



**ORGANIZAREA SISTEMELOR DE COMUNICAȚII  
ȘI INFORMATICE PENTRU MANAGEMENTUL CRIZELOR  
ȘI PROTECȚIA INFRASTRUCTURILOR CRITICE  
ÎN CADRUL POLITICII DE SECURITATE ȘI APĂRARE COMUNĂ  
A UNIUNII EUROPENE**

**COMMUNICATION AND INFORMATICS SYSTEMS  
ORGANIZATION FOR CRISES MANAGEMENT  
AND CRITICAL INFRASTRUCTURES PROTECTION WITHIN  
THE FRAMEWORK OF EUROPEAN UNION'S COMMON  
SECURITY AND DEFENCE POLICY**

*General-locotenent (r) prof. asoc. dr. Constantin MINCU\**

**Rezumat**

*Lucrarea prezintă, pe scurt, studiul proceselor de planificare operațională în cadrul instituțiilor Uniunii Europene, analiza proiectelor Sistemelor de Comunicații și Informatică aflate în derulare, contribuția Armatei României la misiunile conduse de UE și proiectele naționale pentru sprijinul C2, experiența detașamentelor naționale și a grupurilor de experți în UE. Totodată, se încearcă un inventar al lipsurilor și constrângerilor de interoperabilitate în sistemele europene și naționale și analiza lecțiilor învățate în misiunile derulate sub egida Uniunii Europene.*

**Cuvinte cheie:** Uniunea Europeană; Sisteme de comunicații și informatică; C2, managementul crizelor.

**Abstract**

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

**Keywords:** EU; Communication and Informatics Systems; C2; crisis management.

---

\* Membru titular al Academiei Oamenilor de Știință din România, membru al Consiliului Onorific al Academiei Oamenilor de Știință din România, secretar științific al Secției de Științe Militare, Telefon: 0722.303.015, email: mincu\_constantin@yahoo.com.



## **I**ntruducere

Preocupările Uniunii Europene de a face față, cu mai multă forță, multiplicării factorilor de risc și unor noi și violente amenințări, s-au intensificat în ultimii ani.

Beneficiind de experiența unor țări occidentale dezvoltate (multiple lecții învățate din acțiunile politice, economico-financiare și militare anterioare), SUA, ca și NATO, încearcă să-și organizeze instituțiile și sistemele pentru situații complicate, ce pot să apară în spațiul european, dar și în zonele învecinate.

O atenție deosebită este acordată „Sistemelor de Comunicații și Informatică pentru Managementul Crizelor și Protecția Infrastructurilor Critice”.

Lucrarea de față încearcă să prezinte, în mod sintetic, unele aspecte mai importante ale planificării, realizării și utilizării sistemelor de comunicații și informatică pentru sprijinul cadrului instituțional și operațional de punere în practică a Politicii de Securitate și Apărare Comună (PSAC) în Uniunea Europeană, concomitent cu introducerea elementelor de stabilitate și securitate a acestor sisteme, în condițiile provocărilor erei informaționale.

1. Crizele și managementul acestora în cadrul politicii de securitate și apărare comună a Uniunii Europene

Mulți specialiști consideră, pe bună dreptate, că UE nu mai este o organizație exclusiv economică, aceasta își manifestă din ce în ce mai pregnant rolul de manager al crizelor locale și regionale, își dezvoltă proceduri, reguli și mijloace pentru identificarea, clasificarea și protecția infrastructurilor critice de pe teritoriul său.

Este în plină desfășurare procesul instituțional și operațional de acțiune în situații de criză și, pe această bază, determinarea fluxurilor informaționale și a cadrului arhitectural de dezvoltare a sistemelor de sprijin așa cum sunt sistemele de comunicații și informatică (SCI) pentru procesele complexe de comandă și control (C2).

Specialiștii structurilor UE, precum și cei ai țărilor membre, analizează cu intensitate și determinare (dat fiind contextul actual din punct de vedere politic, economic, financiar, juridic, diplomatic și militar):

- Crizele contemporane în domeniul securității:
  - Crizele contemporane și tipurile de crize;
  - Politica Externă și de Securitate Comună, precum și tendințele de evoluție pe termen mediu și lung;
  - implementarea Strategiei Europene de Securitate în domeniul managementului crizelor și al protecției infrastructurilor critice comune și naționale;



- Managementul crizelor prin misiuni conduse de UE în cadrul PSAC, prin participarea și angajamentul statelor membre în materie de capacități și forțe militare și civile:

- dezvoltarea capacității UE de răspuns la crize și stabilirea unui set de misiuni ale acestei organizații, precum și a forțelor necesare;

- clarificarea și implementarea graduală a procesului de planificare și a mecanismului decizional la nivel strategic european pentru managementul crizelor și protecția infrastructurilor critice (instituții, organisme, proceduri, reguli, angajamente etc.).

- Comanda și controlul forțelor utilizate de UE pentru managementul crizelor:

- cristalizarea și implementarea Concepției UE privind comanda și controlul acțiunilor militare și civile (control politic, direcționare strategică, abordare comprehensivă, lanț de comandă ad-hoc, multinaționalitate, unitate de comandă, unitate de efort și flexibilitate);

- organizarea și funcționarea comandamentelor militare pentru conducerea operațiilor UE, inclusiv resurse pentru Sistemul de Comunicații și Informatic (cine, cu ce și până la ce nivel asigură personal și echipamente specifice).

- Lămurirea unor aspecte privind contribuțiile naționale la managementul crizelor și la protecția infrastructurilor critice:

- să nu fie duplicate eforturile cu NATO;

- înțelegerea și procesarea corectă și completă a tendințelor privind contribuțiile Franței, Germaniei și Marii Britanii la PSAC și poziționarea României în acest proces;

- stabilirea pe baze reale de potențial uman, material, financiar și de altă natură a contribuției României la implementarea Politicii de Securitate și Apărare Comună și la eventualele acțiuni.

2. Cerințe și principii privind planificarea și realizarea sistemelor de comunicații și informatice pentru managementul crizelor:

- Se identifică și analizează factorii care influențează planificarea și realizarea sistemelor de comunicații și informatice:

- conectarea robustă a forțelor militare și/sau civile participante;

- colectarea, procesarea și distribuția performantă a datelor și informațiilor;

- realizarea capacității de înțelegere comună a situației reale;

- creșterea eficacității operaționale prin eficiență informațională.

Specialiștii în domeniu consideră că îndeplinirea dezideratelor menționate mai sus depinde de unii factori care influențează procesul de planificare, proiectare, realizare, implementare, dislocare în teatrul de operații și utilizare a SCI în sprijinul misiunilor UE (anexa nr. 1), astfel: interoperabilitatea sistemelor de comandă și



control, inclusiv a SCI care le sprijină; rezultatele cercetărilor în domeniu și proiectele UE pentru sprijinul Politicii de Securitate și Apărare Comună; transformările structurale de la Lisabona; relația UE – NATO în ceea ce privește cooperarea în domeniul proiectării, realizării și implementării SCI în sprijinul operațiilor pentru managementul crizelor; factori de ordin operațional.

- Planificarea SCI pentru managementul crizelor și protecția infrastructurilor critice în cadrul PSAC:

- se consideră strict necesară existența unei arhitecturi integrate a sistemelor de comunicații și informatice care să asigure superioritatea informațională și decizională pe timpul îndeplinirii misiunii;

- definirea cerințelor schimbului informațional la nivel strategic, operativ și tactic în cadrul misiunilor UE;

- cristalizarea și aplicarea unui set de cerințe și principii privind procesul de planificare operațională (selectarea opțiunii, elaborarea Directivei Militare Inițiale, elaborarea capitolelor privind SCI și a anexelor aferente etc.).

- Cadrul organizatoric și arhitectural pentru realizarea SCI în sprijinul misiunii UE pentru managementul crizelor:

- cadrul de lucru arhitectural pentru SCI în UE este identificat ca fiind același cu cel definit de NATO și anume NAF (Arhitectura NATO pentru sisteme C3, V.3)<sup>1</sup>, ceea ce conferă, cel puțin din acest punct de vedere, un avantaj major pentru proiectarea SCI naționale puse la dispoziția forțelor care pot acționa alternativ sub egida celor două organizații.

- Structura și funcțiile SCI ale UE și statelor membre:

- Structura cuprinde: Sistemul de Comunicații și Informatic cu infrastructură fixă, Sistemul de Comunicații și Informatic pentru supraveghere și avertizare timpurie, Sistemul de Comunicații și Informatic dislocabil și sistemele de comunicații și informatice ale statelor membre;

- din punct de vedere structural, SCI se prezintă ca în fig. 1. Se consideră de către specialiști și decidenți UE că acesta va avea o compunere modulară și scalabilă, fiind organizat în centre permanente de comunicații și informatice (CPCI), instalate la Bruxelles și în capitalele statelor membre, centre operative de comunicații și informatice (COCI), fixe și desfășurabile, de sprijin sau terminale, de la nivelul comandamentelor operaționale (OHQ, FHQ, componentele forțelor sau GTL), linii de comunicații (LC) realizate în diferite medii de transport informațional;

---

<sup>1</sup> European Defence Agency, *Network Enabled Capability Implementation Study*, EU NEC Vision third report, Brussels, 09.02.2010, p. 23.



- toate elementele menționate vor fi integrate în infrastructura informațională de transport cu două niveluri de clasificare SECRET UE și RESTRAINT UE (Rețeaua securizată de arie extinsă a UE), care va avea, ca o primă aplicație de bază, sistemul de mesagerie de nivel secret – CAMEO (aplicație software de colaborare în rețea pentru managementul crizelor).

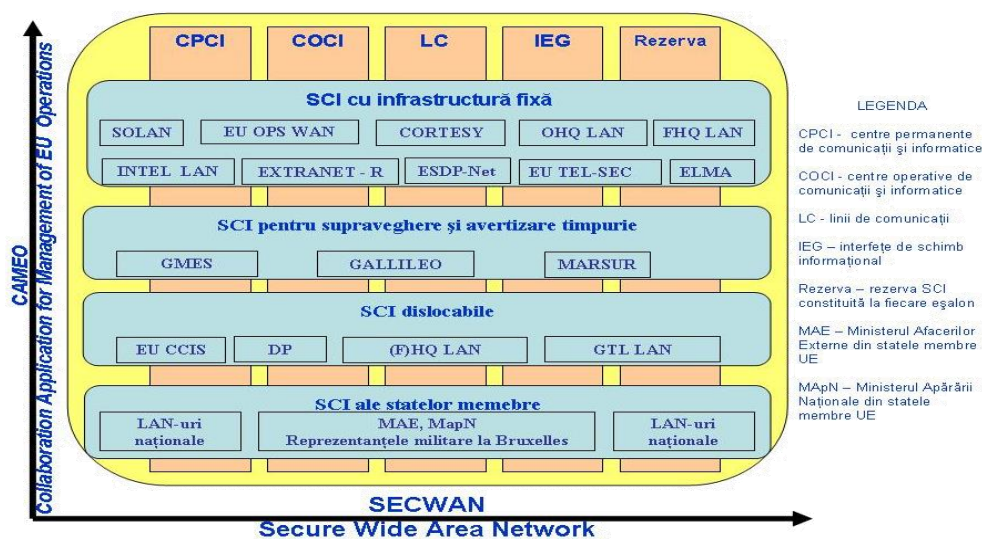


Figura 1. Compunerea sistemului de comunicații și informatic pentru managementul crizelor (abordare structurală)

- Serviciile de bază și funcționale asigurate de un SCI trebuie planificate în funcție de specificul și amploarea misiunii, cerințele schimbului informațional pentru comandă, control, informații, supraveghere și recunoaștere, nevoile de cooperare în teatrul de operații, precum și de disponerea comandamentelor în teren. Serviciile de bază sunt servicii principale de rețea, servicii pentru interoperabilitate, servicii de securitate, servicii pentru management, servicii de comunicații;

- Serviciile funcționale asigurate pot fi pentru: comanda și controlul forțelor întrunite; comanda și controlul forțelor terestre, aeriene și navale; logistică; informații; alte servicii funcționale;

- Pe baza analizei funcționale a unui sistem generic SCI sunt identificate următoarele funcții: interfața cu utilizatorul, facilitățile pentru conferință, acoperirea radio zonală, înștiințarea sau anunțarea publică, asigurarea informațională, comutația de circuite, comutația de pachete, transportul în rețeaua locală, managementul capacității de transfer a datelor, interfața cu utilizatorii



dispersați, interfața cu alte sisteme, transmisiunile exterioare, de securitate, infrastructură ambientală, managementul rețelei, de interconectare.

3. Utilizarea SCI pe timpul misiunilor conduse de UE pentru managementul crizelor și protecția infrastructurilor critice:

- SCI pentru avertizare timpurie și planificare strategică:

- Se consideră că pentru realizarea SCI pentru avertizare timpurie se vor analiza și lua în considerație trei tipuri de fluxuri informaționale, în funcție de opțiunile de comandă și control pentru misiune: fluxul informațional de bază pentru informații de rutină, fluxul informațional pentru informații în operațiile autonome conduse de UE, fluxul informațional pentru informații în operații Berlin Plus (situația existentă în prezent privind SCI pentru aplicarea PSAC se prezintă generic în anexa nr. 2);

- Concluzia care se desprinde din analiza sistemelor actuale de comunicații și informatice în UE este că acestea au, la această dată, un nivel scăzut de interconectivitate, prezintă multe breșe care impun transferul manual al informațiilor și au un nivel prea ridicat de clasificare care, nu întotdeauna, satisface cerințele utilizatorilor și, ceea ce este mai important, nu există o infrastructură unică care să interconecteze automatizat instituțiile PSAC cu factorii de decizie pe linie operațională din capitalele statelor membre.

- Utilizarea SCI dislocabile pentru sprijinul managementului crizelor în cadrul PSAC:

- realizarea unei infrastructuri comune de rețea pentru schimbul informațional la toate nivelurile ierarhice și implementarea unor măsuri specifice de creștere a viabilității sistemelor și serviciilor pe timpul misiunilor conduse de UE;

- această infrastructură comună de rețea presupune interconectarea LAN ale structurilor militare de nivel strategic (OHQ) cu cele de nivel operativ (FHQ) și tactic;

- viabilitatea SCI dislocabile și a elementelor de structură depinde, în opinia celor mai mulți specialiști, de structura lor, de gradul de dispersare a elementelor componente, de gradul de asigurare a rezervei și de complexitatea soluțiilor tehnice adoptate pentru transportul fluxurilor informaționale. Un alt factor de influență specific misiunilor previzibile ale UE este gradul de dependență, la nivel operativ și tactic, de infrastructura de telecomunicații asigurată de operatorii publici din țara gazdă.

- Aspecte privind misiunile SCI, în condițiile implementării capacităților facilitate de rețea (NEC):

- în concepția UE, NEC reprezintă „abilitatea de a crea un mediu unitar pentru o abordare comprehensivă și unificarea eforturilor entităților militare și



civile și a tuturor actorilor, la toate nivelurile, în operațiile pentru managementul crizelor conduse de UE<sup>2</sup>;

- se apreciază că NEC va putea fi implementată în măsura în care se vor crea premisele pentru implementarea unei infrastructuri federalizate pentru schimbul de date, informații și servicii informaționale în sprijinul misiunilor conduse de UE.

• Utilizarea sistemelor de comunicații și informatice pentru sprijinul operațiilor în rețele de calculatoare și apărarea spațiului cibernetic:

- Operațiile în rețele de calculatoare se definesc ca „acțiuni deliberate ce se desfășoară pentru optimizarea rețelelor IT, computerelor și a altor echipamente electronice în scopul câștigării și menținerii supremației informaționale, concomitent cu reducerea capacității adversarului de a acționa în acest sens”;

- La nivelul UE, problematica Operațiilor în Rețele de Calculatoare (ORC) cade sub incidența PSAC, dar nu este încă fundamentată pe deplin din punct de vedere juridic, deși s-au luat unele măsuri specifice în cadrul CE odată cu introducerea Directivei 2006/24/CE privind reținerea datelor generate sau prelucrate de către furnizorii de rețele și servicii de comunicații electronice destinate publicului<sup>3</sup>.

• Armonizarea eforturilor naționale pentru utilizarea sistemelor de comunicații și informatice în sprijinul managementului crizelor

- se apreciază ca necesară înființarea, pe niveluri ierarhice, a funcției de ofițer coordonator pentru managementul informațiilor (OCMI);

- îmbunătățirea cadrului organizațional de dezvoltare a SCI militare și speciale în UE;

- identificarea unor oportunități privind participarea Armatei României la dezvoltarea SCI pentru necesitățile UE (a se vedea experiența românească în misiunea SEEBRIG din Afganistan, precum și valoarea unor specialiști militari români dovedită în misiuni internaționale NATO, ONU, UE).

4. Stabilitatea în funcționarea și securitatea sistemelor de comunicații și informatice pe timpul misiunilor conduse de UE:

➤ Din perspectiva autorităților civile, confruntarea internațională, pe diverse paliere și teme, atrage după sine o multiplicare a raporturilor de forță, în timp ce în plan militar există o aparentă limitare a acestora (restrângerea puterii militare datorită reducerii caracterului violent al confruntărilor). Aceste principii se manifestă în mod practic în contextul desfășurării misiunilor pentru managementul crizelor sub forma unor vulnerabilități ce afectează stabilitatea și securitatea

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

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



sistemului de comunicații și informatic propriu, în ansamblul său, precum și, într-o oarecare măsură, stabilitatea în funcționare a elementelor acestuia:

- Stabilitatea sistemelor de comunicații și informatice în misiunile conduse de UE pentru managementul crizelor:

- această funcționare stabilă presupune adoptarea unor măsuri multilaterale pentru asigurarea stabilității, în condițiilor unei multitudini de factori aleatori ce pot fi estimați, dar nu determinați cu exactitate și prezenței acțiunii perturbatoare a unor factori distructivi provocați de adversar;

- analiza stabilității sistemelor de comunicații și informatice înseamnă, în principal, respectarea unor reguli de bază cum sunt: abordarea globală modulară; criteriul rentabilității; orientarea spre utilizatori; asigurarea procesului unic de introducere a datelor; o soluție generală și independentă de configurare a sistemului; posibilitatea de dezvoltare ulterioară;

- calculul, prin mijloace matematice complexe, a stabilității SCI;

- calculul, pe baze statistice și probabilistice, a disponibilității SCI (disponibilitatea este definită ca probabilitatea unui element component al SCI de a fi în măsură să furnizeze capacitatea funcțională cerută de utilizatori);

- stabilitatea structurilor organizatorice și a fluxului informațional presupune determinarea măsurilor specifice pentru asigurarea stabilității structurilor organizatorice impunând abordarea mai multor domenii, relativ distincte, printre care: continuitatea proceselor de comandă și control și capacitatea de conducere; fiabilitatea mijloacelor tehnice utilizate și a structurilor funcționale; stabilitatea la bruiaje și perturbații electromagnetice; mobilitatea echipamentelor și a elementelor de structură;

- stabilirea unor principii și cerințe privind asigurarea informațională;

- identificarea și punerea în practică a unor soluții pentru armonizarea eforturilor naționale de asigurare a traficului informațional pe timpul misiunilor conduse de UE;

- asigurarea prin măsuri organizaționale și tehnice a securității SCI pe timpul pregătirii și desfășurării misiunilor UE;

- elaborarea și respectarea strictă a unor principii privind securitatea SCI;

- acreditarea, pe baze științifice, a standardelor de securitate a SCI;

- studierea atentă multicriterială a unor provocări la adresa securității SCI, în condițiile mediului facilitat de rețea.

5. Autorii propun unele măsuri, atât pentru autoritățile UE, cât și pentru cele naționale:

- comanda și controlul misiunilor pentru managementul crizelor prin crearea unei structuri permanente C2 și a unui comandament militar strategic unic la Bruxelles;





- asigurarea sistemelor de sprijin, prin abordarea unitară a problematicii SCI în UE;
- stabilitatea și securitatea SCI prin aplicarea standardelor unice de funcționare și securitate;
- exercitarea cu eficiență a managementului riscului de securitate informațională;
- implementarea, cu mai multă forță și eficiență, în Armata României, a procedurilor SCI NATO și UE;
- identificarea unor măsuri organizatorice și tehnice pentru creșterea eficienței SCI operative și tactice dislocabile;
- implementarea managementului informațional, în toate sistemele, rețelele și serviciile UE.:

\* \* \*

În concluzie, propunem următoarele direcții majore de dezvoltare în domeniul SCI destinate sprijinului misiunilor conduse de UE pentru managementul crizelor și protecția infrastructurilor critice:

- revederea concepțiilor operațiunilor și detalierea lor suficientă pentru creșterea simplității și evitarea ambiguităților pe timpul implementării în cadrul misiunilor;
- standardizarea proceselor și reglementărilor la toate nivelurile operaționale;
- dezvoltarea și implementarea SCI în conformitate cu scenariile operative;
- definirea arhitecturilor de interconectare a rețelelor existente și crearea unei infrastructuri comune pentru lanțul C2;
- revederea nivelurilor de clasificare a rețelelor și definirea unor cerințe comune obligatorii în domeniul SCI, pentru UE și statele membre.



## BIBLIOGRAFIE

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



- 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.
- ALEXANDRESCU C-tin., ILINA D., MINCU C-tin., *Bazele matematice ale orgaizării sistemelor de transmisiuni*, Editura Militară, București, 1994.
- FRUNZETI T., *Considerații asupra participării Armatei României la acțiuni colective*, Editura Universității Naționale de Apărare „Carol I”, București, 2006.
- GYA G., *ESDP and EU Mission Update*, European Security, Brussels, 2007.
- MERLINGEN M., Ostrauskaitė R. (ed.), *European Security and Defence Policy – An Implementation Perspective*, Routledge, Abington, 2008.
- TIMOFTE G, TUDOSE E., CONSTANTIN G., *Protecția informațiilor în sistemele de comunicații militare moderne*, Editura Inedit, București 2006.
- BOMQVIST P., *CIO Target document for Networking and Information Infrastructure (NII)*, Swedish Armed Forces, Stockholm, 2009.
- DOMINGO A., Wietgreffe H., *TN-1009, NATO Deployable CIS Target Architecture Document*, Edition 2.0, NC3A, The Hague, 2004.
- FRUNZETI T., *Gestionarea crizelor în războiul rece*, Lumea Militară, nr. 1, București, 2006.
- GAMOW G., *PHYS Z.* 51, 204 (1928).
- FORSTER D., *Hydrodynamic Fluctuations* (Benjamin, New York, 1975) Vol. I.
- RING P., SCHUCK P., *The Nuclear Many-Body Problem* (Springer-Verlag, Berlin, 1980).
- SANDULESCU A., DUMITRESCU O., *Phys. Lett. B* 24, 212 (1967).
- E. S. Paul *et al.*, *Phys. Rev. C* 61, 064320 (2000).
- SOLOVIEV V. G., *Theory of Atomic Nuclei* (Institute of Physics Publishing, Bristol, 1992).

