COMMUNICATIONS AND INFORMATION SYSTEMS IN SUPPORT OF EUROPEAN UNION-LED CRISIS MANAGEMENT MISSIONS

Dănuț ȚIGĂNUȘ

"Carol I" National Defense University, Bucharest, Romania

This essay assesses the communications and information systems (CIS) in support of the civilian and military structures deployed in the European Union led crises management operations and missions. The article emphasizes the specific structure and function of CIS taking in consideration the particularities of EU led missions. The integration of the EU institutional networks and systems with the national systems provided by the EU member states is considered a key element. The analysis-part of this paper starts with the specific EU command and control system for crises management missions based on two autonomous solutions and one relying on NATO capabilities. Further, it continues with the challenges of the classified information exchange at the operational theatre level. The most important contribution of this article is based on the long term vision implementation measures for the CIS structure, roles, functions and services provided and the information management infrastructure. CIS deployment mechanisms are described with references to the practical situation of the CIS deployed in support of crises management operations and missions. Two important definitions are provided regarding the CIS for crisis management and their roles in the specific EU operational environment. The system view of the operational CIS is depicted and analysed also, with a focus on the integration aspects of the infrastructure as the information transport layer for the information exchange flow. The last part of the article focuses on the CIS functions for the deployed systems which are detailed alongside with the C2 and Information Exchange Requirements in the EU operational environment. The variety of the theoretical approaches to determine the CIS infrastructure for EU-led civilian and military missions triggers the conclusion that the planning and implementation process is extremely complex especially in the context of the new security environment and requires national participation and adaptation of the national and institutional development programs in the CIS field.

Key words: *Communications and Information Systems (CIS), EU Common Security and Defence Policy, Information Exchange Gateway, Operational Headquarters (OHQ), Force Headquarters (FHQ), crisis management, EU-led missions.*

Unlike traditional military operations conducted by NATO or national armed forces in coalition operations, the diversity of operational scenarios in which communications and information systems (CIS) can be used for crisis management missions led by the EU produces an

essential element of specificity in the planning, implementation and use of these systems.

On the other hand, the different nature of command and control system in the Common Security and Defence Policy (CSDP), based on the ad-hoc solution chosen by the political decision-factor for each operational scenario and depending on the availability of the Member States to accept one of the seven existing command and control possibilities for EU-led operations, entails the establishment of similar CIS specific solutions from case to case. Mention should be made that five of these possibilities are offered by the United Kingdom, France, Germany, Italy and Greece, as strategic operational command posts (Operational Headquarters - OHQ) provided by a framework member state. Another option is implemented through EU Cell at SHAPE based on a Berlin Plus operation and resorting to NATO command and control capabilities. The EU Operation Center in Brussels could be activated by EU External Action Service and this is the third C2 option for an EU-led Crisis Management Operation.

The planning process shall apply to support the military strategic, operational and tactical headquarters and the institutional administrative and management system, including information exchange between these commands.

The same happens with the CIS in support of the civilian missions, the difference consisting in that the strategic management is carried out by the Civilian Planning and Conduct Capability (CPCC) which, acting as an operational command for all civilian ongoing EU-led missions, has continuously available communications and information systems to achieve the internal information flow and the communications with the operational theatres. In this case, the major problems of planning, deployment and implementation of the related CIS are related to the strategic communications with the operational theatres and, in particular, to the creation of the infrastructure in theatre for specific support of these missions.

It is important to note that the CIS for crisis management operations have to support both the functional and operational requirements, and the technical requirements (i.e. systems availability, efficient use of the hardware and software, availability of information, information security and interoperability with other similar systems).

To understand the organizational and procedural planning framework for communications an information systems in support of EU-led Crisis Management Operations (CMOs) we must first define their concept, role, structure, functions performed, criteria of engagement into the mission and the responsibilities of the specialised personnel in the operational environment.

Thus, the communication and information system for crisis management under Common Security and Defence Policy is defined, from a conceptual perspective, as a set

of basic and functional distributed components, organically interacting under the action of the human factor. Its primary objective is to facilitate the monitoring, early warning, operational planning, command and control and decision making processes in order to identify the measures, methods and procedures designated to bring a crisis situation under the national or international forces control and to allow the conduct of coordinated actions using civilian and/ or military instruments to return the situation back to normality.

Regarding the role of CIS, the literature in the field covers the following aspects: the role of staff and personnel, the operating procedures, the information management mechanism and the physical infrastructure needed for the support of decision making together with the aspects of planning, preparation, execution and evaluation of operations (Burlacu: 2007).

The EU institutions are involved in the monitoring of the operational situation in the area affected by the crisis and are responsible for the planning, preparation, execution and evaluation of a mission for crisis management. The EU Member States will provide the Headquarters, forces and the military and/or civilian means for deployment and intervention in the field. These forces must be supported by the CIS to perform efficient information flow directed at all hierarchical levels, from the political-strategic level down to the tactical level in the operational theatre.

The EU specificity requires a comprehensive approach in providing the SCI for the exchange of information between civilian and military entities acting for crisis management, in order to coordinate their efforts and the efficient use of all instruments that EU decides to commit to specific management of a crisis.

This approach is different from what is the Civil-Military Cooperation (CIMIC) or the corresponding principle of cooperation between NATO military forces and other forces or NGOs acting together to achieve desired effects and the operational objectives in a broader theatre security framework.

Hence, the role of the CIS in support of the crisis management practiced by the EU is to ensure the timely and effective information exchange within the command and control, cooperation and monitoring given its capacity to support the conduct of military and/or civilian action in the mission, the extension of the communication and information system from the permanent locations to the deployed locations outside the EU territory, and to ensure the necessary redundancy in order to allow the channels and services manoeuvre.

Communications and information systems will be based on complex, coherent and integrated network architecture, from commercial sources, national military and/or belonging to the EU, supported by a robust and sufficient infrastructure

which is formed from a series of mixed terrestrial and satellite communications in order to provide broadband capabilities for collecting, processing and disseminating data and information.

Based on this architecture, we can determine the structure of communications and information system for UE-led CMOs. This includes:

a) CIS with fixed infrastructure, consisting of the federalisation of the following components: IOLAN (Intranet Office Local Area Network - unclassified), SOLAN (Secure Office Local Area Network - classified), EU OPS WAN (EU Operation Wide Area Network), ESDP-NET (European Security and Defence Policy Network - formal messaging system for EU security and defense issues), Cortesy (COREU Terminal Equipment-general messaging system between communications centres), INTEL LAN (Intelligence Local Area Network), Extranet R (classified messaging system between EU and Member States), EU-TEL-SEC (EU encrypted telephone system), the OHQ and FHQ LANs in the permanent location.

b) CIS for surveillance and early warning: GMES (Global Monitoring for Environment and Security), Galileo (Global Navigation Satellite System), MARSUR (Maritime Surveillance System).

c) Deployable CIS consisting of: Operational Headquarters (OHQ) LAN, Deployed Force headquarters - (F)HQ, Deployable Packages (DP), EU command and control system (EU CCIS) and the CIS elements of the deployable Battlegroups (BGs).

d) CIS of the Member States: national integrated systems in support of crisis management, belonging to Member States.

The structure of the communications and information system for crisis management operations is presented in **Figure 1**.

The CIS for EU-led CMOs will have a modular and scalable structure, being organised with permanent communications and information centres (PCIC), installed in Brussels and in the capitals of the Member States, operational communications and information centres (OCIC), fixed and deployed, transit or end-user set up in the operational headquarters (OHQ, FHQ, components or BGs forces) and communications lines (CL) achieved in various transport media information (optical fibre, copper circuits, radio, radio relay, satellite).

This architecture will support the operational command and control (C2) option established at political-strategic level, and will provide the information exchange gateways for interconnection of the classified networks and domains as well as the CIS spare part usually established at 10% of quantitative active network equipment and terminals.

Based on this vision all elements will be integrated on the communications infrastructure

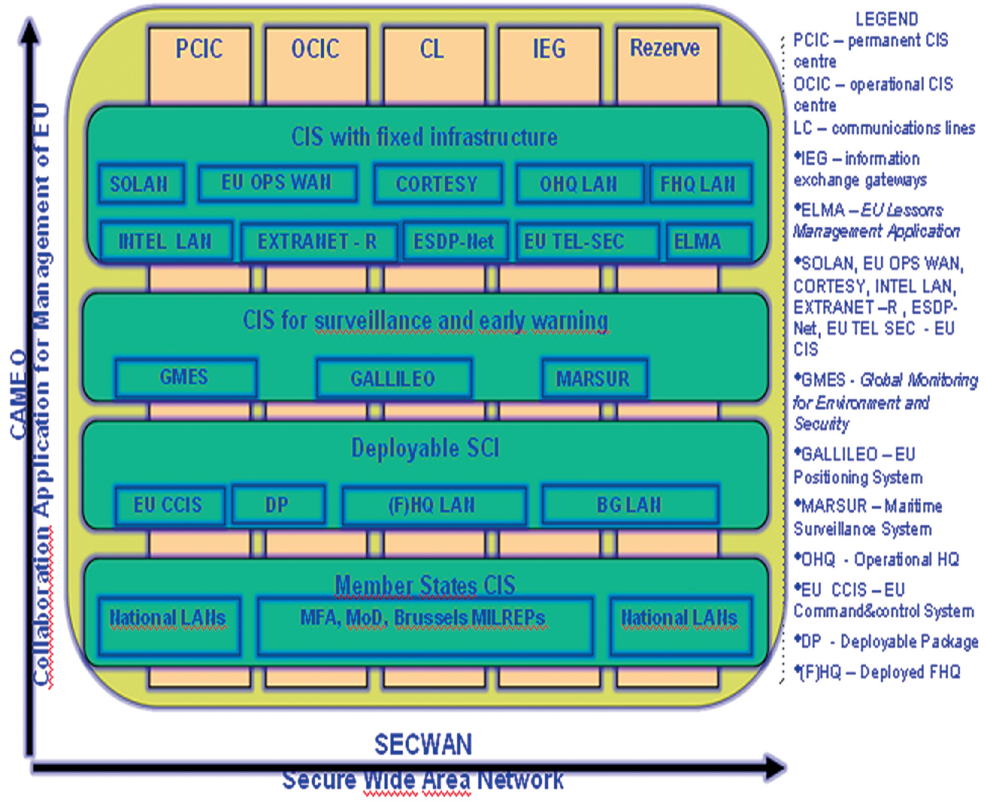

Fig. 1. *The structure of the CIS for EU-led Crisis Management Operations*

transport layer containing two classification domains, SECRET UE and RESTREINT UE. Both domains will be integrated on the EU SECWAN (EU Secure Wide Area Network) which is using CAMEO (Collaboration Application for Management of EU Operations) as a collaboration application for planning of EU-led operations.

From physical implementation perspective the CIS in support of CMOs are formed from three basis elements, as follows:

- Integrated network infrastructure for voice, date and VTC services. This infrastructure facilitates information flow and generates the optimal conditions for data exchange between various actors in the field;

- Hardware equipment as servers, terminal work stations and active network equipment needed for the system to maintain its operational status;

- Software elements: operating system, databases and applications, the logical storage and the client core and functional applications.

In terms of organizational structures, the implementation of efficient communications and information units, sub-units and formations should be based on scientific studies results (Timofte G, Tudose E., Vişan D: 2006, p. 70), as their set up will take into account the following elements:

- operational and technical conditions of employment of CIS in support of crisis management mission;
- experience and lessons identified from completed or ongoing operations in terms of CIS organizational structures;
- the number of users in the permanent and deployable command posts;
- the skills and knowledge of users and specialized technical assistance requirements during the CIS support;
- the number and the field deployable command posts;
- the time to install, make available and redeploy the CIS;
- the staff necessary to maintain viability, reliability and stability in the functioning of the CIS in terms of the engagement;
- the traffic volume estimated at maximum load times of the information flow;
- the need for interconnection with other communications and information systems, governmental structures or security units acting simultaneously in the operational theatre.

It is considered that for the installation, operation, removal and redeploy of the CIS in support of crisis management missions conducted by a brigade, there is a need to engage a CIS structure equivalent to a company, and for a battalion level there is a need for a platoon CIS level.

CIS will have modular structures and composition and will be organized

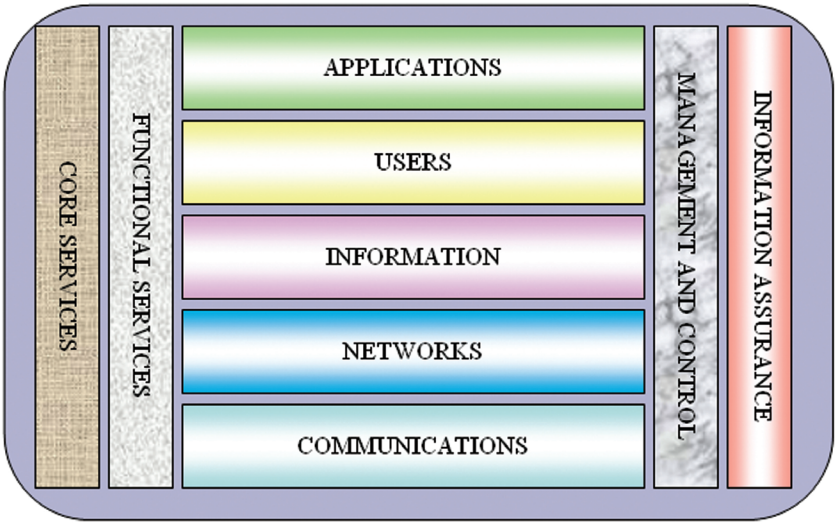

Fig. 2. - *Communications and information system for EU-led Crisis Management Operations (system view)*

in teams of specialized types of communications and information services. Deployable units will organize the operational al helpdesks at headquarters level for assistance, having included in their structure specialists in communications, computing, information assurance and security.

From a system view a crisis management CIS structure can be represented schematically as in **Figure 2** and includes a set of integrated subsystems with the central hub as the communities of interest / users with each individual profile determined by its position in the crisis management system, the right of access to information circulated and the place to access the system.

The principles underlying the design of such a system are: availability, sustainability, reliability, security, flexibility, interoperability and standardization. All subsystems shown in the figure will provide basic services tailored to the needs of the mission and function. The need to extend the services provided in places of permanent locations of communications and information systems, both at institutional and national level will be considered.

Functional and core services provided by a CIS in support of crisis management operations should be planned depending on the nature and extent of the mission, information exchange requirements for command, control, intelligence, surveillance and reconnaissance, the need for cooperation in operational theatre and the location of the field headquarters.

These services can be valuable, based on a robust architecture built on open standards or commercial and private military standards, as appropriate.

Also, services must be correlated in function to the capabilities using ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance) in the mission.

CIS core services of the CIS in support of the EU-led Crisis Management Operations are, as follows:

a) core network services: Common data exchange services, virtualization services, Geo/GIS services, automatic data processing services (office), network search services (web browsing), multimedia (voice, fax, video conferencing) services, import/ export data;

b) services for data interoperability: database replication, military organizational messaging, formatted messaging, e-mail, directory services, storage services, file services, file transfer, multi-service collaboration;

c) security services: authentication, information separation, intrusion detection, integrity services, encryption services, recovery services;

d) services for configuration management: configuration control, network management, data management, central services, security management;

e) communications services: bandwidth management, operational status monitoring, quality of service (QoS), routing services and allocation of streams, IP services,

ISDN services (Integrated Services Digital Network), radio and radio relay services.

Functional services provided by a communications and information system for crisis management could be: joint systems, land forces CIS, air forces CIS, naval forces CIS, logistics CIS, intelligence CIS, special forces CIS and others.

Based on the functional analysis (Timofte G, Tudose E., Vişan D: 2006, p.154) of a general CIS for crisis management the following functions can be identified:

a) The user interface contains all the elements involved in the human-computer interface: phones, fax machines, radios, portable terminals and fixed communications and information systems, screens and keyboards, automatic data conversion devices (scanner) and printers; microphones, speakers, cameras and video monitors system for audio and video teleconferencing and loudspeaker system notification / public announcement.

b) Conference facilities for audio and video teleconferencing secure and non-secure. Teleconferences IP (Internet Protocol) are done through a gateway function, having the role of IP addresses administration and to provide access to security areas defined in the local area network. Services provided under the facility of the conference are: voice / video classified and unclassified, switching and point to point capability and integration of data applications.

c) Area radio coverage provides communications between fixed and mobile units (military or civilian structures, vehicles or individuals) using fixed or portable devices. An implicit requirement of this function is the short message service (SMS). The EU specificity in this area is the radio devices diversity used by the EU military and civilian forces on the ground, on one hand and the need for coordination with all NGOs acting in the same area of operation, on the other hand. Another element of difficulty lies in the lack of coordination between the specialised authority for spectrum management of the EU mission and similar elements on the host nation territory, either because of legislative gap in this field or because of organizational limitations, as the case in many countries on the African continent. An effective spectrum management can be achieved only if the specialized structure of the crisis management mission will take over the responsibility of coordination and allocation of the frequencies for all actors on the operational theatre.

d) Strategic CIS extension. After installing the HQ command post in the theatre, the function modules are connected to CIS for crisis management at tactical level and if necessary with the extensions through modules developed at strategic level. The CIS modules to provide this function should be installed nearby the deployable communication modules that interconnect, the major C2 centers (operational and force

HQs, components HQs, Point of debarkation/ embarkation, etc.).

e) Information Assurance has to support the expansion of the core services and the access to functional applications of the strategic communications and information systems, based on the EU security policy and must also provide a platform for implementing the classified and unclassified domains of the mission. The Information Assurance function should include specialized management function which provides specific information exchange in security field between different systems.

f) Local area Network transport function is provided for interconnecting local area network physical elements of the HQ CIS, ensuring transparent connectivity for all services (packet and circuit switching, access services and local and external functional applications, etc.).

g) Dispersed user interface implements a service interface that can be used to access external networks with packet switching. Access to a network requires the use of an encryption equipment EU accredited to the classified ISDN or IP access router. This function does not replace the LAN infrastructure, but requires that an efficient access solution for staff liaison with the operational headquarters of the mission is implemented. The scenario implementation of this function requires additional protection measures to eliminate or reduce the risk of information compromise, where the user would be forced to facilitate the diversion of any service.

h) The interface function between systems or between different security domains in the same system is achieved through the implementation of the IEG (Information Exchange Gateway).

i) Network management function provides support for the use and maintenance of C2 means, including monitoring tools, configuration, fault detection and isolation, restoration of services on affected components and functions. Management of the deployable CIS provides classified data transport function for traffic management and therefore its separation from the user for all areas of security. For this purpose the encryption protocols and applications management solutions used in conjunction with IPsec will be implemented. Optionally, this function can be implemented in the communications modules and peripherals.

j) The interconnection function ensures interoperability between products, components, modules and systems.

The variety of the theoretical approaches to determine the CIS infrastructure for EU-led civilian and military crisis management operations and missions brings the conclusion that the planning and implementation process is extremely complex, especially in the context of the new security environment. This process requires national participation and adaptation of the national and

institutional development programs in the CIS field. On a short term, one solution could be the extension of the EU institutional operational network, EU OPS WAN, from political-military level in Brussels to the national military representatives in Belgium, and the EU Member States's capitals. This network could be further used for planning, deployment and redeployment of EU forces on missions and operations.

REFERENCES

[1] Burlacu M. (2007) *Operational Headquarter's C4I system for command and control of joint military operations*, PhD thesis, Defence National University "Carol I", Bucharest, p.156.

[2] Timofte G, Tudose E., Vişan D. (2006) *Battlefield digital military communications systems*, Inedit, Bucharest, pp. 70, 154.

[3] Burlacu M. (2005) *C4I systems of modern armed forces of NATO members states. Direction and perspectives on their evolution at the beginning of the 3rd millennium,* scientific research essay, "Carol I" Defence National University, Bucharest, pp. 26-28.