bandă militară
BANDA Ku – satelit în bandă comercială