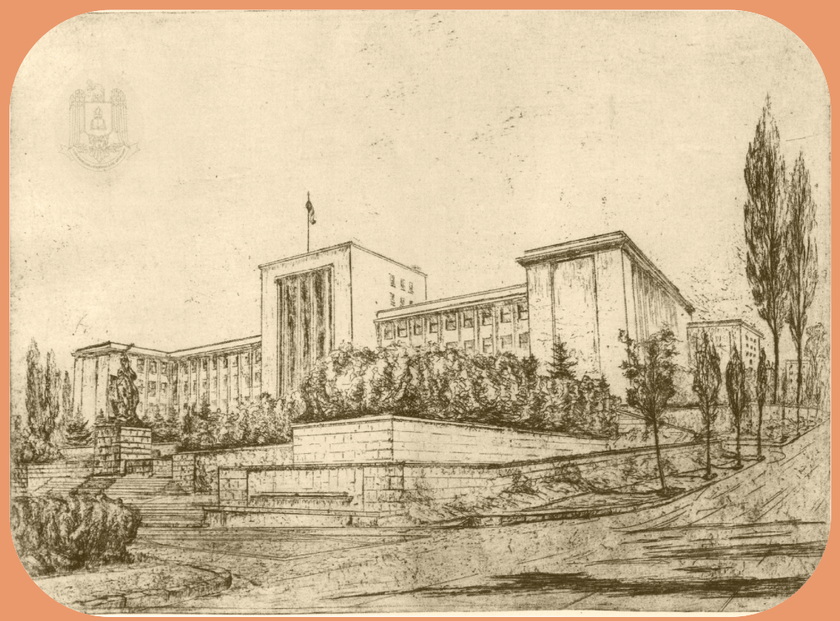
1889-2009



120 de ani
de la înființarea Școlii Superioare de Război

ISSN 1582-7410

REVISTA DE ȘTIINȚĂ MILITARĂ ANUL IX, 2009 NR. 1 (16)

Revista de Științe Militare

Editată de Secția de Știință Militară
a Academiei Oamenilor de Știință din România

Nr. 1 (16)
Anul IX, 2009

1859-2009
150 de ani
de la Unirea Principatelor Române

Revista de Ştiinţe Militare

Editată de Secţia de Ştiinţă Militară
a Academiei Oamenilor de Ştiinţă din România

1859-2009
150 de ani
de la Unirea Principatelor Române

Nr. 1 (16)
Anul IX, 2009

Acest număr cuprinde comunicările ştiinţifice prezentate în cadrul simpozionului cu tema: ***"Sisteme integrate de comandă şi control"****, ce a avut loc la 25 mai 2009 în sala de marmură a Cercului Militar Naţional, în organizarea Secţiei de Ştiinţe Militare din Academia Oamenilor dre Ştiinţă din România.*

ISSN 1582-7410

C U P R I N S

CUVÂNT DE DESCHIDERE

Doamnelor şi domnilor,

Sunt onorat să deschid lucrările simpozionului intitulat „Sisteme integrate de comandă şi control", organizat de către Academia Oamenilor de Ştiință din România (Secția de Ştiințe Militare) împreună cu Universitatea Națională de Apărare „Carol I".

În societatea tehnologică şi informațională a secolului XXI, tehnologia informației este utilizată nu numai în societatea civilă ci şi în domeniul militar.

Comanda şi controlul reprezintă un proces iterativ de luarea deciziilor strâns legat de procesul de feedback ce se stabileşte între realitatea existentă în spațiul de luptă şi măsurile cuprinse în planurile şi corectivele acestora la nivelul comenzii. Schimbările generate în aceste domenii de era informațională au adus unele modificări ale modului de abordare pe această linie, schimbări ce comportă o serie de oportunități şi de provocări despre care vor vorbi câțiva generali şi colonei, profesori universitari şi doctori în ştiințe militare, personalități ale ştiinței şi culturii româneşti, 5 dintre aceştia fiind membri ai Secției de Ştiințe Militare ai AOS.

Dezvoltarea tehnologică şi ştiințifică contemporană influențează în mare măsură planificarea, organizarea, comanda şi desfăşurarea acțiunilor militare.

În acest context, structurile militare sunt asigurate cu sisteme specifice de comandă şi control, de optimizare a activităților de colectare, prelucrare, stocare, distribuție şi protecție a informațiilor, de achiziție a sistemelor integrate de comandă, control, comunicații, computere şi informații (C4I), care asigură comanda şi controlul acțiunilor militare în timp real sau aproape real. Fiecare categorie de Forțe are Sisteme de Comandă şi Control, ceea ce înseamnă că şi categoriile de Forțe ale Armatei României sunt dotate cu aceste sisteme moderne. Astfel, există Sistemul de Comandă şi Control Aerian Național (SCCAN), Sistemul C4I pentru Forțe Terestre şi, în perspectiva apropiată se va realiza Sistemul de Comandă şi Control al Forțelor Navale..

General (r) prof. univ. dr. Vasile CÂNDEA
Preşedintele Academiei Oamenilor de Ştiință din România

COMANDA ŞI CONTROLUL ÎN OPERAȚIILE MILITARE MODERNE

General (r) prof. univ. cons. dr. Eugen BĂDĂLAN
General-locotenent (r) conf. univ. dr. Florian PINTA

"A strong collective defence of our populations, territory and forces is the core purpose of the Alliance and remains our most important security task"

O frază memorabilă înscrisă în Declarația finală a Summit-ului de la Kehl/Strasbourg, din aprilie 2009, care, pe lângă faptul că reconfirmă importanța colosală a Art.5 din tratatul de la Washington, reprezintă elementul cheie care va sta la baza noului Concept Strategic al NATO pentru următorii 20 de ani!

INTRODUCERE

Optsprezece ani în urmă, la Summit-ul de la Roma din 1991, NATO a început cu bună credință transformarea sa post Război Rece, prin adoptarea unei noi Concepții Strategice. Deşi în acel moment Alianța nu inițiase încă nicio operație, în mai puțin de un an, aeronavele sale dotate cu sisteme aeropurtate de avertizare timpurie (AWACS) patrulau pe cerul de deasupra Bosniei şi Herțegovinei, iar comandamentele mobile ale comenzii Grupului de Armate Nord, care nu mai există în prezent, erau împrumutate ONU pentru a deveni comandamentele Forței de Protecție a Națiunilor Unite. Cei doi paşi au lansat NATO într-o serie din ce în ce mai variată şi solicitantă de angajamente operaționale în interiorul şi în afara Europei, mai întâi în Balcani şi Marea Mediterană şi apoi în Afganistan, Irak şi regiunea Darfur din Sudan. De asemenea, aceştia au determinat apariția unui model de cooperare politică şi operațională crescândă între NATO, ONU, UE şi OSCE fundamentat pe decizia adoptată în decembrie 1992 de miniştrii de externe ai țărilor NATO, potrivit căruia

Alianţa urma să fie pregătită să sprijine operaţiile de menţinere a păcii desfăşurate sub autoritatea Consiliului de Securitate al ONU.

1. NOŢIUNI GENERALE PRIVIND COMANDA ŞI CONTROLUL

Comanda şi controlul se manifestă sub diferite forme, în toate organizaţiile umane structurate mai mult sau mai puţin ierarhic, ca funcţie de bază, specifică organizării şi conducerii. David Alberts în lucrarea *„Aranjamentele de comandă în operaţiile de menţinere a păcii”*[1], remarca apariţia şi evoluţia separată a conceptului de comandă şi control, în domeniul militar şi în managementul industrial, în primul rând datorită caracterului specific al acestora.

J. Wiliam Snyder Jr., în studiul *„Command versus Operational Control”* [2] referindu-se la **“comandă”,** sublinia că aceasta **„este mai întâi o artă”,** în cadrul căreia comandanţii formulează concepţii, imaginează stadiul final de atins, stabilesc misiuni pentru forţe, alocă resurse corespunzătoare, evaluează riscuri şi iau decizii. Pe timpul luptei, comandanţii observă şi înţeleg ceea ce se întâmplă, iau decizii rapide pentru deplasarea şi acţiunea forţelor la locul şi timpul potrivit şi anticipează schimbările în evoluţia situaţiei. Comandanţii conduc, direcţionează şi motivează subordonaţii şi organizaţia, pentru îndeplinirea misiunii. Comanda este, aşadar, **„afacerea comandantului”. „Controlul”,** pe de altă parte, **„este o ştiinţă”** a forţelor militare prin care statul major lucrează independent sau în cooperare cu alte state majore, pentru implementarea ordinelor comandantului. Controlul este, deci, **„afacerea statului major”.**

Paralel cu eforturile de formulare a unei definiţii care să reunească un consens cât mai larg, are loc o extindere a sintagmei **„comandă şi control”,** cunoscută şi sub abrevierea „C2”, către „C3” (+comunicaţii), „C4” (+computere), „C4I2” (+informaţii şi intelligence), „C4I2SR” (+recunoaştere şi supraveghere). Alte două acţiuni, „coordonarea” şi „cooperarea” tind să se alăture comenzii, fiind deja întrebuinţată sintagma „C6”, complicând şi mai mult lucrurile.

Dincolo de abordarea conceptuală amintită, specialiştii NATO, în special comunitatea dedicată strict studiului comenzii şi controlului (NC3A-Agenţia NATO pentru Consultare, Comandă şi Control) atribuie sintagmei „C2” o înţelegere mai largă. Astfel, *„comanda şi controlul reprezintă o funcţie a comandantului, a statului major şi a altor elemente de comandă, destinată*

[1] Alberts, David and Richard E. Hayes, Command Arrangements for Peace Operations, Washington, DC, Command and Control Research Program (CCRP) Publication Series, 1985, cap. 1.

[2] Snyder, Wiliam, Jr., Command versus Operational Control, Washington National Defense University Press, 2000, p.54.

menţinerii unui nivel ridicat de operativitate, pregătirii operaţiilor şi conducerii trupelor, în vederea îndeplinirii misiunii" [3].

2. EVOLUŢIA STRUCTURILOR DE COMANDĂ-CONTROL NATO, POST RĂZBOI-RECE

Noua structură de comandă aprobată la Summit-ul de la Praga în 2002, caracterizată de accentul pus pe comandamentele întrunite şi componente, reflectă învăţămintele desprinse din aranjamentele de comandă pentru managementul operaţiilor din Balcani, care au evoluat în timp sub auspiciile Comandamentului Forţelor Aliate din Europa de Sud de la Neapole, Italia.

IFOR, în 1995, şi KFOR, în 1999, s-au bazat pe capabilităţile de asigurare a intrării forţelor în teatru ale Corpului Aliat de Reacţie Rapidă (ARRC), care fusese înfiinţat în 1994 pentru a fi comandamentul conducător al ambelor operaţii. Ca parte a noii Structuri de Forţe, de asemenea aprobată în 2002, ARRC a devenit un model pentru alte şase comandamente terestre de Forţe cu Nivel Înalt de Operativitate (HRF). Prin rotaţie, cele şapte corpuri multinaţionale furnizează componenta terestră a NRF.

Alte câteva dintre acestea împreună cu Canada furnizează, de asemenea, personalul pentru nucleul comandamentului multinaţional HRF de nivel corp, al Forţei Internaţionale de Asistenţă de Securitate (ISAF) din Afganistan. Prin dubla lor utilitate, pentru NRF şi ISAF, aceste comandamente au dobândit competenţele şi deprinderile esenţiale în vederea planificării şi desfăşurării atât a unei reacţii rapide, cât şi a unor operaţii de mare durată.

Este de remarcat, în acest context, că angajarea NATO în Afganistan a deschis calea abordărilor inovative în privinţa folosirii mai flexibile a forţelor Alianţei în sprijinul operaţiilor non-NATO conduse de ţări aliate sau de organizaţiile internaţionale sau în mod concertat cu acestea. Când în 2002 Germania şi Olanda au solicitat sprijinul NATO pentru a le facilita exercitarea în comun a comenzii ISAF, înainte ca acesta să devină o operaţie condusă de NATO, expertiza şi mijloacele oferite prompt de NATO au demonstrat că Alianţa dorea şi era aptă să contribuie la planificarea şi desfăşurarea operaţiilor conduse de alţii. Cooperarea operaţională între ISAF şi Comandamentul Forţelor Multinaţionale din Afganistan condus de SUA şi parteneriatul în domeniul instruirii Forţelor Irakiene de Securitate dintre Misiunea NATO de Instruire şi Comandamentul Multinaţional pentru Securitatea Tranziţiei condus de SUA au ilustrat felul în care Alianţa poate acţiona colectiv prin modalităţi care sunt complementare la eforturile individuale ale diferiţilor aliaţi.

[3] Definiţie disponibilă pe: http//www.nato.int/docu/glossary/eng/pdf (April 07.2005).

Acestea au pus în evidenţă, de asemenea, adaptabilitatea Alianţei la condiţiile aflate în evoluţie. În acest sens, sprijinul NATO pentru Uniunea Africană în vederea întăririi misiunii acesteia de menţinere a păcii în regiunea Darfur din Sudan confirmă progresele realizate din 2002 în încercarea de a face ca sprijinul NATO să fie disponibil pentru operaţiile non-NATO.

3. PRINCIPIILE ARANJAMENTELOR DE COMANDĂ – CONTROL SPECIFICE ALIANŢELOR DIN CARE ROMÂNIA FACE PARTE

Deşi diferite din punct de vedere al scopului pentru care au fost create, NATO şi UE au în comun voinţa politică şi capacitatea de participare, alături de alte structuri internaţionale, la menţinerea păcii şi stabilităţii în zonele unde interesele statelor membre se manifestă. Dezvoltarea dimensiunii de securitate în cazul UE[4] şi angajarea Alianţei în operaţii de gestionare a crizelor[5] în afara ariei tradiţionale de acţiune, conferă celor două organizaţii un statut de necontestat în cadrul instrumentelor pe care comunitatea internaţională le are la dispoziţie, în rezolvarea situaţiilor de criză.

Dacă NATO şi-a dezvoltat şi perfecţionat, în cei 60 de ani de existenţă, un set de politici şi proceduri de acţiune bazate, în principiu, pe folosirea instrumentului militar, experienţa UE în domeniul gestionării crizelor este relativ recentă[6]. Caracterul predominant „civil" al misiunilor UE (deşi mare parte din acestea s-au desfăşurat cu aport militar, atât în faza de planificare, cât şi în cea de execuţie), nu a exclus preocupările structurilor militare comunitare de a dezvolta şi perfecţiona doctrine, concepte şi politici proprii de management al crizelor. În privinţa *capabilităţilor de comandă şi control,* la nivelul ambelor organizaţii s-a convenit, însă, că întrucât majoritatea statelor UE sunt şi membre NATO[7], trebuie *„evitată duplicarea eforturilor şi dezvoltările de structuri paralele".*

Prin urmare, *principiile* specifice aranjamentelor de comandă între NATO şi UE au la bază faptul că *participarea la operaţiile de management al crizelor se face pe bază de* **„voluntariat"** în ambele organizaţii, *statele membre contribuind cu forţe acolo unde există interese comune, dar şi individuale.*

"Consensul" - ca principiu de bază care guvernează luarea deciziei în ambele organizaţii, are o nuanţă de flexibilizare în cazul UE, care poate face apel la

[4] The Treaty of the European Union, Brussels, 1992.
[5] The Alliance'Strategic Concept, Brussels, 1999.
[6] Politica Europeană de Securitate şi Apărare, lansată cu ocazia summit-ului de la Köln din 1999, a devenit operaţională în 2001, odată cu crearea structurilor politico-militare în cadrul celui de-al doilea pilon al UE.
[7] Un numar de 21 state membre UE sunt şi membre NATO. Fac excepţie Turcia, Norvegia, Islanda, SUA şi Canada.

aşa-zisa **„abţinere constructivă”** în situaţiile în care consensul nu este atins, astfel încât participarea la operaţii să nu fie blocată.

Un principiu important, din perspectiva aranjamentelor de comandă, îl reprezintă **“controlul politic al operaţiilor”,** care se efectuează în NATO de către Consiliul Atlanticului de Nord (CAN), iar în UE de către Comitetul Politic şi de Securitate (CPS), sub autoritatea Consiliului Uniunii Europene, prin stabilirea obiectivelor politico-militare ale operaţiei, a scopurilor şi mijloacelor pentru atingerea acestora.

„Abordarea cuprinzătoare a managementului crizelor”, principiu caracteristic UE, dar folosit din ce în ce mai mult şi de Alianţă, s-a impus ca răspuns la incapacitatea instrumentului militar de a gestiona consecinţele crizelor în domeniul reconstrucţiei şi dezvoltării în zonele devastate de conflicte sau acolo unde instituţiile statului nu au avut capacitatea administrativă exercitării şi impunerii autorităţii legii.

În sfârşit, principiul **„multinaţionalităţii”,** caracteristic ambelor organizaţii, reflectă modul în care se realizează procesul de generare a forţelor, ţinând cont de cerinţele operaţionale. Statele membre, precum şi statele contributoare cu trupe care nu sunt membre UE sau NATO, pot participa la operaţii de management al crizelor şi, implicit, pot fi reprezentate în structura de comandă şi control, cu observaţia că responsabilitatea organizării lanţului de comandă revine comandantului operaţional.

Cu privire la acest aspect, trebuie observat că pentru conducerea operaţiilor de management al crizelor NATO poate utiliza structura permanentă de comandă (compusă, la nivel strategic, din Comandamentul Aliat pentru Operaţii şi, la nivel operativ, din trei comandamente întrunite), în timp ce UE are mai multe opţiuni: utilizarea comandamentelor naţionale, puse la dispoziţie de către statele membre[8], recurs la mijloacele şi capabilităţile NATO[9] (aranjamente cunoscute sub sigla “Berlin +”) sau activarea Centrului Operaţional din cadrul Secretariatului General al Consiliului.

4. AUTORITATEA DE COMANDA-CONTROL ÎN OPERAŢIILE MULTINAŢIONALE LA CARE PARTICIPĂ ARMATA ROMÂNIEI

Modalităţile de manifestare a autorităţii de comandă şi control au constituit în permanenţă un subiect “fierbinte” pe agenda de lucru a liderilor politici şi

[8] În prezent, 5 state membre pun la dispoziţia UE comandamente naţionale: Franţa, Marea Britanie, Germania, Italia şi Grecia.

[9] Consultation between the EU and NATO in the context of a possible EU-led operations making use of NATO’s common assets and capabilities, Brussels, 2003.

militari, mai ales în ultimii 18 ani, când evoluţiile spectaculoase din mediul de securitate au impus găsirea unor soluţii moderne acestei paradigme, având în vedere specificul participării la operaţii multinaţionale. Iar "nodul gordian" l-a reprezentat, fără îndoială, încredinţarea comenzii forţelor proprii unui comandant străin. Dacă în cadrul alianţelor tradiţionale, aceasta şi-a găsit în mare parte rezolvarea, prin stabilirea unor standarde şi proceduri clare, în cazul coaliţiilor ad-hoc aranjamentele de comandă şi control au fost şi sunt încă relativizate de înţelegerile politice dintre statele participante.

Apartenenţa României la Alianţa Nord-Atlantică şi la Uniunea Europeană poate induce ideea rezolvării de la sine a problemei conducerii forţelor în operaţii, prin simpla aplicare a standardelor şi procedurilor existente, singura preocupare constituind-o implementarea şi respectarea acestora. În parte, acest lucru este adevărat, dacă avem în vedere faptul că ambele organizaţii, îndeosebi NATO, în evoluţia lor, şi-au dezvoltat structuri de comandă proprii, pe care le-au exersat şi le-au perfecţionat continuu pentru a satisface, într-o măsură cât mai mare, exigenţele operaţionale şi sensibilităţile participanţilor, ceea ce a conferit o anumită garanţie a stabilităţii aranjamentelor de comandă.

Acceptând că în cazul operaţiilor multinaţionale aranjamentele de comandă vor continua să reprezinte *"înţelegeri temporare, instituite între comandanţi internaţionali şi diferite forţe naţionale puse la dispoziţie, referitoare la nivelul şi limitele de exercitare a autorităţii asupra acestora, pentru îndeplinirea unei misiuni comune"*[10], se impune să sesizăm nuanţele care reflectă funcţionarea acestui mecanism complex al conducerii militare operaţionale, indiferent de situaţie, şi care determină deciziile naţionale privind subordonarea trupelor proprii altor comandamente.

Întâi de toate, faptul că prerogativele de **"comandă totală"**[11] („full command") care asigură puteri depline în organizarea şi întrebuinţarea forţelor, în scopul îndeplinirii misiunii încredinţate nu sunt atribuite comandanţilor internaţionali de către niciun stat sau guvern prin derogarea de la drepturile sale suverane asupra forţelor naţionale participante la operaţii multinaţionale. Aceasta înseamnă, desigur, că la nivelul Alianţei sau Coaliţiilor de forţe se recunoşte şi se respectă această cutumă, chiar dacă neexercitarea comenzii totale de către un comandant internaţional presupune un grad de autoritate mai scăzut decât atunci când se foloseşte în scopuri pur naţionale.

Nici România nu putea face excepţie de la această regulă, aşa încât deciziile privind participarea cu forţe la misiuni internaţionale, în afara graniţelor

[10] Alberts, David, Richard E. Hayes, op.cit. p.22.
[11] Joint Chiefs of Staff Publication 1-02, p.8.

ţării şi aranjamentele de comandă specifice fiecărei operaţii se adoptă de către autorităţile abilitate ale statului – Parlament, Preşedinte, Consilul Suprem de Apărare a Ţării, Guvern – şi se implementează de către ministerele de resort. În cazul Armatei, responsabilitatea exercitării comenzii totale revine Autorităţii Naţionale de Comandă.

În acelaşi timp, trebuie acceptat faptul că, în operaţiile multinaţionale, care presupun o asamblare de forţe diferite pentru atingerea unui obiectiv propus, comandamentele nu pot funcţiona fără delegarea anumitor prerogative de comandă naţională către un comandant internaţional.

Astfel, comandantului internaţional i se poate delega **"comanda operaţională"**[12] (OPCOM), respectiv „autoritatea de a stabili misiuni şi sarcini pentru subordonaţi, de a disloca unităţi, a resubordona forţe şi a reţine sau delega controlul operaţional şi/sau tactic", precizându-i-se şi forţele asupra cărora deţine această autoritate. Şi în acest caz, însă, se poate produce o diminuare a controlului naţional asupra propriilor forţe întrucât, din punct de vedere practic, "forţele aflate sub OPCOM pot fi angajate în misiuni fără aprobarea autorităţii naţionale, fiind extrase din operaţii numai cu consimţământul celui care exercită comanda". Din această cauză unele state[13] (SUA, de exemplu, dar şi România), reţin comanda operaţională la nivel naţional şi deleagă doar **"controlul operaţional",** (OPCON)[14], adică „autoritatea de a direcţiona forţele alocate, în scopul îndeplinirii misiunilor", ceea ce acoperă, în general, toate aspectele legate de desfăşurarea operaţiilor militare, inclusiv pregătirea comună a forţelor, permiţând comandantului internaţional un control maxim, fără o comandă deplină.

Prin extensie, delegarea autorităţii de **„comandă tactică"** (TACOM)[15] sau de **"control tactic"** (TACON)[16] asupra structurilor naţionale presupune, în general, aplicarea aceloraşi principii ca în cazul OPCOM/OPCON, cu menţiunea că sunt „limitate la direcţionări privind controlul mişcării sau al manevrelor din zona de operaţii, necesare îndeplinirii misiunii", la nivel tactic.

În sfârşit, mai trebuie să subliniem că delegarea comenzii şi controlului în cadrul misiunilor internaţionale este atributul exclusiv al Autorităţii Naţionale de Comandă şi se realizează prin **"transfer de autoritate"** (TOA)[17] către autoritatea de comandă multinaţională desemnată la nivelul alianţei sau coaliţiei.

---

[12] NATO Glossary of Terms and Definitions, AAP-6, Brussels, p.79.
[13] Presidential Decision Directive-25 (PPD-25), 1996, pp.4-6.
[14] NATO Glossary of Terms and Definitions, p.79.
[15] NATO Glossary of Terms and Definitions, p.80.
[16] Ibidem, p.80.
[17] Ibidem, p.87.

Este şi cazul forţelor militare româneşti aflate în misiuni internaţionale, pentru care comanda operaţională se exercită de către Şeful Statului Major General, prin Comandamentul Operaţional Întrunit, iar controlul operaţional este transferat prin delegare de autoritate către comandanţii militari internaţionali desemnaţi de către SHAPE sau comandamentele de coaliţie, pentru fiecare operaţie în parte.

CONCLUZII

Comanda şi controlul sunt elemente esenţiale în orice operaţie sau activitate militară. Bine exercitate, comanda şi controlul înseamnă putere adăugată sau... dezastru, în cazul unor deficienţe. Aranjamentele de comandă trebuie să fie suficient de flexibile, pentru a răspunde unei diversităţi largi de cerinţe, în primul rând politice. În această privinţă, nu există o reţetă universal valabilă care să fie aplicată, fiecare operaţie având specificul său.

Participarea României la misiunile internaţionale din Balcanii de Vest, Irak sau Afganistan, atât în cadrul operaţiilor multinaţionale aliate cât şi al celor de coaliţie, a relevat cu prisosinţă că deşi la nivelul culturii decizionale se manifestă un conservatorism puternic de păstrare a atributelor comenzii centralizate, interpretările actuale converg, din ce în ce mai mult, către ideea delegării responsabilităţilor către eşaloanele subordonate.

SISTEME C4I
DEFINIREA CONCEPTELOR
ŞI EVOLUȚIA ACESTORA

General-maior (r) prof. cons. dr. Constantin MINCU

I. INTRODUCERE

Dezvoltările rapide în tehnologie şi, în special, în domeniul informațional determină schimbări majore în toate planurile activităților umane, inclusiv în cel militar.

Am putea pleca, în demersul nostru, de la afirmația părintelui *Microsoft*, Bill Gates, aceea că „Uneltele erei industriale au extins capacitățile brațelor noastre. Uneltele erei digitale extind capacitățile minții noastre".

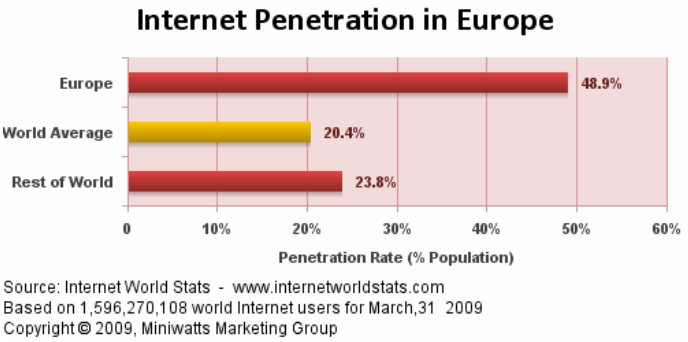
De la debutul mediului de rețele Internet din anii '60 (rețeaua Arpanet dezvoltată şi pusă în funcțiune de către Departamentul Apărării al SUA) şi până astăzi, evoluțiile sunt uriaşe, în întreaga lume, inclusiv în țările mai slab dezvoltate. De la câteva sute de utilizatori, îndeosebi instituții guvernamentale, universități şi institute de cercetare – dezvoltare, s-a ajuns, în decembrie 2008, la un număr de 1,6 miliarde, reprezentând un grad de penetrare de 23,8% din populația globului.

Internet Usage in

	Population (2008 Est.)	% Pop. of World	Internet Users, Latest Data	Penetration (% Population)	User Growth (2000-2008)	Users % Table
Europe	803,903,540	12.0 %	393.373.398	48,9 %	274,3 %	24,6 %
Rest of World	5,906,125,530	88.0 %	1.202.896.71	20,4 %	370,1 %	75,4 %
TOTAL WORLD	6,710,029,070	100.0 %	1.596.270.10	23,8 %	342,2 %	100,0 %

NOTES: (1) European Internet Statistics were updatet for. (2) Population is based on data from the Census Bureau. (3) The usage numbers come from various qualified sources, mainly from data published by Nielsen Online, ITU Gfk, and other trustworthy sources. (4) Data may be cited, giving due credit and establishing an active link back to Internet World Stats. Copyright © 2009, Miniwatts Marketing Group. All right reserved worldwide.

Figura 1. Utilizarea Internetului



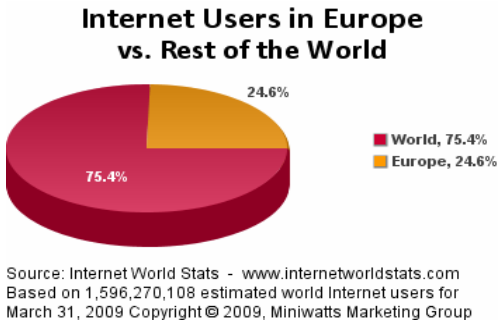


Figura 2. Utilizarea Internetului în Europa

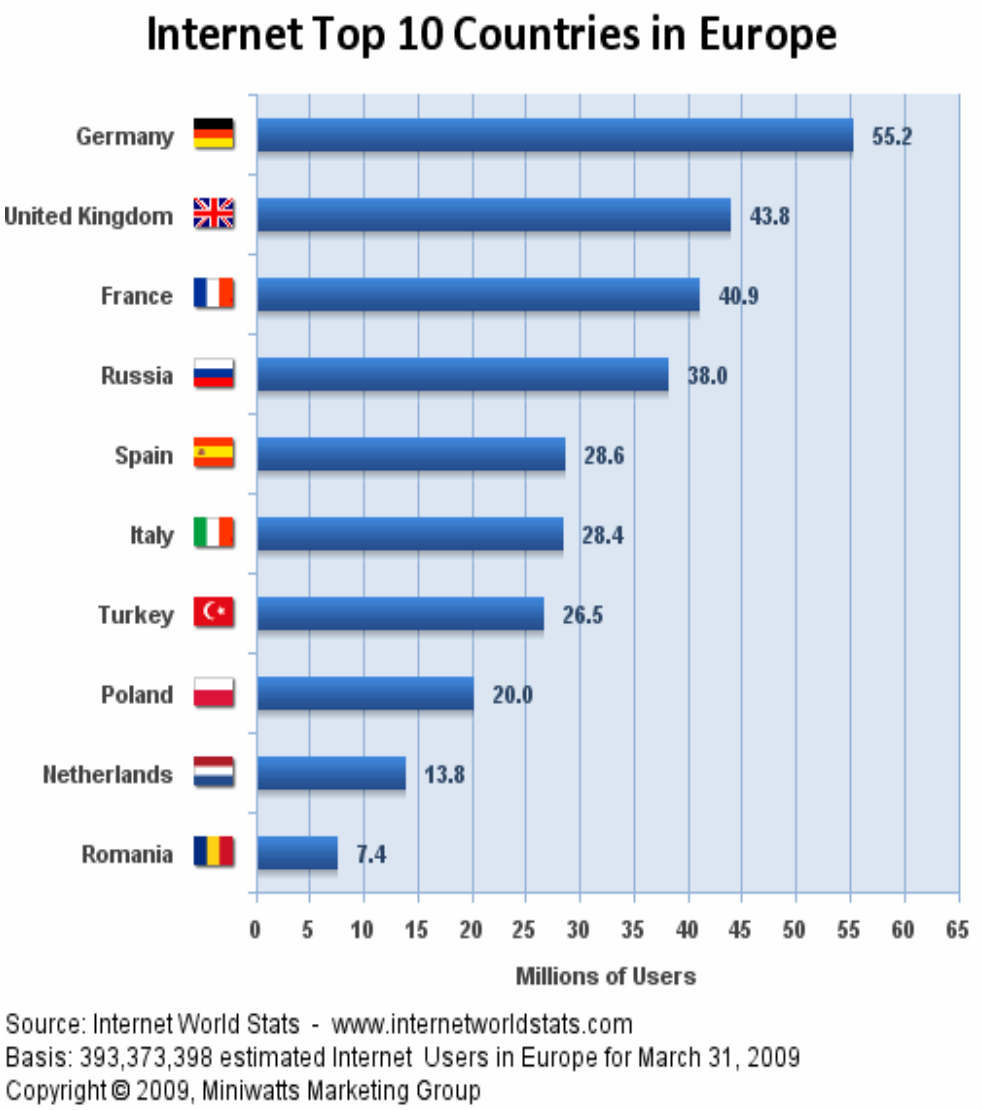

Internet Top 10 Countries in Europe
Germany
55.2
United Kingdom
43.8
France
40.9
Russia
38.0
Spain
28.6
Italy
28.4
Turkey
26.5
Poland
20.0
Netherlands
13.8
Romania
7.4
0 5 10 15 20 25 30 35 40 45 50 55 60 65
Millions of Users
Source: Internet World Stats - www.internetworldstats.com
Basis: 393,373,398 estimated Internet Users in Europe for March 31, 2009
Copyright © 2009, Miniwatts Marketing Group

Figura 3.

Nr. Crt.	Ţara	Populaţia (estimată 2008)	Utilizatori Internet – decembrie 2008	% din populaţie (penetrare)	Creştere (2000 - 2008)
1	Estonia	1.307.605	854.600	65,4 %	133,1 %
2	Slovenia	2.007.711	1.300.000	64,8 %	333,3 %
3	Latvia	2.245.423	1.324.800	59,0 %	783,2 %
4	Lithuania	3.565.205	2.103.471	59,0 %	834,9 %
5	Slovakia	5.455.407	3.018.400	55,3 %	364,4 %
6	Hungary	9.930.915	5.215.400	52,5 %	629,4 %
7	Poland	38.500.696	20.020.362	52,0 %	615,0 %
8	Czech Republic	10.220.911	4.991.300	48,8 %	399,1 %
9	Croatia	4.491.543	1.984.800	44,2 %	892,4 %
10	Macedonia	2.061.315	906.979	44,0 %	2.923,3 %
11	Turkey	75.793.836	26.500.000	35,0 %	1.225,0 %
12	Romania	22.246.862	7.430.000	33,4 %	828,8 %
13	Bulgaria	7.262.675	2.368.000	32,6 %	450,7 %
14	Serbia	8.032.338	2.602.478	32,4 %	550,6 %
15	Bosnia-Herzegovina	4.590.310	1.441.000	31,4 %	20.485,7 %
16	Belarus	9.685.768	2.809.800	29,0 %	1.461,0 %
17	Russia	140.702.094	38.000.000	27,0 %	1.125,8 %
18	Moldova	4.324.450	700.000	16,2 %	2.700,0 %
19	Albania	3.619.778	580.000	16,0 %	23.100,0 %
20	Ukraine	45.994.287	6.700.000	14,6 %	3.250,0 %

Figura 4. Utilizarea Internetului în Europa Centrala şi de Est

Nr. Crt.	Ţara	Populaţia (estimată 2008)	Utilizatori Internet – decembrie 2008	% din populaţie (penetrare)	Creştere (2000 - 2008)
1	Netherlands	16.645.313	13.791.800	82,9 %	253,6 %
2	Iceland	304.367	273.930	90,0 %	63,1 %
3	Sweden	9.045.389	7.295.200	80,7 %	80,2 %
4	Norway	4.644.457	3.993.400	86,0 %	81,5 %
5	Denmark	5.484.723	4.408.100	80,4 %	126,1 %
6	Finland	5.244.749	4.353.142	83,0 %	125,9 %
7	Luxembourg	486.006	363.900	74,9 %	263,9 %
8	United Kingdom	60.943.912	43.221.464	70,9 %	180,7 %
9	Faroe Islands	48.668	37.500	77,1 %	1.150,0 %
10	Switzerland	7.581.520	5.762.700	76,0 %	170,0 %

Figura 5. Top 10 state europene, după rata de penetrare a Internetului

Toate instituţiile unui stat modern (politice, financiare, culturale, educaţionale, ştiinţifice, militare etc.), care stochează şi prelucrează un volum foarte mare de date, utilizând infrastructuri hardware şi un set corespunzător de aplicaţii software, nu se mai pot lipsi de aportul de eficienţă şi competitivitate al tehnologiei IT&C.

Revenind la domeniul militar, putem să observăm şi să analizăm evoluţiile în domeniul sistemelor informaţionale, îndeosebi începând cu anii '70. Progresele importante au fost determinate de mai mulţi factori, printre care enumerăm:

- *dezvoltările tehnologice* în producţia echipamentelor de comunicaţii civile şi militare (miniaturizare, putere, extinderea benzilor de frecvenţe, tipuri de modulaţie, capacităţi de transport mari etc.);
- *creşterea performanţelor computerelor* de toate tipurile (capacităţi de memorie, viteze de prelucrare, utilizare uşoară, miniaturizare, rigidizare etc.);
- *unirea conceptuală,* tehnologică şi operaţională a echipamentelor şi reţelelor de comunicaţii digitale cu echipamentele de calcul electronic şi aplicaţiile software specifice fiecărui domeniu de activitate;
- *presiunile mari asupra structurilor militare de comandă şi control* pentru scurtarea ciclului conducerii şi pentru efectuarea unei analize multicriteriale rapide a unui volum uriaş de date şi informaţii necesare planificării şi conducerii operaţiei (luptei);
- *perfecţionarea senzorilor opto-electronici* şi apariţia unor noi tipuri cu performanţe ridicate, plasate pe diferite platforme, terestre, aeriene, navale, cosmice;
- *apariţia şi dezvoltarea hărţilor* digitale utilizând metode performante de cartografiere prin folosirea fotografiilor aeriene şi cosmice precum şi a capacităţilor de calcul al unor super-computere (în special în cazul SUA);
- *apariţia şi dezvoltarea conceptului de „război informaţional"* şi în consecinţă, a măsurilor de protecţie pentru infrastructura informaţională proprie, concomitent cu distrugerea (afectarea) infrastructurii inamicului;
- *elaborarea* unor noi concepte privind ducerea războiului.

II. DEFINIREA UNOR CONCEPTE ŞI SISTEME

În era informaţională, pe primul plan se situează exploatarea tehnologiei informaţiei şi comunicaţiilor, pentru a facilita dezvoltarea a ceea ce se numeşte în zilele noastre „societatea cunoaşterii", accesul rapid şi simplu a miliarde de oameni la o bibliotecă virtuală uriaşă, diseminată în mii de capacităţi de stocare. Această evoluţie nu avea cum să nu influenţeze puternic mediul militar, mai ales că realizări importante au fost generate sau înfăptuite de reprezentanţi ai multor armate.

În scopul de a evidenția cât mai realist problemele ce decurg din definirea unor concepte şi realități, în domeniul sistemelor informaționale, inclusiv în cel al sistemelor militare, cunoscute acum sub denumirea de C4I (şi variantele dezvoltate în timp), vom încerca unele clarificări, astfel:

- *mediul informațional global* care cuprinde personalitățile, organizațiile, sistemele etc., multe dintre ele în afara cadrului militar sau al autorităților naționale de comandă care colectează, prelucrează şi distribuie informațiile la nivel național şi internațional;
- *infrastructura informațională națională* care cuprinde rețelele de telecomunicații publice şi private, tehnologiile de satelit şi terestre, în special în domeniul comunicațiilor radio şi a celor prin fibră optică, ce livrează informațiile instituțiilor şi la domiciliul persoanelor, informațiile şi conținutul acestora care circulă în infrastructură pentru bazele de date, terminalele hardware şi produsele software pentru accesul la informații, personalul care colectează, stochează, prelucrează şi generează noi informații etc.
- *infrastructura informațională a apărării* care cuprinde resursele necesare pentru transferul, prelucrarea, stocarea şi afişarea informațiilor, mijloacelor tehnice pentru comandă şi control, cercetare şi alte categorii de mijloace pentru transmiterea vocii, imaginilor fixe şi în mişcare, servicii multimedia deosebit de utile sistemului național de apărare;
- *mediul informațional militar* care constă din sistemele informaționale şi structurile organizatorice proprii şi ale adversarului, militar şi de alte categorii, ce sprijină sau influențează în mod semnificativ operațiile militare. Acesta trebuie să asigure servicii pentru conectarea terminalelor de la domiciliu la sistemele din zona de operații, trecerea de la starea de pace la cea de război, asigurarea suportului tehnic pentru comunicații în timp real, necesare pentru îndeplinirea misiunii şi cooperarea între toate categoriile de structuri militare, economice, sociale, politico-administrative locale, zonale şi naționale;
- *sistemele informaționale (C4I)* care constau în infrastructura, structurile organizatorice, personalul şi componentele care colectează, prelucrează, stochează, transmit, afişează, distribuie şi acționează în conformitate cu informațiile obținute. Acestea formează structura care sprijină procesele de stat major, cele de elaborare a deciziilor şi care asigură o imagine comună relevantă, ce contribuie la sincronizare în utilizarea forței, comutarea sistemelor de senzori şi de armament de către comandanți, susține capacitatea de luptă şi protejează activitățile şi sistemele de comandă şi control.

Corelația dintre aceste medii este prezentată în figura 6.

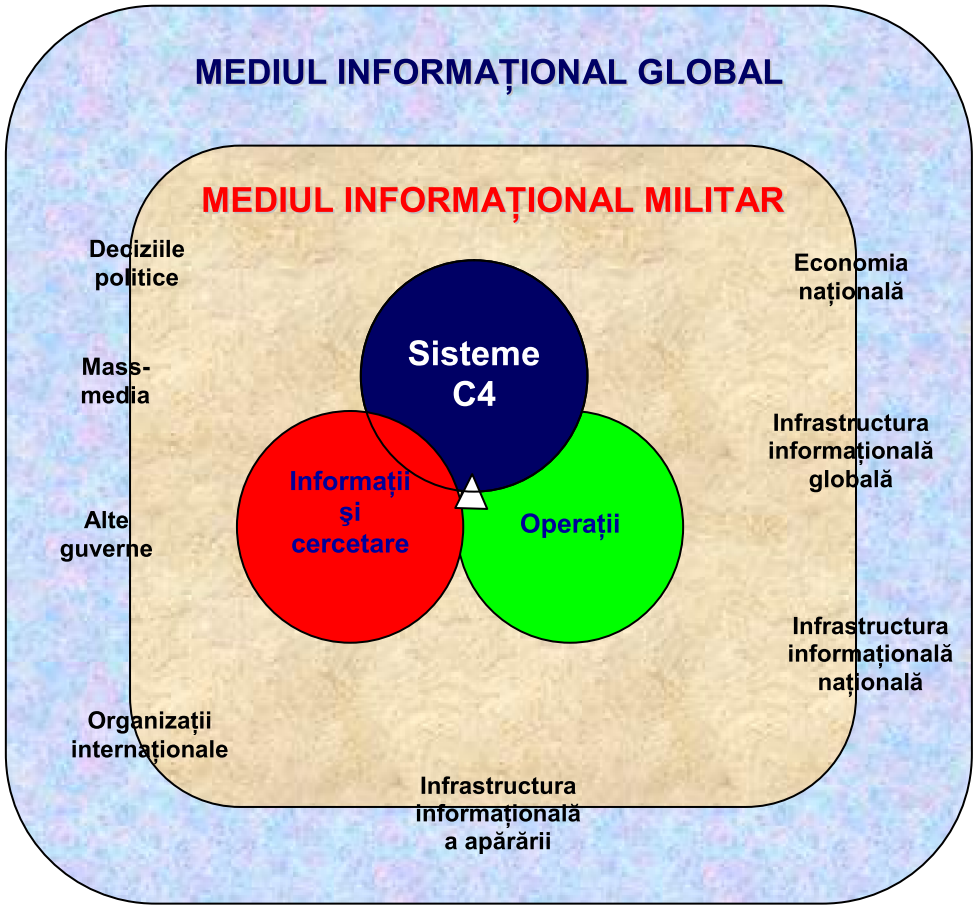


Figura 6. Mediul informațional global şi militar

Dezvoltarea fără precedent din tehnologia informației şi comunicațiilor a creat noi procedee de gestionare şi prelucrare a datelor. Acestea includ imagini, grafică color, scheme, hărți digitale, baze de date care se combină cu tehnici moderne de comunicații (sateliți, stații radio cu salt de frecvență, radiorelee pe microunde, stații radio troposferice şi ionosferice) care desfăşurate, asigură infrastructuri globale, naționale şi militare.

Mediile de desfăşurare a acţiunilor militare s-au diversificat şi au dobândit noi dimensiuni:

- mediul fizic (terestru, aerian, naval, cosmic);
- mediul electromagnetic;
- mediul psihologic;
- mediul cibernetic.

Tipologia câmpului de luptă, după opinia unor specialişti de marcă occidentali, este analizată după criterii conceptuale, psihologice, geografice, fizice, ale sistemelor de comandă şi control, informative etc.

Supremaţia informaţională reprezintă gradul de dominare informaţională care oferă personalului posibilitatea de a utiliza sistemele informaţionale (C4I) pentru a obţine avantaje operaţionale în conflict sau de a controla o anumită situaţie, concomitent cu reducerea posibilităţilor adversarului de a utiliza informaţiile necesare proceselor similare pentru trupele proprii.

Creşterea fluxului informaţional prin utilizarea sistemelor de comunicaţii cu structură distribuită, folosirea unităţilor speciale, a ofiţerilor şi echipelor de cercetare, precum şi inovaţiile din sistemele de senzori, procesoare, comunicaţii şi calculatoare, pot oferi comandamentelor o cunoaştere a situaţiei operative, prin accesul imediat la informaţiile despre adversar şi trupele proprii.

Viziunea câmpului de luptă prin realizarea unei cunoaşteri clare a situaţiei curente a trupelor proprii în conexiune cu cea a adversarului şi condiţiilor de mediu, imaginea situaţiei finale dorite care reprezintă îndeplinirea misiunii, vizualizarea secvenţială a activităţilor care vor conduce forţele proprii din situaţia iniţială până la cea finală.

Cunoaşterea situaţiei prin analiză, însuşirea intenţiei comandantului şi concepţiei luptei (operaţiei) în conexiune cu imaginea clară a disputei şi posibilităţilor adversarului şi forţelor proprii.

Managementul informaţional prin colectarea şi prelucrarea unor cantităţi foarte mari de informaţii, reducerea duratei ciclului de comandă, elaborarea deciziilor în timp scurt.

În realizarea acestor deziderate capitale pentru obţinerea succesului în activităţile militare, un rol foarte important îl au sistemele de comandă, control, comunicaţii, computere şi informaţii (C4I).

Sistemele integrate de tip C4I (+ variante) cuprind doctrine, proceduri, structuri organizatorice, personal, echipamente şi dispozitive auxiliare destinate să-l sprijine pe comandant şi statul său major în exercitarea comenzii şi controlului asupra întregii game de acţiuni de luptă (operativitate).

Pentru o înţelegere cât mai corectă a problemelor referitoare la structura şi funcţionarea acestor sisteme considerăm util să clarificăm terminologia minimală specifică:

- *Comanda (command)* – autoritatea pe care un comandant, în serviciu militar, o exercită în mod legal asupra subordonaţilor săi, în conformitate cu gradul sau atribuţiile sale. Comanda include autoritatea şi responsabilitatea pentru utilizarea eficientă a resurselor la dispoziţie şi pentru planificarea folosirii forţelor militare pentru îndeplinirea misiunilor primite. De asemenea, acesta cuprinde şi responsabilitatea pentru starea de sănătatea, condiţiile de viaţă, moralul şi disciplina personalului subordonat;
- *Controlul (control)* – autoritatea care poate fi exercitată de către comandant asupra unei părţi din activităţile subordonaţilor sau a altor structuri organizatorice subordonate temporar;
- *Comanda şi controlul (command and control)* – autoritatea şi conducerea exercitate de către un comandant desemnat asupra forţelor organice şi subordonate temporar pentru îndeplinirea misiunii. Funcţiile de comandă şi control sunt executate printr-un ansamblu organizat de personal, echipamente tehnice, comunicaţii, aparatură auxiliară şi proceduri utilizate de către comandant pentru planificarea, conducerea, coordonarea, controlul forţelor şi acţiunilor de luptă în scopul îndeplinirii misiunii.

Corelaţiile dintre comandă, leadership şi managent

- Managementul se referă, în primul rând, la alocarea şi controlul resurselor (umane, materiale şi financiare) pentru îndeplinirea obiectivelor. În domeniul militar, managementul este definit ca „*utilizarea unei game largi de tehnici pentru a îmbunătăţii planificarea, organizarea şi desfăşurarea operaţiei (luptei), logisticii, administrării şi achiziţiilor*”. În esenţă, atât managementul cât şi comanda conţin elemente care aparţin leadership-ului, elaborării şi controlului (în sensul de verificare, constatare şi corectare).

În principiu, comanda (în special, identificarea misiunilor ce trebuie îndeplinite şi motivarea lor) cuprinde atât activităţi ce ţin de management (alocarea mijloacelor şi a altor resurse pentru realizarea acestora) şi leadership (repartizarea misiunilor subordonaţilor).

În figura 7 sunt prezentate relaţiile dintre aspectele comenzii (conducerea, elaborarea deciziilor şi controlului) şi cele trei componente de bază (conceptuală, morală şi fizică). Comanda este apreciată drept „capacitatea şi voinţa de a ralia personalul subordonat spre scopul comun în conexiune cu caracterul comandantului care inspiră încredere”.

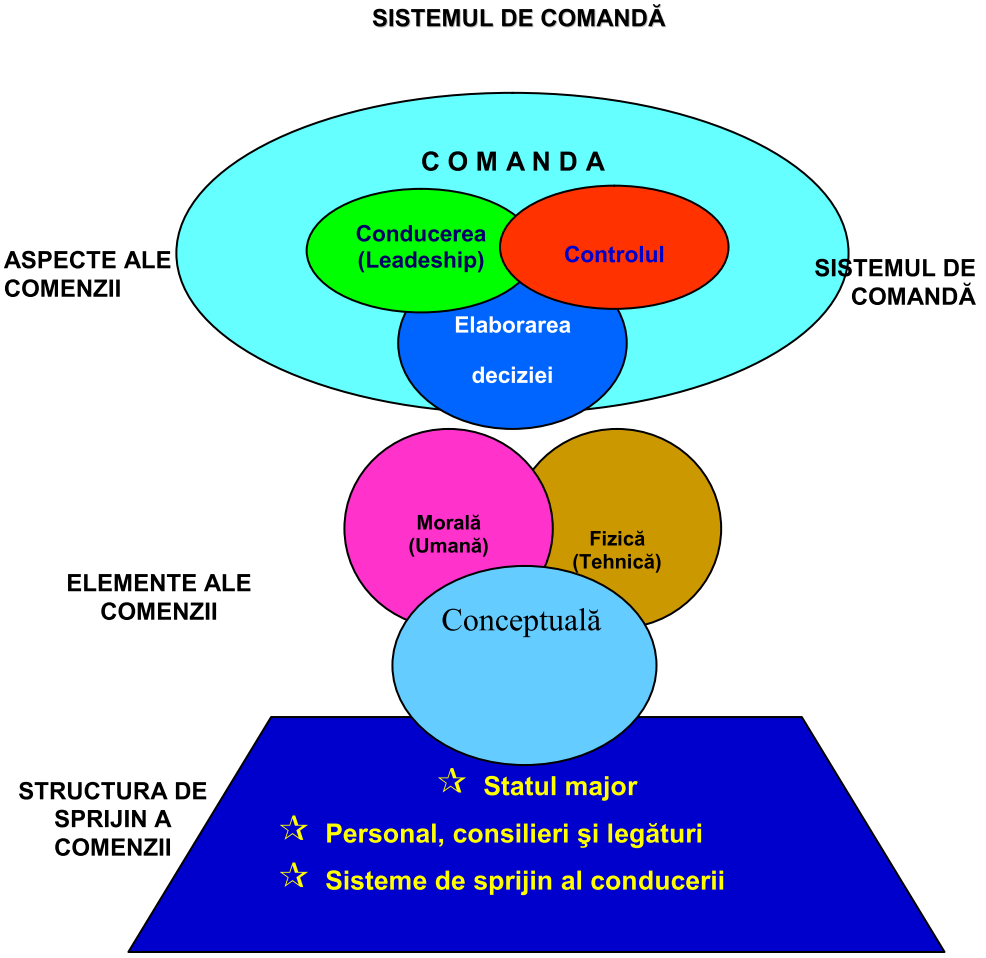


Figura 7. Modelul comenzii

În principiu, ciclul de comandă asistat de sistemele C4I integrate constă din cinci elemente desfăşurate secvenţial:

- *cunoaşterea situaţiei* care cuprinde activităţile de asigurare (colectare), stocate, completate şi validare a informaţiilor;
- *analiza situaţiei* ce include activităţi privind prevederea, compararea şi aprecierea informaţiilor obţinute în prima fază, evaluarea situaţiei

generale, a efectelor acţiunilor curente şi viitoare, proprii şi ale adversarului, capacităţi de luptă şi compararea cursurilor acţiunilor de luptă;

- *planificarea* care cuprinde activităţile de utilizare a rezultatelor din analiza situaţiei şi misiunii, precum şi actualizarea (modificarea) planurilor de acţiune;
- *elaborarea ordinelor de acţiune* ce solicită participarea comandanţilor sau a ofiţerilor desemnaţi de aceştia şi presupune luarea unor decizii prin aplicarea planurilor şi schimbarea intensităţii sau scopului acţiunii;
- *execuţia şi controlul* care urmăresc implementarea deciziei şi presupun legături continue cu eşalonul superior, subordonaţii şi vecinii pentru verificarea îndeplinirii misiunilor.

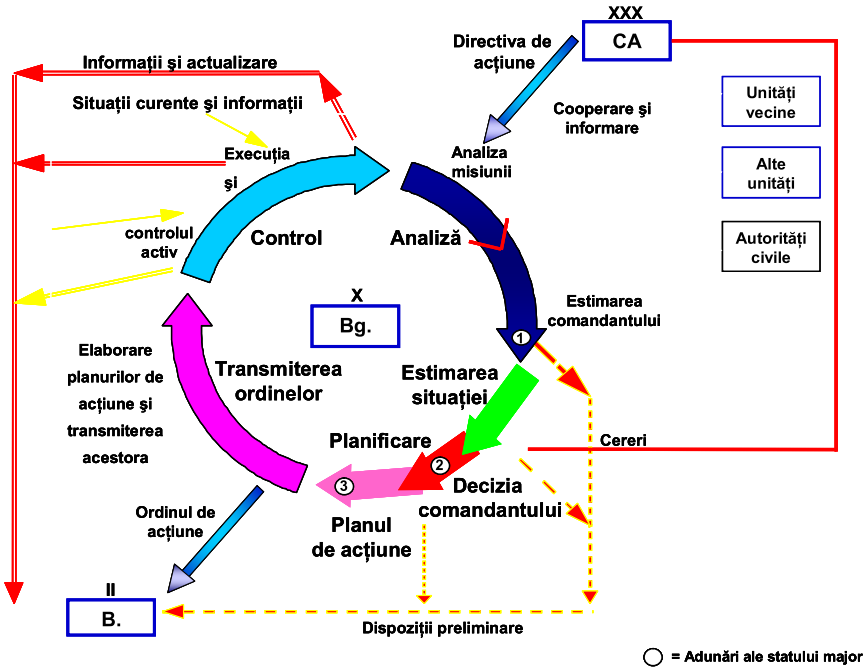


Figura 8. Ciclul de comandă

Activităţile informaţionale implică obţinerea, transportul, prelucrarea, conversia, distribuţia, utilizarea, protecţia, exploatarea şi managementul informaţiilor (figura 9).

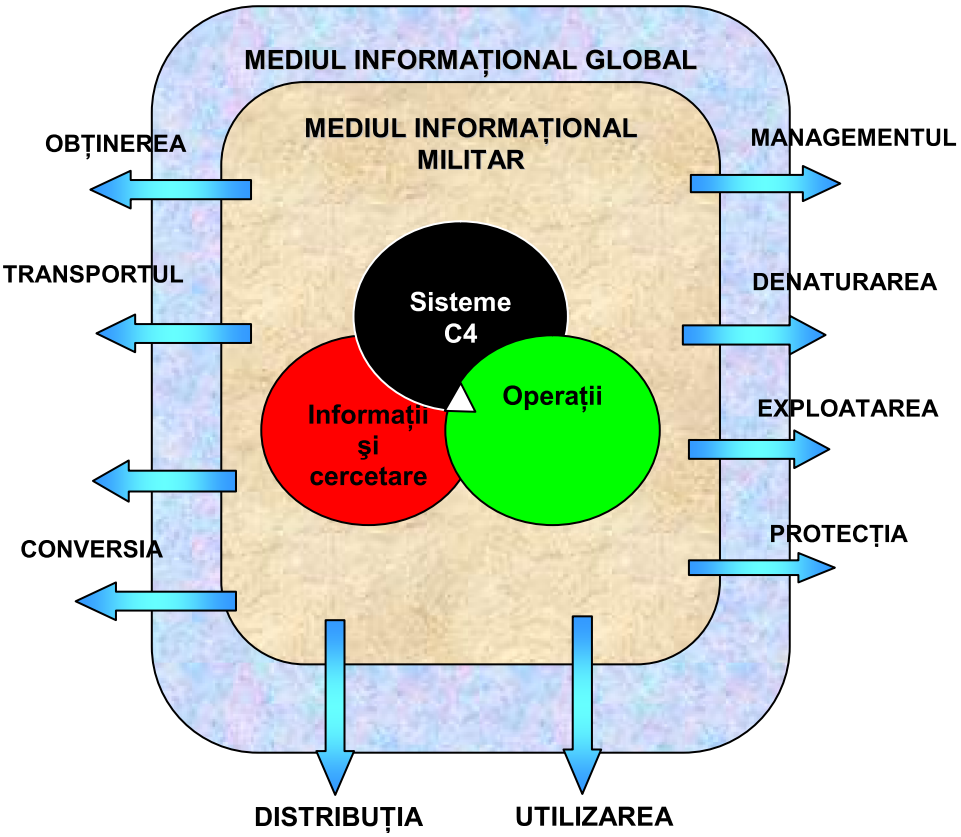


Figura 9. Activităţile informaţionale în sistemele C4I

Colectarea presupune achiziţia (obţinerea) şi filtrarea iniţială a datelor pe baza nevoilor planificate şi prezentarea lor într-o formă adecvată pentru transmitere. Aceste informaţii vizează misiunea, adversarul, trupele proprii, terenul, starea vremii şi timpul la dispoziţie. Procesul de obţinere a informaţiilor se realizează cu ajutorul sistemelor electronice, activităţilor operative de cercetare şi recunoaştere, cercetarea strategică, operativă şi tactică, conlucrarea cu organele de poliţie şi mass-media etc.

Transportul presupune transmiterea sau comunicarea informaţiilor şi datelor la dispozitivele de recepţie destinate.

Prelucrarea datelor constă în stocarea, extragerea din dispozitivele de memorie, actualizarea, filtrarea şi sinteza lor pentru a rezulta minimum de informaţii într-o formă utilizabilă.

Conversia informaţiilor presupune transformarea acestora dintr-o formă în altă formă fără pierderi sau modificarea preciziei lor în scopul transmiterii şi afişării sub formă de text, imagini în format fix şi în mişcare, date pentru calculatoare etc.

Distribuţia (diseminarea) informaţiilor presupune transmiterea informaţiilor prelucrate celor mai potenţiali utilizatori.

Utilizarea informaţiilor (după ce datele sunt obţinute, analizate şi verificate) are drept scop actualizarea şi cunoaşterea situaţiei reale pentru a perfecţiona continuu sau adopta deciziile, planurile şi acţiunile militare.

Protecţia informaţiilor presupune analiza vulnerabilităţii forţelor şi mijloacelor proprii de comandă şi control la acţiunile adversarului de natură electronică, distrugere fizică, inducere în eroare, propagandă precum şi stabilirea mijloacelor, aplicarea şi verificarea măsurilor de contracarare. Elementele de infrastructură ce trebuie protejate sunt bazele de date, reţelele de calculatoare, sistemele de comunicaţii, de cercetare şi mijloacele auxiliare din cadrul acestora.

Exploatarea informaţiei este descrisă drept acţiunea de a obţine avantaje pentru scopurile operaţionale militare din orice informaţie achiziţionată. Aceasta implică interceptarea şi analiza mesajelor adversarului, extragerea informaţiilor din bazele lui de date, întreprinderea măsurilor de denaturare, degradare sau manipulare a capacităţilor informaţionale ale acestuia.

Denaturarea informaţiilor adversarului se realizează prin măsurile de atac la adresa comenzii şi controlului (C2W) şi vizează influenţarea, degradarea sau distrugerea informaţiei şi sistemelor informaţionale (C4I) ale acestuia.

Managementul informaţiei solicită o coordonare şi sincronizare atentă a informaţiilor şi sistemelor informaţionale (C4I) şi cuprind: managementul spectrului electromagnetic, alegerea surselor şi sistemelor ce se utilizează, asigurarea unor fluxuri informaţionale fiabile (cu integrarea pe verticală şi orizontală), interceptarea informaţiilor de la mai multe surse.

Structura sistemelor C4I2 poate fi analizată pe subsisteme, astfel:

- subsistemul de comandă şi control (C2) cu structuri organizatorice pentru realizarea ciclului de comandă şi suportul tehnic şi informaţional aferent;
- sistemul de comunicaţii – echipamente, metode, proceduri şi personal care transmit informaţiile între toate componentele dispozitivului de luptă (operativ);

- reţelele locale şi extinse de calculatoare – suportul hardware şi software pentru prelucrarea, stocarea şi conversia informaţiilor;
- subsistemul de informaţii care colectează, prelucrează şi distribuie informaţiile personalului din statul major (despre inamic, trupele proprii şi mediu);
- interoperabilitatea – cerinţele implementate în componentele tehnice (hardware) şi de programare (software) care să permită interconectarea facilă a elementelor structurale şi transferul informaţional fără impedimente.

Se cunosc mai multe variante de sisteme de comandă şi control integrate:

- *C3I* – Command, Control, Communications and Intelligence = Comandă, Control, Comunicaţii şi Informaţii;
- *C4I* – Command, Control, Communications, Computers and Intelligence = Comandă, Control, Comunicaţii, Computere şi Informaţii;
- *C4I2* – Command, Control, Communications, Computers, Intelligence and Interoperability = Comandă, Control, Comunicaţii, Computere, Informaţii şi Interoperabilitate;
- *C4RISTA* – Command, Control, Communications, Computers Reconnaissance, Intelligence, Surveillance and Target Acquisition = Comandă, Control, Comunicaţii, Computere, Recunoaştere, Informaţii, Supraveghere şi Achiziţia Ţintelor;
- *C4ISR* – Command, Control, Communications, Computers Intelligence, Surveillance and Reconnaissance = Comandă, Control, Comunicaţii, Computere, Informaţii, Supraveghere şi Recunoaştere;
- *C4IFTW* – Command, Control, Communications, Computers, Intelligence For the Warrior = Comandă, Control, Comunicaţii, Computere şi Informaţii pentru luptător;
- *C4IEWS* – Command, Control, Communications, Computers, Intelligence, Electronic Warfare and Sensors = Comandă, Control, Comunicaţii, Computere, Informaţii, Război Electronic şi Senzori etc;
- *C4ISTAR* – ISTAR> informaţii, supraveghere, achiziţia ţintelor şi cercetare.

Comanda şi controlul reprezintă un proces ciclic esenţial prin care acţiunile forţelor militare sunt planificate, conduse, coordonate şi controlate (corectate) pentru a îndeplini o misiune. Acest proces începe cu colectarea informaţiei despre situaţia care este evaluată şi analizată, cursurile de acţiune alternative pentru schimbarea situaţiei în avantajul comandantului şi apoi propuse şi elaborate în formă de planuri, luarea deciziilor privind acţiunile ce vor fi desfăşurate; aprobarea şi aplicarea deciziilor. Acţiunile modifică deci situaţia iniţială şi procesul este reluat. Esenţa procesului o reprezintă luarea deciziilor şi aplicarea lor în timp oportun. Responsabilitatea maximă revine comandantului care solicită sprijinul

statului major privind obţinerea şi asigurarea informaţiilor, analiza şi anticiparea situaţiei, recomandă cele mai potrivite cursuri ale acţiunilor de luptă, pregăteşte planurile, ordinele şi dispoziţiile, aprobă şi dispune diseminarea deciziilor, supervizează şi monitorizează modul de executare a acestora.

La aceste activităţi participă toate compartimentele statului major.

În acest scop se pot constitui următoarele structuri logice (figura 10):

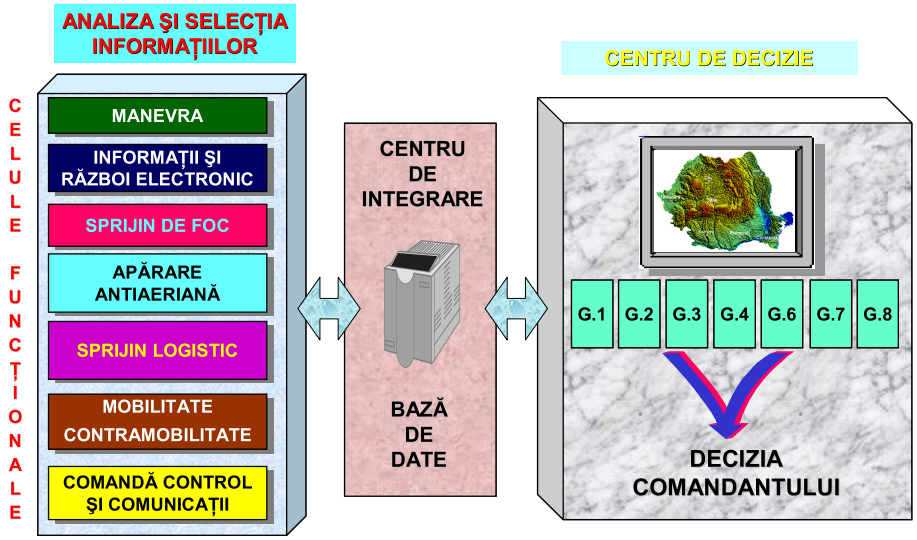


Figura 10. Organizarea logică a unui comandament

▪*un număr de celule funcţionale în cadrul unui centru de analiză şi selecţie a informaţiilor* care depind de tipul comandamentului şi nivelul ierarhic al comenzii;

▪*un centru de decizie* unde comandantul, sprijinit de statul-major, analizează situaţia şi formulează ordine şi dispoziţii;

▪*un centru de sinteză* care asigură servicii informaţionale şi de comunicaţii celulelor funcţionale şi centrului de decizie.

În centrul de analiză şi selecţie a informaţiilor pot funcţiona următoarele celule:

▪*controlul manevrei condusă de G* 3 cu responsabilitatea controlului şi sprijinului acţiunilor de luptă. În acest scop pregăteşte planurile de acţiune şi

ordinele de operaţii, recepţionează, analizează şi aprobă cererile de sprijin aerian, coordonează manevra trupelor în câmpul tactic, ţine evidenţa întrebuinţării unităţilor şi propune folosirea armamentului special;

▪*sprijinul de foc, condusă tot de G 3*, răspunde de planificarea şi coordonarea acestuia, elaborează planurile în acest scop şi urmăreşte aplicarea lor, propune organizarea artileriei terestre şi rachetelor pentru luptă şi priorităţile de lovire a ţintelor inamice;

▪*apărarea antiaeriană (G 3)* care coordonează această activitate şi îndeplineşte funcţiile de control al spaţiului aerian prin actualizarea situaţiei aeriene şi a unităţilor de profil, planificarea şi conducerea focului antiaerian la diferite înălţimi în zona de responsabilitate;

▪*informaţii şi război electronic (G 2)* ce prelucrează şi sintetizează informaţiile de cercetare. Responsabilităţile principale privesc managementul informaţiilor: colectarea, analiza, interpretarea şi distribuirea acestora. De asemenea, cooperează cu alte organe de specialitate din zona de responsabilitate pentru planificarea acţiunilor viitoare;

▪*logistica (G 1 şi G 4)* care realizează managementul resurselor umane, tehnice, materiale şi medicale, a transporturilor şi mentenanţei;

▪*mobilitatea şi contramobilitatea (G 3)* ce ţine evidenţa stării căilor de comunicaţii şi ia măsuri pentru amenajarea genistică a terenului, realizarea trecerilor şi obstacolelor, planificarea şi realizarea distrugerilor şi fortificaţiilor etc.;

▪*comandă, control şi comunicaţii (G 6)* planifică, realizează şi asigură funcţionarea sistemelor de comunicaţii şi informatice, conduc operativ elementele şi unităţile de specialitate.

În acelaşi timp între aceste structuri logice sunt relaţii funcţionale strânse, potenţate de sistemul de legături interioare (prin mijloace de comunicaţii şi staţiile de lucru din reţeaua locală de calculatoare) şi cele exterioare (prin sistemul de comunicaţii) între structurile de conducere şi cele operaţionale (figura 11).

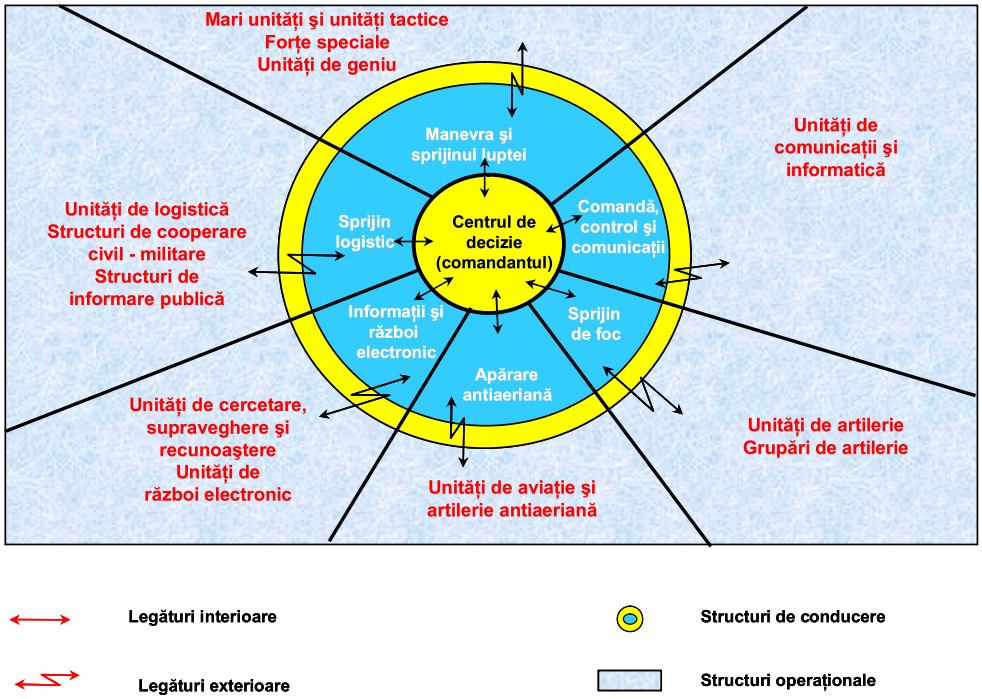


Figura 11. Organizarea funcţională a unui comandament

III. SISTEME C4I (+ VARIANTE) DIN UNELE ARMATE MODERNE (1970 - 2009)

Toate armatele NATO, începând cu anii ’70, au demarat un proces amplu de modernizare a sistemelor de comunicaţii şi informatică (CIS), iar mai târziu, a unor complexe sisteme integrate de tipul C3I (C4I, variante).

Fără a insista prea mult asupra motivelor care au determinat această opţiune, putem vorbi despre următoarea etapizare:

- *Anii ‘70:*

1. Dezvoltarea unor reţele de comunicaţii militare permanente, la început analogice, apoi analogice-digitale mixte şi în final (anii ‘80) digitale (SUA, Franţa, Germania, Italia, Marea Britanie);

2. Creşterea capacităţii transportului de date în detrimentul utilizării comunicaţiilor de voce şi, ca urmare a exploziei reţelelor globale comerciale, denumite generic Internet;

3.Cercetarea, dezvoltarea şi implementarea unor sisteme (reţele) automatizate CIS pentru eşaloanele operative şi tactice, cum au fost:

- M.S.E. – SUA;
- AUTOKO – Germania;
- SOTRIN – Italia
- RITA – Franţa

4.Creşterea rolului comunicaţiilor militare bazate pe:

- HF, VHF şi UHF terestre, aeriene şi navale;
- comunicaţii radio prin sateliţi militari şi civili.

▪ *Anii '80 şi anii '90*

1. Dezvoltarea şi implementarea la toate eşaloanele a unor sisteme puternic integrate de tipul C3I (C4I şi variante)

- promotori: SUA, Marea Britanie, Italia, Franţa, Germania.

2. Apariţia şi utilizarea la trupe a hărţilor digitale, fapt ce a permis un mai mare grad de precizie al mişcării forţelor şi o integrare din ce în ce mai pronunţată a diverşilor senzori opto-electronici;

3. Dezvoltarea unei noi clase de senzori opto-electronici şi integrarea acestora în sistemele de arme, ducând la o mare precizie şi o reacţie în timp real;

4. Aplicarea unor lecţii învăţate din conflictele care au avut loc în lume (îndeosebi de către Armata SUA);

5. Elaborarea unor noi concepte în domeniul C4I (+ variante) în SUA şi la NATO.

▪ *După 1999 şi până în prezent*

1. Dezvoltarea unor concepte noi în cadrul NATO în ceea ce înseamnă NATO ENABLED CAPABILITIES (NEC);

2. Lansarea şi consolidarea conceptului de „Război bazat pe reţea " (Armata SUA după 1999);

3. Creşterea eforturilor NATO de a ridica nivelul armatelor europene din NATO, în domeniul C4I (+ variante) (este şi cazul României);

4. Dezvoltarea conceptului de „reţea de reţele" sau „sistem de sisteme" însemnând un grad cât mai ridicat de compatibilitate (interoperabilitate) între sistemele diferite din aceeaşi ţară şi între sisteme ale aliaţilor;

5. Creşterea rolului comunicaţiilor VoIP după modelul reţelelor comerciale (INTERNET);

6. Perfecţionarea mijloacelor fizice şi electronice de protecţie a comunicaţiilor de voce şi date;

7. Utilizarea mult mai largă a sistemelor GPS atât în planificarea sistemelor C4I, cât şi în folosirea sistemelor de arme.

IV. CONCLUZII

1. Armatele statelor membre NATO (şi nu numai) acordă resurse financiare şi umane considerabile pentru consolidarea unor capacităţi C4I (+ variante) la toate nivelurile ierarhice, pentru toate categoriile de forţe şi în toate mediile de ducere a acţiunilor de luptă (în Armata SUA, anual, un procent de 10 – 14 % din bugetul destinat înzestrării merge spre această zonă).
2. Se fac progrese mari în implementarea „capabilităţilor de război bazate pe reţea”. În SUA, acţiunea a demarat în forţă în 2002 cu o alocare bugetară de 7 miliarde de dolari până în 2009.
3. Modelul internetului pătrunde tot mai repede în reţelele militare. Luptătorul va căuta informaţia dorită utilizând un motor de căutare similar cu, de exemplu, Google pe Internet (trecerea de la împingerea informaţiei la extragerea informaţiei).
4. Se dezvoltă, după modelul soluţiilor comerciale, sistemele de calcul distribuite, bazele de date distribuite şi aplicaţiile de colaborare complexe.
5. Cercetătorii şi cei implicaţi în dezvoltările tehnologice şi militare acţionează pentru dezvoltarea unor sisteme (reţele) care au controlul securităţii şi al configurării.

INFLUENȚELE RĂZBOIULUI BAZAT PE REȚEA ŞI A CAPABILITĂȚILOR FACILITATE DE REȚEA ASUPRA SISTEMELOR C4ISR

Colonel (r) prof. univ. cons. dr. Gruia TIMOFTE

În mod particular, războiul actual în care calculatoarele au fost implementate în sistemele de armament şi de comunicații are o vechime de numai 30 de ani. În zilele noastre, calculatorul este omniprezent şi utilizat în aproape orice domeniu al societății moderne. Această tendință este cunoscută sub denumirea mai cuprinzătoare de *tehnologia informației şi comunicațiilor.*

Primul calculator electronic programabil, numit Robinson, a fost inventat în Anglia în anul 1940. Acesta a fost utilizat, în principal, pentru spargerea codurilor de cifrare germane. Trei ani mai târziu a apărut calculatorul numit Colossus care avea o viteză de lucru de o mie de ori mai mare. Din 1946, utilizarea calculatorului s-a extins de la aplicațiile militare spre preocupări ştiințifice. Compania americană IBM a realizat modelul 701, numit inițial „calculator pentru apărare", care a primit imediat 18 comenzi pentru utilizare în proiectarea aeronavelor, motoarelor cu reacție şi alte aplicații care solicitau operațiuni repetitive.[1] Din motive de siguranță, capacitățile de calcul au fost orientate spre cercetările privind armele nucleare,[2] dar, în acelaşi timp, sistemele informatice pentru managementul afacerilor şi inventarea

[1] http://www-03.ibm.com/ibm/history/exhibits/701/701_intro.hthl

[2] Wineguard D., Akera A., "A Short History of the Second American Revolution," *University of Pennsylvania Almanac*, v.42, no.18, January 30, 1996, p.6.

limbajelor software au validat ideea că invenţiile din timp de război produc aplicaţii comerciale. Creşterea exponenţială a numărului de calculatoare nu a fost prevăzută, în special în afara comunităţilor ştiinţifice.

Apariţia echipamentelor cu circuite integrate şi componente discrete la sfârşitul anilor 1960 a declanşat o evoluţie rapidă în comunicaţiile pentru câmpul de luptă în următoarele două decenii. Comunicaţiile tactice nu erau automatizate în sensul utilizării calculatoarelor, programelor specializate sau interconectării automate.

În 1965, fizicianul Gordon Moore, co-fondator al Intel, a prevăzut că numărul de tranzistori pe un circuit integrat se va dubla la fiecare interval de 18 luni şi că această tendinţă va continua pentru un viitor previzibil. Moore şi cei mai mulţi experţi se aşteaptă ca această lege să rămână valabilă pentru încă cel puţin două decenii.

Calculatorul personal (PC) a fost introdus în mediul comercial de către IBM în anul 1981. Au fost dezvoltate protocoalele de transfer al fişierelor (FTP şi apoi TCP/IP)[3] şi, în curând, a fost realizat un model cu 7 niveluri pentru transferul datelor prin reţele cu mai multe calculatoare. Într-adevăr, avea loc maturizarea Internetului, împreună cu schemele grafice şi limbajul HTML, pentru a realiza World Wide Web la începutul anilor `90. Înainte de această perioadă, foarte puţine persoane aveau o adresă de e-mail sau un site web prin care să fie contactaţi. În „Furtuna Deşertului" nu s-a utilizat pe scară largă e-mail-ul, dar creşterea exponenţială a numărului de calculatoare personale, a mesajelor de poştă electronică şi a site-urilor web avea să înceapă doi ani mai târziu. Era războiului bazat pe reţea era la debut.

Din punct de vedere lingvistic, sistemul C4I s-a născut la începutul anului 1990. Calculatorul a fost introdus la nivelul corpului de armată şi eşaloanele subordonate la sfârşitul anului 1970. Tot în 1970, telefoanele comerciale au fost dotate cu tastatură (cu două tonuri, multifrecvenţă). Comutatoarele conduse prin calculator ofereau apel cu mai multe frecvenţe, precum şi apeluri cu preempţiune şi căi de rutare de rezervă. Acest sistem nou de comutaţie împreună cu un sistem radio terestru a devenit cunoscut ca sistem radio de abonat mobil.

În prezent puterea de prelucrare a calculatoarelor (computaţia) a ajuns la valori de $1456x10^{12}$ operaţii pe secundă cu 129.600 procesoare. În Internet, una din cinci persoane de pe glob navighează în această reţea de reţele, iar numărul de telefoane mobile a depăşit 4 miliarde.

[3] http://www.cisco.com/univercd//cc//td/doc/cisintwk/ito_doc/ip.htm

De altfel, observaţiile pe durata a 100 de ani (1920-2020) demonstrează că tehnologia continuă să avanseze într-un ritm exponenţial, transformările tehnologice sunt modele care nu pot fi previzionate în intervale de 20 de ani, sursele de investiţii pot alterna între sectorul privat şi cel guvernamental, iar războaiele apar la intervale impredictibile.

Lărgimea de bandă reprezintă unitatea de măsură a cantităţii de date transmise în unitatea de timp. Un articol recent menţiona: "În Primul Război Mondial, capacităţile de comunicaţii militare ale SUA erau de 30 cuvinte pe minut. În cel de-al Doilea Război Mondial acestea au fost de circa 60 de cuvinte. În Vietnam, au fost puţin peste 100 de cuvinte. În 2010 se preconizează să fie de $1,5x10^{12}$ cuvinte pe minut în cadrul unui teatru de operaţii. Aceasta reprezintă echivalentul Bibliotecii Congresului în fiecare minut. Undeva în acest volum se află şi informaţiile unui batalion, componentă a forţei întrunite sau comandantului acesteia".[4]

Pentru a satisface cerinţele comandantului, arhitectura sistemului C4ISR trebuie să includă tehnologiile din generaţia următoare. Multe din aceste tehnologii sunt, de fapt, vizualizate ca părţi ale reţelei informaţionale globale şi sistemelor de luptă ale viitorului. Acestea sunt planificate să fie implementate în intervalul 2013-2020. Ceea ce nu pot fi niciodată previzionate sunt tehnologiile disruptive, precum World Wide Web de la începutul anilor `90, de exemplu. Tehnologiile disruptive sunt acelea care realizează noi produse prin noi metode (căi). Iniţial, acestea pot costa mai mult şi pot fi mai puţin eficiente decât cele mult mai mature („tehnologii de susţinere"). Sau eventual, acestea devin mult mai ieftine şi mai bune astfel încât scot de pe piaţă vechile tehnologii.

1. Mediul informaţional

Noul mediu informaţional constă dintr-o combinaţie de personal, organizaţii şi sisteme care colectează, prelucrează diseminează sau acţionează asupra informaţiilor.[5] În cadrul acestuia personalul şi sistemele automatizate observă, se orientează, decid şi acţionează conform informaţiilor şi, de aceea, reprezintă mediul principal de elaborare a deciziilor. Acesta este constituit din trei dimensiuni interdependente, astfel (figura 1):

[4] Rogers M., "C4I Interoperability for Our Warfighters," *Military Information Technology*, 7 iss.10 (December 31, 2003).
[5] Joint Publication 3-13, *Information Operations*, Department of Defense, Washington, D.C., 2006, p.I-6.

- dimensiunea fizică – compusă din sistemele de comandă şi control şi infrastructura de sprijin care permite conducerea operaţiilor în toate mediile. În aceasta se găsesc platformele şi reţelele de comunicaţii care le interconectează;
- dimensiunea informaţională – în care se colectează, prelucrează, stochează, disemineză, afişează şi protejează informaţiile. În aceasta se exercită comanda şi controlul, se transmite intenţia comandantului, se găsesc fluxurile de informaţii cu conţinutul aferent;
- dimensiunea cognitivă cuprinde mintea factorilor de decizie şi a celor cărora li se adresează aceştia. Este dimensiunea în care oamenii gândesc, percep, vizualizează şi decid. Reprezintă cea mai importantă dimensiune dintre cele trei prezentate şi este afectată de ordinele comandanţilor, nivelul de instruire şi alte motivaţii personale. Luptele şi campaniile pot fi pierdute în acest domeniu. Această dimensiune este influenţată de factori ca leadership-ul, moralul, unitatea de acţiune, emoţiile, starea de spirit, nivelul de instruire şi experienţă, cunoaşterea situaţiei, precum şi de opinia publică, percepţii, mass-media.

Dimensiunea fizică	- Locul unde mediul informaţional se suprapune peste lumea reală. - Sisteme şi reţele informaţionale. - Elemente caracteristice: sistemele de comunicaţii şi calculatoare, precum şi infrastructura de sprijin.
Dimensiunea informaţională	- Locul unde informaţia este colectată, prelucrată, stocată, diseminată, afişată şi protejată. - Natură dublă: informaţia însăşi şi mediul specific. - Interconectează dimensiunile fizică şi cognitivă. - Caracteristici esenţiale: conţinutul informaţiei şi fluxului informaţional, calitatea informaţiei.
Dimensiunea cognitivă	- Locul unde are loc elaborarea deciziei cu sprijinul mijloacelor automatizate. - Locul unde are loc elaborarea deciziei de către oameni. - Dimensiuni intangibile precum moralul, unitatea de acţiune, opinia publică, cunoaşterea situaţiei. - Caracteristici esenţiale: percepţii, emoţii, cunoaştere şi înţelegere.

Figura 1. Mediul informaţional

Dezvoltările din tehnologie permit ca informaţiile să fie colectate, prelucrate stocate, diseminate, afişate şi protejate în afara procesului cognitiv în cantităţi şi la viteze imprevizibile anterior. În timp ce tehnologia pune la dispoziţia opiniei publice cantităţi mari de informaţii, factorii care afectează percepţia asigură contextul pe care indivizii îl utilizează pentru a transforma datele în informaţii şi cunoştinţe.

Există criterii care definesc calitatea informaţiei în raport cu scopurile urmărite. Varietatea scopurilor solicită aplicarea diferită a criteriilor de evaluare. În plus, fiecare decizie se bazează pe evaluarea diferenţiată a criteriilor de calitate în scopul de a elabora cea mai bună decizie.

De asemenea, timpul şi resursele limitate trebuie să fie luate în considerare în ceea ce priveşte obţinerea informaţiei. În plus, există costuri reale asociate cu calitatea informaţiei obţinute privind realizarea scopului, precum şi a proceselor de obţinere, prelucrare, stocare, transport şi distribuţie a acesteia.

2. Războiul bazat pe reţea şi capabilităţile facilitate de reţea

Abordarea războiului bazat pe reţea (RBR) reprezintă manifestarea conceptelor erei informaţionale în domeniul militar. Studiile efectuate au demonstrat că interconectarea forţelor în reţea le permite acestora să îndeplinească o gamă diferită de misiuni cu eficienţă şi eficacitate maxime.[6] RBR implică colaborarea şi partajarea informaţiei pentru a oferi cele mai potrivite mijloace pentru a fi întrebuinţate de către comandanţi pe timpul desfăşurării operaţiilor.[7] Obiectivele războiului bazat pe reţea includ următoarele: autosincronizarea sau aplicarea măsurilor necesare fără a mai primi ordinele tradiţionale, îmbunătăţirea înţelegerii intenţiei comandantului eşalonului superior şi a situaţiei operaţionale la toate nivelurile de comandă, creşterea abilităţii de a pătrunde în cunoştinţele comune ale forţelor proprii şi de coaliţie pentru a reduce "ceaţa şi fricţiunea" utilizate frecvent în descrierea luptei.[8]

---

[6] Dr. Kimberly Holloman, Evidence Based Research, Inc., "The Network Centric Operations Conceptual Framework," *Presentation at the Network Centric Warfare 2004 Conference*, Washington, D.C., Jan. 20,
2004, [http://www.oft.osd.mil/library/library.cfm?libcol=2].

[7] U.S. Department of Defense, *Report on Network Centric Warfare*, 2001, [http://www.defenselink.mil/nii/NCW/ncw_sense.pdf] , and Ret. Admiral Arthur Cebrowski, Speech to Network Centric Warfare 2003 Conference, January 2003, [http://www.oft.osd.mil].

[8] "Ceaţa" reprezintă termenul care descrie incertitudinea privind ceea ce se va întâmpla pe timpul luptei, în timp ce "fricţiunea" este termenul care descrie dificultatea transpunerii intenţiei comandantului în acţiunile din câmpul de luptă.

Elementele esenţiale ale implementării RBR cuprind următoarele: îmbunătăţirea regulilor şi teoriei RBR prin simulare, testare, experimentare şi experienţa de luptă; aplicarea teoriei RBR pe scară largă în organizaţiile militare; accelerarea interconectării în reţea a forţei întrunite; accelerarea implementării conceptelor şi capabilităţilor bazate pe reţea; experimentarea conceptelor bazate pe reţea pentru a dezvolta noi modalităţi de a conduce RBR; soluţionarea provocărilor care pot apărea în utilizarea RBR cu forţele de coaliţie; dezvoltarea doctrinei şi tacticilor potrivite pentru RBR.

Tehnologiile care sprijină RBR. Unii observatori au remarcat că preţul intrării în operaţiile specifice RBR îl reprezintă realizarea unei reţele de senzori. De exemplu, aeronavele şi alte platforme devin senzori şi oferă noi capabilităţi de a comunica şi combina datele, iar multe sisteme de armament nu mai sunt considerate simple muniţii, ci devin părţi ale sistemului de senzori şi sunt ghidate spre ţinte până când explodează.

Arhitectura reţelei. RBR este în mare măsură dependent de interoperabilitatea echipamentelor de comunicaţii, datelor şi software-ului pentru a facilita interconectarea personalului, senzorilor şi platformelor deservite şi nedeservite. O parte din tehnologiile RBR se bazează pe liniile radio cu vizibilitate pe microunde, în infraroşu sau laser. O altă parte de tehnologii prelucrează informaţiile pentru transmiterea pe magistrale de mare capacitate, prin fibră optică, radiorelee pe microunde sau sateliţi la joasă şi înaltă altitudine. Planificarea utilizării acestor tehnologii trebuie să permită comunicaţii rapide între persoane din toate categoriile de forţe, partajarea rapidă a datelor şi informaţiilor între platformele mobile şi senzorii utilizaţi de categoriile de forţe. Arhitecturile trebuie să aibă abilitatea de autoconfigurare dinamică şi restructurare a reţelei când unul sau mai multe centre sunt scoase din funcţiune.

- *Sateliţii.* Sateliţii sunt esenţiali pentru realizarea comunicaţiilor mobile în zone îndepărtate, precum şi pentru asigurarea imaginilor, navigaţiei, informaţiilor despre vreme, capabilităţilor de avertizare privind atacurile cu rachete şi comunicaţiile cu comandamentele îndepărtate pentru sprijin suplimentar. Sistemul de poziţionare globală (GPS), constituit din 28 de sateliţi de navigaţie, ajută la identificarea şi localizarea forţelor, precum şi a ţintelor pentru întrebuinţarea armamentului (de exemplu: a rachetelor de croazieră). Oricum, chiar dacă numărul de sateliţi militari a crescut, până la 84% din comunicaţiile prin satelit asigurate în OIF au provenit de la cei comerciali.[9]

[9] Jefferson Morris, "GAO: DOD Needs New Approach to Buying Bandwidth," *Aerospace Daily*, Dec. 12, 2003; "DISA Chief Outlines Wartime Successes," *Federal Computer Week*, June 6, 2003.

Lărgimea de bandă radio. Digitalizarea comunicaţiilor reprezintă o componentă esenţială a programului de transformare a forţei militare. Tehnologia digitală face ca utilizarea spectrului de frecvenţe să se realizeze mult mai eficient decât în cazul tehnologiei analogice. Oricum, începând cu anul 1991, există o creştere explozivă a cerinţelor de bandă de frecvenţe, datorită eforturilor de a creşte viteza de livrare a informaţiilor digitale. Oficialităţile din domeniul apărării sunt preocupate de modul în care banda de frecvenţe radio la dispoziţie pentru sistemele militare va creşte corespunzător în raport cu cerinţele de viitor.

Vehiculele nedeservite. Acestea, cunoscute de asemenea ca vehicule aeriene fără pilot, vehicule terestre şi vehicule subacvatice sunt, în principal, utilizate pentru supraveghere, deşi misiunile lor implică şi folosirea în luptă.[10]

Circuite integrate pentru procesoare. Legea lui Gordon Moore despre circuite integrate prevede că, la fiecare interval de 18 luni, acestea vor deveni de 2 ori mai dense şi mai rapide la aproximativ acelaşi preţ de cost, aceasta însemnând că vor fi de 4 ori mai puternice. Ramurile industriale care utilizează tehnologia calculatoarelor se bazează pe această lege pentru realizarea investiţiilor în sisteme tehnologice viitoare.

Nanotehnologia. Noile materiale realizate prin nanotehnologie pot schimba echipamentele din spaţiul de luptă într-un mod greu de imaginat. Sistemele de armament pot deveni mai mici şi mai uşoare, iar noile reţele miniaturizate de senzori pot detecta, localiza, identifica, urmări şi lovi ţintele potenţiale mult mai eficient. Oricum şi alte ţări realizează cercetări şi progrese în acest domeniu. În 2000, în 18 ţări din Asia, 25.000 persoane s-au pregătit prin doctorat în domenii aferente nanotehnologiei, în timp ce în SUA numărul acestora a fost mai mic de 5.000.[11]

Software. Software-ul reprezintă o componentă importantă în toate sistemele complexe de apărare utilizate în RBR. Mulţi analişti din industria de software cred că globalizarea economiilor determină un proces global de dezvoltare a software-ului.

Oricum, tehnologia reprezintă numai unul din elementele de putere ale RBR. Alţi analişti declară că RBR solicită schimbări în comportament, prelucrare şi organizare pentru a transforma dezvoltarea capabilităţilor erei informaţionale în putere de luptă. Prin noile utilizări ale tehnologiilor RBR, conceptele inflexibile sunt transformate în concepte dinamice care pot asigura o nouă şi avantajoasă flexibilitate pentru acţiunile de luptă. Uneori, personalul poate să nu utilizeze

[10] Adam Herbert, "New Horizons for Combat UAVs," *Air Force Magazine*, Dec. 2003.
[11] CRS Report RS20589, *Manipulating Molecules: The National Nanotechnology Initiative*.

integral capabilităţile noilor sisteme deoarece nu s-au adaptat la cerinţele noi de comportament.[12]

Avantajele RBR. Literatura care apare sprijină teoria că puterea este din ce în ce mai mult derivată din partajarea informaţiei, accesul la aceasta şi viteza de transmitere. Acest punct de vedere a fost confirmat de rezultatele obţinute în experienţele operaţionale recente arătând că atunci când forţele sunt într-adevăr întrunite, cu capabilităţi complet integrate şi acţionând conform principiilor RBR, ele pot exploata pe deplin avantajele războiului erei informaţionale. Câteva din avantajele militare ale operaţiilor din cadrul RBR sunt următoarele:

(1) Forţele interconectate pot consta din unităţi de dimensiuni mici care se pot deplasa mai uşor şi mai repede, aceasta însemnând efective mai reduse cu mai puţine platforme şi logistică minimă care pot îndeplini eficient o misiune cu costuri reduse.

(2) Forţele interconectate pot lupta utilizând noi tactici. În timpul OIF, forţele din trupele de uscat ale SUA s-au deplasat într-un asemenea mod care a fost descris ca „tactica roiului". Deoarece interconectarea la reţea permitea militarilor să se urmărească unul pe altul, forţele au putut înainta dispersat, în unităţi mici, independente, eludând necesitatea de a menţine o formaţie compactă. Toate unităţile cunosc locaţia celorlalte. Dacă o unitate întâmpină o dificultate, alte unităţi independente din apropiere pot sosi rapid în ajutorul acesteia, „roind" pentru a ataca inamicul din toate direcţiile concomitent. Beneficiile pot fi următoarele: (1) sunt necesare mai puţine efective şi mai puţine echipamente, astfel ducerea războiului este mai puţin costisitoare; (2) este mai greu pentru un inamic să atace eficient o formaţiune larg dispersată; (3) unităţile luptătoare pot acoperi mai mult teren, deoarece nu trebuie să menţină o formaţie sau să micşoreze ritmul de deplasare urmărind vehiculele; (4) cunoaşterea locaţiei tuturor unităţilor proprii reduce fratricidul pe timpul acţiunilor de luptă; şi (5) tactica „roiului" permite ca un atac să fie direcţionat drept în structura de comandă a inamicului, subminând sprijinul acestuia prin acţiuni din interior, decât să ducă lupte numai la periferie.

(3) Modul în care soldatul individual gândeşte şi acţionează pe câmpul de luptă se schimbă, de asemenea. Când o unitate întâmpină o dificultate în teren, ei comunică prin radio cu Centrul de operaţii tactice, privind tipul de problemă, utilizând chat-ul online. Problema este analizată de către experţi care pot fi localizaţi oriunde există conexiuni la reţea.[13]

---

[12] Frederick Stein, Senior Engineer, MITRE Corporation, *Presentation on Network Centric Warfare Operations*, 4th Annual Multinational C4ISR Conference, McLean, Virginia, May 6, 2004.

[13] Joshua Davis, "If We Run Out of Batteries, This War is Screwed," *Wired Magazine*, June 2003, [http://www.wired.com/wired/archive/11.06/battlefield.html].

(4) Timpul senzor-trăgător este redus. Utilizând sistemele RBR, soldaţii din teren au capabilitatea de a realiza o „analiză la faţa locului" a informaţiilor primare de la display-urile senzorilor, decât să aştepte întoarcerea raportului de analiză de la punctele de comandă distante.[14]

Supraestimarea informaţiilor. Unii analişti susţin că tehnologia erei informaţionale face timpul şi distanţa mai puţin relevante şi că informaţiile cresc viteza de derulare a evenimentelor şi tempoul operaţional al războiului.[15] Alţii cred că interconectarea pentru schimbul informaţional nu este un substitut suficient pentru manevra în luptă şi că superioritatea informaţională şi cunoaşterea situaţiei nu sunt cele mai semnificative componente ale puterii de luptă. Ca în jocul de şah, aceştia din urmă cred că prin cunoaşterea următoare a mişcării se asigură succesul în luptă (de exemplu: prin analiza corectă a mişcărilor anticipate şi a tacticii inamicului).[16]

Alţi observatori declară de asemenea că resursele informaţionale uriaşe pot fi supraestimate ca pe un mijloc de desfăşurare eficientă a operaţiilor militare şi că deciziile militare importante nu pot conduce totdeauna la o analiză raţională bazată pe informaţii. Unele probleme ridicate de către aceştia cuprind mai multe aspecte.

(1) Schimbările cantitative în informaţii şi analiză conduc deseori la schimbări calitative în comportamentul individual şi organizaţional care sunt uneori contraproductive.

(2) Bazarea pe sisteme informaţionale sofisticate poate conduce la o încredere excesivă în management.

(3) Informaţiile bogate, un mediu bogat în oportunităţi pot modifica valoarea informaţiilor, redefini obiectivele misiunii şi conduce la posibila creştere a şanselor pentru consecinţe inacceptabile.

Interoperabilitatea. Se ridică unele probleme dacă organizaţiile militare pot realiza adevărate reţele şi sisteme care să asigure interoperabilitatea între toate structurile şi categoriile de forţe.

Limitările determinate de banda de frecvenţe. Se ridică întrebarea dacă banda de frecvenţe pentru comunicaţii va satisface cerinţele viitoare din ce în ce mai mari. Când problema devine critică se impune stabilirea de priorităţi în transmiterea mesajelor, ceea ce defavorizează unele categorii de utilizatori, dar menţine sistemul funcţional.

---

[14] U.S. Department of Defense, Office of the Secretary, *Unmanned Aerial Vehicles Roadmap*, 2002-2007, Dec. 2002.

[15] David Alberts, John Garstka, Frederick Stein, *Network Centric Warfare*, DOD Command and Control Research Program, Oct. 2003, p. 21.

[16] Edmund Blash, USAR, "Network-Centric Warfare Requires a Closer Look," Signal Forum, *Signal Magazine*, May 2003.

Fabricarea în exterior şi transferul de tehnologie. O creştere a utilizării forţei de muncă din alte ţări pentru tehnologii înalte, incluzând programarea calculatoarelor şi fabricarea de circuite integrate poate conduce la un transfer de cunoştinţe şi tehnologie cu efecte negative asupra superiorităţii tehnice şi avantajelor RBR. Grupul Gartner a determinat că firmele americane au cheltuit pentru servicii de tehnologia informaţiei în străinătate 1,8 miliarde de dolari în 2003 şi 26 miliarde de dolari în 2007 (în special în India şi China).[17]

Programele militare esenţiale

În 2004, oficialii de la Pentagon au utilizat o listă de programe de înaltă tehnologie "Net-Centric Checklist" care a inclus şi capabilităţi bazate pe reţea pentru platforme militare (tabelul 1).[18]

Net-Centricity este un program care va sprijini activităţile de tehnologia informaţiei pentru colaborarea bazată pe reţea. Fuziunea pe orizontală reprezintă o componentă care determină cât de repede programele militare şi ale comunităţii de informaţii pot fi extinse la un mediu operaţional bazat pe reţea. Echipamentele de evaluare a reţelei de informaţii globale sunt o componentă care testează interoperabilitatea sistemelor esenţiale, într-o manieră punct la punct, inclusiv a Sistemului Radio Tactic Întrunit (JTRS) şi a celui de extensie a lărgimii de bandă a GIG (GIG BE).

Tehnologia Tactică de Tragere Avansată a Forţelor Aeriene (AT3) este un sistem care combină informaţiile colectate de o reţea de senzori aeropurtată, pentru a identifica cu precizie sistemele de apărare antiaeriană ale inamicului. Sistemul se bazează pe coordonarea informaţiilor de la sisteme diferite de la bordul aeronavelor.

Link 16 pentru Forţele Aeriene. Liniile tactice de date sunt utilizate în luptă pentru schimbul mesajelor de informaţii între echipamente tehnice (precum radarele de urmărire), informaţii despre ţinte, starea platformei, imagini şi misiuni de comandă.

Capabilitatea de Angajare Cooperativă Navală (CEC) este un sistem ce conectează navele şi aeronavele Forţelor Navale care acţionează într-o zonă delimitată, în cadrul unei singure reţele integrate de apărare antiaeriană, în care datele colectate de radarele de pe fiecare platformă sunt transmise în timp real altor unităţi din reţea. Fiecare unitate fuzionează datele din reţeaua CEC cu datele de la

[17] Paul McDougall, "Optimizing Through Outsourcing," *Information Week*, Mar. 1, 2004, p.56.

[18] CRS Report for Congress, Order Code RL 32411, *Network Centric Warfare: Background and Oversight for Congress*, Congressional Research Service, Washington, D.C., 2006, pp.15-20.

radarul propriu şi cu cele recepţionate de la alte unităţi. Drept rezultat, unităţile din reţea partajează o imagine de apărare antiaeriană comună, în timp real. CEC permite unei nave să lanseze rachete antiaeriene pentru distrugerea rachetelor împotriva navelor lansate de către inamic, chiar dacă nava nu le vede, utilizând datele de tragere obţinute de la radarele altor unităţi din reţea. De asemenea, permite lansarea acestora de către orice navă din grupare, chiar dacă nu ea este ţinta atacului, realizându-se astfel manevra dinamică şi în colaborare a mijloacelor la dispoziţia grupării.

Sistemul de Comandă al Forţei XXI din trupele de uscat la nivel brigadă şi mai jos (FBCB2). Sistemul FBCB2, utilizat împreună cu echipamentele de calcul ale Sistemului de urmărire a forţelor proprii (BFT) reprezintă principalul sistem digital de comandă şi control al trupelor de uscat, ce foloseşte internetul tactic pentru transmiterea în timp real a datelor de luptă necesare forţelor din spaţiul tactic. În timpul OIF, acest sistem a fost utilizat pe mai multe platforme de luptă, realizându-se o mai bună coordonare a efortului în timp şi spaţiu, reducând la zero apariţia fratricidului.

Sistemul Radio Tactic Întrunit (JTRS). Programul JTRS oferă calea de a concentra programele separate ale categoriilor de forţe ale armatei într-un efort de dezvoltare întrunit. În cadrul programului se folosesc mijloace radio definite software, programabile, care vor asigura interoperabilitatea cu sistemele radio existente în dotare prin intermediul unor interfeţe speciale, şi care vor asigura capabilităţi suplimentare de acces la hărţi, imagini şi video, permiţând luptătorului să comunice direct cu senzorii din spaţiul de luptă.

Sistemul de Luptă Aeriană fără pilot (J-UCAS). Programul combină alte două programe dezvoltate de forţele aeriene şi forţele navale într-o arhitectură comună, în scopul maximizării interoperabilităţii. Toate cele patru categorii de forţe ale SUA dezvoltă şi se dotează cu avioane fără pilot pentru sprijinul acţiunilor la nivel tactic, iar rata de achiziţie a acestor sisteme a depăşit estimările de acum câţiva ani.

Tabelul nr. 1

Program ($)	2003	2004	2005	2006	2007	2008	2009
Horizontal Fusion (mil.)	-	-	206,422	207,815	210,864	222,126	226,586
GIG Evaluation (mil.)	-	-	7,800	8,200	8,600	9,100	9,500
AT3 (mil.)	11,023	5,815	-	-	-	-	-
LINK 16 (mil.)	50,535	70,481	141,012	218,743	228,009	161,909	153,606
Navy CEC (thousands)	106.020	86.725	103.452	-	-	-	-
Army FBCB2 (thousands)	59.887	47.901	23.510	-	-	-	-
JTRS (thousands)	95.790	259.990	249.880	-	-	-	-
J-UCAS (mil.)	667,307	380,105	1043,498	986,156	-	-	-

NNEC reprezintă abilitatea cognitivă şi tehnică a Alianţei de a realiza o federaţie de componente variate din mediul operaţional, de la nivelul strategic (inclusiv NATO HQ) până la cel tactic, printr-o infrastructură de reţea şi informaţională.[19]

Din perspectivă strategică şi operativă, scopul este îmbunătăţirea eficienţei misiunii prin conectarea unui număr de senzori (colectori), factori de decizie şi efectori (elemente operaţionale) pentru a asigura cel mai bun flux de informaţii de-a lungul întregului lanţ de comandă. Figura 2 ilustrează aceste principii, în cazul specific al unui scenariu cu timp de acţiune critic care evidenţiază câteva idei importante:

[19] Ruud v. Dam, *NATO Network Enabled Capabilities*, Presentation at AFCEA Symposium, Paris, 2006.

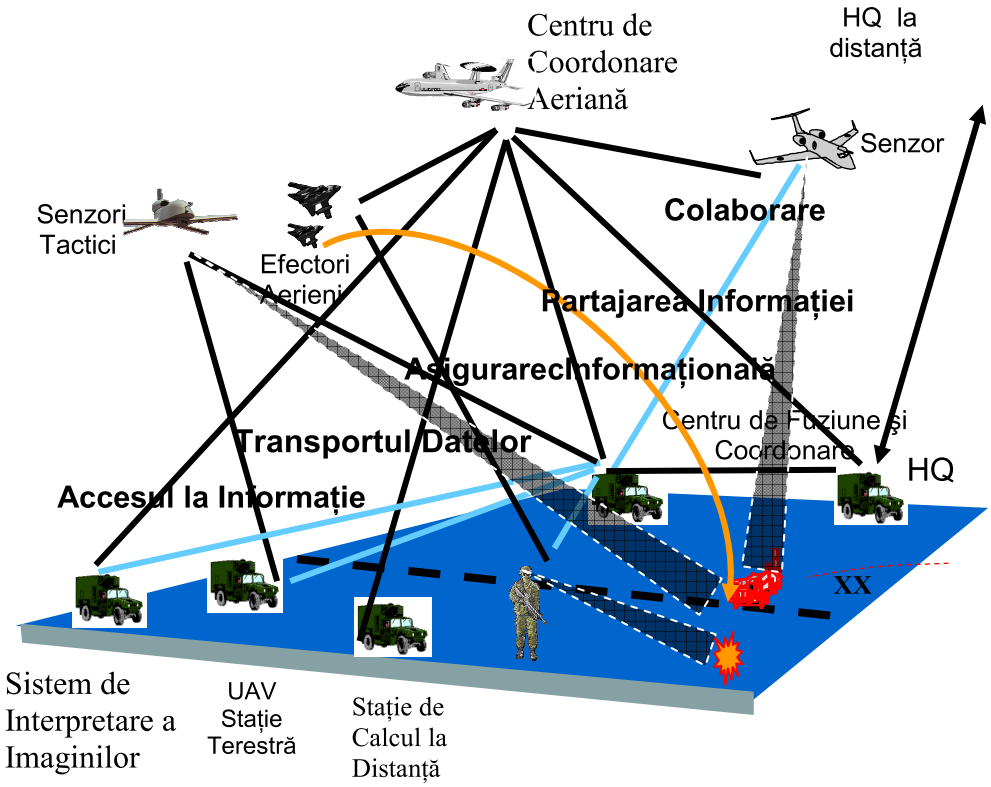


Figura 2. Exemplu de scenariu cu timp de acțiune critic

3. Sistemul C4ISR

Sistemul C4ISR nu este privit ca un singur sistem, ci mai mult ca un sistem de sisteme (figura 3) în care fiecare sistem produce şi/sau consumă servicii. Un principiu de bază în concepția orientată pe servicii este separarea producătorilor şi consumatorilor pe funcționalități. Serviciile nu sunt produse, în mod necesar, pentru un singur scop particular; acestea sunt în schimb produse independent de consumatori şi sunt făcute disponibile pentru utilizarea de către orice consumator autorizat.

Conceptul de sistem de sisteme înseamnă, de asemenea, că serviciile şi informațiile rezidente în sistemele existente şi în cele noi sunt integrate şi combinate. Astfel sunt create serviciile şi informațiile cu valoare ridicată. Nu este

necesar ca infrastructura şi sistemele tehnice care produc servicii să fie noi, chiar dacă sistemele noi pot fi desigur incluse. Sistemele vechi existente pot fi integrate într-un mediu de servicii prin includerea unor structuri de date în interiorul altora. Soluțiile C4ISR sunt complet scalabile; serviciile şi capabilitățile pot fi dezvoltate mai departe, iar gama de servicii şi sisteme poate fi extinsă în timp într-o manieră evolutivă.

C4ISR reprezintă integrarea doctrinelor, procedurilor, structurilor organizaționale, personalului, echipamentelor tehnice şi produselor software, facilităților, comunicațiilor şi cercetării pentru a sprijini abilitatea comandantului de a realiza comanda şi controlul de-a lungul întregii game de operații militare. C4ISR asigură comandanții cu date oportune şi precise şi sisteme pentru planificare, monitorizare, conducere, control şi raportarea desfăşurării operațiilor.

Sistemul de comandă şi control – facilitățile, echipamentele, procedurile şi personalul sunt esențiale pentru un comandant în planificarea, comanda şi controlul forțelor subordonate şi primite în sprijin pentru îndeplinirea misiunii.

Sistemul de comunicații este un ansamblu de echipamente, metode, proceduri şi personal (dacă e necesar), organizat pentru a îndeplini funcțiile de transfer al informațiilor. Cuprinde sisteme de transmisie, de comutație şi de utilizator. Poate îndeplini şi funcții de stocare şi prelucrare în sprijinul transferului de informații.

Sistemul informatic (de calculatoare) - un ansamblu de echipamente, metode, proceduri şi personal (dacă e necesar) organizat pentru realizarea funcțiilor de prelucrare a informațiilor. Poate transfera informații în sprijinul funcțiilor de prelucrare (de exemplu: în cadrul rețelelor locale de calculatoare).

Sistemul de informații (cercetare) - echipamente, metode, proceduri şi personal pentru realizarea produselor informative prin colectarea, prelucrarea, integrarea, evaluarea, analiza şi interpretarea informațiilor la dispoziție privind forțele ostile sau potențial ostile, zonele actuale sau potențiale de acțiune.

Sistemul informativ – orice sistem oficial sau neoficial care gestionează obținerea datelor, prelucrarea şi interpretarea lor pentru a asigura judecăți de valoare decidenților.

Sistemul de senzori – ansamblu de echipamente, metode, proceduri şi personal organizat pentru descoperirea personalului, obiectelor, fenomenelor sau activităților şi înregistrarea, prelucrarea şi transferul informațiilor captate.

ISR – sistem care colectează şi prelucrează informații pentru realizarea produselor informative despre amenințări şi mediu pe timpul operațiilor, precum şi informații pentru identificarea, urmărirea şi angajarea țintelor.

ISTAR – combină informațiile de la senzori, le stochează în baze de date comune, asigură mijloacele pentru managementul resurselor de colectare şi a

datelor colectate, analizează şi prezintă rezultatele, ierarhizează ţintele pe priorităţi după anumite criterii prestabilite.

Arhitectura sistemelor C4ISR trebuie să fie abordată din trei puncte de vedere (operaţional, sistemic şi tehnic) concomitent cu relaţiile dintre ele.

Domeniul operaţional impune sistemului cerinţele informaţionale ce trebuie satisfăcute din punct de vedere cantitativ şi calitativ, iar cel sistemic oferă serviciile necesare în acest sens.

Domeniul sistemic, la rândul său, solicită celui tehnic soluţii (standarde, proceduri, rutine) pentru implementarea sistemului conform cerinţelor operaţionale: conectivitate, interoperabilitate, compatibilitate, calitate şi oportunitate a serviciilor etc.

Prin arhitectură, în general, se înţelege cadrul de lucru sau structura care descrie relaţiile dintre toate elementele componente ale forţei, sistemului sau activităţii[20].

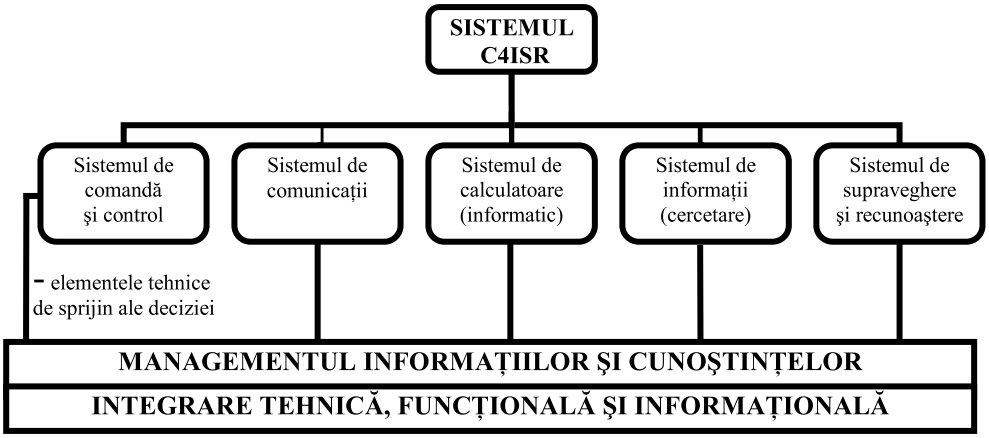


Figura 3. Structura sistemului C4ISR

Din punct de vedere operaţional, arhitectura se referă la centrele reţelei, misiunile şi sarcinile realizate, informaţiile care trebuie vehiculate pentru îndeplinirea misiunii (tipul, frecvenţa, misiunile şi activităţile sprijinite, natura acestora).

[20] *Glosar cu termeni şi definiţii în domeniul comunicaţiilor şi informaticii*, Ministerul Apărării Naţionale, Bucureşti, 2008, p.7.

Din punct de vedere sistemic sunt analizate: sistemul în ansamblu, serviciile şi funcţionalitatea interconectării asigurate pentru sprijinul activităţilor operaţionale prin schimbul de informaţii între centrele reţelei.

Din punct de vedere tehnic este analizat setul minim de reguli care guvernează organizarea, interacţiunile şi interdependenţele dintre părţile (elementele) sistemului în scopul satisfacerii cerinţelor operaţionale. Aceasta cuprinde o serie de standarde tehnice, rutine de implementare, selecţia standardelor, regulilor şi criteriilor care pot fi organizate în profiluri ce gestionează sistemul sau serviciile elementelor pentru o arhitectură dată.

Există şi unele aspecte generale ale arhitecturii care vizează analiza acesteia din toate punctele de vedere (operaţional, sistemic şi tehnic). Acestea asigură informaţii pertinente referitoare la întreaga arhitectură (scop, domenii, cadrul de timp, mediu etc.). Aceste condiţii cuprind doctrine, tactici, tehnici şi proceduri, obiective relevante şi viziunea declarată, concepţia de operaţii, scenarii şi condiţiile de mediu.

Arhitecturile se clasifică în următoarele tipuri:

- integrată – în care elementele de date sunt unic identificate şi utilizate sistematic în cadrul tuturor produselor şi din toate punctele de vedere ale arhitecturii;
- de tip federativ – care asigură un cadru general pentru dezvoltarea arhitecturii sistemului, mentenanţei şi utilizării care aliniază, localizează şi conectează arhitecturi diferite prin standarde de schimb informaţional;
- mixtă – care rezultă din integrarea sau concentrarea componentelor din arhitecturi integrate diferite.

Sistemul are 2 părţi principale: serviciile şi infrastructura. Partea serviciilor cuprinde: comunicaţiile şi colaborarea; informaţiile despre situaţie; operaţiile informaţionale; comandă şi control; sprijinul angajării. Partea de infrastructură cuprinde: stratul de control; stratul de convergenţă; stratul de conectivitate.

Serviciile de comunicaţii şi colaborare asigură funcţionalitatea, transmiterea şi partajarea informaţiilor. Serviciile privind informaţiile despre situaţie implică obţinerea, prelucrarea şi diseminarea informaţiilor despre situaţie. Operaţiile informaţionale cuprind servicii pentru analiza şi influenţarea informaţiilor altora şi protecţia informaţiilor despre situaţia proprie. Comanda şi controlul implică servicii pentru sprijinul deciziei şi manipularea ordinelor. Sistemele de angajare şi efectorii sunt conectaţi la mediul C4ISR, implicaţi în fluxul informaţional şi controlaţi de serviciile de sprijin ale angajării.

Stratul de control conţine funcţionalităţi şi servicii de sprijin care sunt utilizate pentru a asigura serviciilor menţionate mai sus caracteristicile şi trăsăturile necesare precum securitate, mobilitate şi accesibilitate.

Stratul de convergenţă asigură realizarea conectivităţii într-o manieră unificată, pe baza Protocolului Internet şi a faptului că diferitele tipuri de reţele fixe, mobile şi wireless care aparţin stratului de conectivitate, pot fi utilizate la parametrii planificaţi.

4. Noi cerinţe pentru sistemele C4ISR

Institutul pentru Inginerie Electrică şi Electronică (IEEE) defineşte termenul de architectură ca "structura componentelor, relaţiile dintre ele, principiile şi regulile care guvernează proiectarea şi evoluţia lor în timp."[21] Cadrul arhitectural are în vedere diferenţierea dintre o descrire a arhitecturii şi o implementare a acesteia. Acesta divide arhitectura în trei viziuni – operaţională, sistemică şi tehnică definite astfel:

- viziunea operaţională — o descriere a sarcinilor şi activităţilor, elementelor operaţionale şi fluxurilor informaţionale necesare pentru îndeplinirea sau sprijinul unei operaţii militare;
- viziunea sistemică — o descriere, inclusiv grafică a sistemelor şi interconexiunilor asigurate pentru realizarea interconectărilor sau sprijinul acţiunilor de luptă;
- viziunea tehnică — setul minim de reguli privind guvernarea, interacţiunile şi interdependenţele dintre părţile sau elementele sistemului, a cărui scop este de a se conforma unui set specific de cerinţe.[22]

Principalele lecţii învăţate şi concluzii pentru dezvoltarea viitoare a sistemelor C4ISR sunt următoarele:[23]

- sistemele de comutaţie existente au fost proiectate să suporte cerinţe de bandă pentru 93% voce, 7% date şi 0% video;
- sistemele de transmisiuni bazate pe linii terestre cu vizibilitate directă sunt limitate ca bandă de frecvenţe;
- sistemele de abonat mobil nu au flexibilitatea necesară pentru transmisiuni de voce şi date; în acelaşi timp, nu pot fi desfăşurate complet în funcţie de timp, distanţă şi tempoul operaţional;

---

[21] *C4ISR Architecture Framework Study,* (Washington, D.C.: U.S. Department of Defense, 18 December 1997), p.15.

[22] DoD Architecture Working Group, *DoD Architecture Framework Study*, (Washington, D.C.: U.S. Department of Defense, 9 February, 2004), vol 1. pp.2-4.

[23] Cogan K., Lucio R., Network Centric Warfare Case Study, Volume II: *A View of C4 Architecture at the Dawn of Network Centric Warfare*, U.S. Army War College, Carlisle Barrackis, Pennsylvania, 2006, Chapter 4-5.

- un punct de comandă principal de divizie are numai un flux de date de 512 Kbps; instalarea punctului de comandă se realizează în 45-60 minute cu capabilităţi de funcţionare iniţiale;

- sistemele vechi nu sunt capabile să asigure interoperabilitatea tot timpul;

- mari dificultăţi s-au creat prin combinarea sistemelor vechi, cu cele comerciale şi ale agenţiilor militare;

- sistemul de comandă în luptă al trupelor de uscat cuprinde 8 sisteme de comandă şi control specializate pentru a putea asigura o imagine comună a câmpului de luptă;

- a fost creată o bază de date întrunită comună pentru afişări grafice, localizarea forţelor proprii, echipamentelor specifice ale inamicului, informaţii logistice, situaţia unităţilor vecine şi superioare, activitatea vehiculelor aeriene fără pilot, viteza şi direcţia de luptă a rachetelor de croazieră, condiţiile de vreme, mobilitatea etc.;

- managementul spectrului electromagnetic a fost o preocupare majoră la toate nivelurile;

- platformele de comunicaţii mobile nu au fost modernizate;

- nu au fost asigurate sisteme de comunicaţii pentru situaţii cu timp critic şi capabilităţi pentru comanda din mişcare;

- în 2004 cerinţele de date pentru fiecare soldat au crescut cu peste 100% faţă de „Furtuna Deşertului”;

- o problemă majoră în cadrul coaliţiei de forţe a fost lipsa de interoperabilitate;

- comunicaţiile prin satelit au asigurat capabilităţi pentru comanda din mişcare, dar nu pentru toate unităţile;

- instrumentele de colaborare au fost utilizate între grupuri mici de utilizatori, datorită limitelor reţelei informaţionale;

- au fost utilizate multe sisteme de operare, dar cu puţină interoperabilitate.

Pe timpul OIF au fost luate măsuri pentru modernizarea unor sisteme (Reţeaua tactică informaţională a luptătorului – WIN-T, Centrul reţelei întrunite - JNN, Punctul de comandă al viitorului – CPOTF), de adaptare a echipamentelor la cerinţele exponenţiale de frecvenţe, de scurtare a duratei ciclului de achiziţie de la 10 la 3 ani, creşterea capacităţii de transmitere pe flux de la 1024 Kbps la 8192 Kbps etc.

Până în anul 2010 sunt vizate 5 componente principale ale sistemelor C4ISR:

▪o reţea informaţională cu senzori multipli care să asigure cunoaşterea dominantă a spaţiului de luptă pentru comandanţi şi forţe;

▪capabilităţi avansate de management al luptei care să permită desfăşurarea globală a forţelor mai rapid şi mai flexibil decât un potenţial adversar;

▪capabilităţi de desfăşurare a operaţiilor informaţionale ofensive şi defensive;

▪o reţea de comunicaţii întrunită cu capacitate adecvată, fiabilitate şi conectivitate sporite pentru toate structurile organizaţionale militare;

▪un sistem de protecţie a reţelelor de comunicaţii şi calculatoare globale.

Aceste ultime măsuri au fost deja aprobate pentru toată gama de echipamente tehnice şi produse software. Se presupune că unele dintre aceste tehnologii vor fi aplicate în generaţiile viitoare de reţele şi sisteme C4ISR.

IMPLEMENTAREA CAPABILITĂȚILOR FACILITATE DE REȚEA ŞI INTEROPERABILITATEA ÎN ARMATA ROMÂNIEI

General-locotenent (r) prof. univ. dr. Cristea DUMITRU
- membru corespondent al Secției Ştiințe Militare -

1. Examinarea dezvoltării capabilităților C4I din Armata României pentru a fi în concordanță cu mediul NEC NATO

Un specific al operațiunilor militare ale secolului XXI îl reprezintă creşterea continuă a complexității, datorită îngemănării nivelurilor strategice, operative şi tactice, a întrepătrunderii obiectivelor militare şi civile, precum şi datorită realizării obiectivelor în comun cu aliații. Din ce în ce mai mult, comandanții militari sunt puşi în fața problemei privind concilierea modului tradițional de ducere a operațiilor militare cu obiectivele misiunii de ansamblu şi ale politicii naționale.

În acest moment, cuvântul cel mai important în zona militară este "TRANSFORMAREA". Acesta este un cuvânt cheie în NATO şi, deci, în acelaşi timp şi în Armata României. În esență, cuvântul se referă la:

• reconsiderarea naturii operațiunilor militare, precum şi reconsiderarea doctrinelor, a competențelor şi a dotării materiale;

• influența transformării asupra sistemelor C4I, unde pot fi întâlnite următoarele două cadre generale, şi anume, capabilitățile facilitate de rețea şi Infrastructura Națională Critică (Critical National Infrastructure – CNI)

Scopul principal al celor două cadre îl constituie obținerea superiorității informaționale, cel din urmă fiind unul din pilonii de bază ai conceptului NEC.

Capabilitățile facilitate de rețea permit un sprijin mai rapid şi mai bun al întregului spectru de operații. Rezultatele cheie aşteptate sunt:

• superioritate informațională şi decizională (primul obiectiv al NEC);

• asigurarea coerenței informaționale şi interoperabilității tuturor utilizatorilor;

• creşterea receptivității;

• creşterea flexibilității.

Aceste rezultate devin posibile doar în cadrul unei Infrastructuri Informaționale şi de Rețele (Networking and Information Infrastructure – NII) care pune laolaltă senzori, centre de comandă-control şi efectori, indiferent dacă sunt tereştri, maritimi sau aerieni.

Apreciem că criteriile de bază ale NEC sunt următoarele:

• rețele inteligente;

• aplicații de gestiune a informațiilor incluse în nodurile rețelei;

• distribuirea de servicii de bandă largă;

• garantarea unei anumite calități a serviciilor (QoS) punct la punct;

• soluții de securitate distribuite uniform în întreg sistemul;

• mobilitatea utilizatorilor.

Scopul conceptelor NEC îl constituie crearea de rețele inteligente, capabile să contribuie operativ la gestiunea şi diseminarea informațiilor. Acest scop implică existența aplicațiilor de gestiune a informațiilor incluse în nodurile rețelei, implementarea de aplicații de comandă-control şi administrative (Intranet), utilizarea pe scară largă de instrumente grafice şi imagistice.

Pentru aceste aplicații sunt necesare servicii de bandă largă. Aceste servicii necesită date în timp real, adică servicii multimedia cu o anumită calitate a serviciilor pentru semnale video, gestiunea senzorilor, controlul efectorilor etc.

Tot acest mediu solicită soluții de securitate, distribuite uniform în sistem, pentru a deservi diferite comunități de utilizatori (securitatea informațiilor, autentificarea şi înregistrarea utilizatorilor etc.).

Iar, nu în ultimul rând, conceptul NEC necesită sprijinul mobilității utilizatorilor, sisteme şi tehnologii specifice care extind serviciile de voce, date şi multimedia unităților din teren, până la nivel de soldat.

Luând în considerare cel de-al doilea cadru menționat, este necesar să subliniem că acesta a început să aibă consistență după 11 Septembrie, iar criteriile de bază sunt următoarele:

• medii de transport proprietare sau dedicate;

• realizarea unei redundanţe a reţelei (sisteme de tip grătar), diversificarea mediilor de transmisie (radioreleu, satelit, fibră optică);

• restabilirea automată a conexiunilor utilizatorilor prin intermediul mecanismelor cu Prioritate Multiplă şi Preempţiune;

• sistemul de Suport al Operaţiilor integrate (Operations System Support - OSS);

• utilizarea de echipamente criptare on-line certificate;

• sisteme de control al accesului la sistemele publice.

Infrastructura de Informaţii şi Reţele este compusă din Infrastructura Informaţională şi de Reţele (NII) la nivel strategic – RMNC; Infrastructura Informaţională şi de Reţele la nivel tactic; Sisteme Informatice Funcţionale (Functional Area Services), precum şi din utilizatori şi misiuni.

Primul element implementat şi unul dintre cele mai importante este Reţeaua de Transmisiuni Permanentă (RTP). Aceasta reprezintă infrastructura de bază a Reţelei Militare Naţionale de Comunicaţii.

RRONS este o reţea monocanal bazată pe echipamente radio performante, proiectate să furnizeze capabilităţi de comunicaţii pentru statele majore ale categoriilor de forţe şi marile unităţi dislocabile sau din forţele de generare regenerare, în mişcare, precum şi ca soluţie de rezervă pentru RTP, asigurând cu preponderenţă comunicaţii de date.

Pentru a furniza în unele zone capabilităţi de comunicaţii suplimentare, există elemente dislocabile ale RTP dispuse pe containere sau pe autospeciale.

Fiecare dintre categoriile de forţe (în special aviaţia şi marina) poate realiza subreţele proprii specifice.

Pentru a creşte performanţele RMNC, considerăm că trebuie adoptată o strategie evolutivă. Această strategie este bazată, în principal, pe următoarele etape:

• estimarea sistemelor existente;

• proiectarea unei Arhitecturi Globale (Overarching Architecture - OA) naţionale;

• dezvoltarea Arhitecturilor de Referinţă şi a celor Ţintă necesare (Reference Architectures – RA, Target Architectures - TA);

• urmărirea unui parcurs pentru Arhitecturile Ţintă.

Etapele au început să fie deja abordate în funcţie de cerinţele operaţionale şi fondurile la dispoziţie.

Astăzi, RTP reprezintă infrastructura Reţelei Militare Naţionale de Comunicaţii, care este utilizată de toate structurile Armatei României. Peste acest sistem de comunicaţii au fost realizate: sistemul INTRANET militar (INTRAMAN), sistemul de video-teleconferinţă criptat, aplicaţiile specifice forţelor navale (ARGUS), de mediu etc. La nivel strategic, acestea reprezintă

pilonii Infrastructurii Informaţionale şi de Reţele. Conceptul de dezvoltare al RMNC va permite evoluţia către o componentă a confederaţiei de reţele NATO. Performanţele actuale ne permit capabilităţi operaţionale şi interconectarea cu alte reţele cu anumite limitări. Ceea ce este însă important este că se încearcă îmbunătăţirea acestor capabilităţi.

Infrastructura Informaţională şi de Reţele strategică oferă comunicaţii în sprijinul unui număr important de aplicaţii funcţionale, cum ar fi SCCAN (inclusiv conexiunile senzorilor – FPS117, GAP FILLER şi radarele şi vectorii analogici modernizaţi – baze aeriene, rachete sol-aer, unităţi de Război Electronic), Sistemul de Supraveghere şi Avertizare NBC, Sistemul Informatic Meteorologic Integrat Naţional, SCOMAR, INTRANET-ul Militar etc.

În prezent, RTP este o reţea bazată pe sistemul EUROCOM Extins cu porţi către alte reţele de tip EUROCOM, STANAG şi ITU-T. Toate acestea asigură un înalt nivel de interoperabilitate cu reţelele comerciale (ITU-T) şi cu cele tactice (STANAG şi/sau EUROCOM). De asemenea, RTP se interconectează cu Sistemul General de Comunicaţii al NATO (NGCS). În viitor, RTP va oferi servicii utilizatorilor NATO de pe teritoriul naţional. RTP se interconectează şi cu Reţeaua Militară Naţională de Comunicaţii a Republicii Italiene prin intermediul sistemului satelitar SICRAL. De asemenea, există posibilitatea interconectării cu reţelele tactice ale altor naţiuni.

Reţeaua Radio Operativă de Nivel Strategic are drept scop furnizarea de capabilităţi minime de voce, date şi de tip "link", pentru toate comandamentele unităţilor tactice şi operative, în cazul în care alte mijloace de comunicaţii nu pot fi utilizate. RRONS este folosită la nivelul statelor majore ale categoriilor de forţe, pentru unităţile de nivel tactic şi operativ (cu accent pe unităţile ce sunt puse la dispoziţia NATO). Comunicaţiile asigurate sunt protejate la intercepţie şi bruiaj prin criptoare încorporate şi salt de frecvenţă. RRONS are capabilităţi de integrare cu serviciile de mesagerie din INTRAMAN.

Principalele servicii oferite de INTRANET-ul militar sau INTRAMAN, precum şi sistemele informatice pentru care acesta constituie infrastructura de sprijin sunt:

• serviciile informatice de bază (poştă electronică, fişiere şi imprimare, WEB, gestionarea ierarhică a activităţilor, gestionarea ierarhică a fluxurilor de documente etc.).

• suport pentru sistemele informatice funcţionale:
  - Sistemul Informatic de Sprijin al Acţiunilor Militare (SISAM);
  - Sistemul Informatic de Informaţii al Apărării (SIA);
  - Sistemul Informatic de Modelare, Simulare (SISMIM);
  - Sisteme de armament (SISARM)

- Sistemul Informatic de Asistare a Învățământului Militar (SIMIL);
- Sistemul Logistic Integrat (AILS).

Există o serie de extensii în afara teritoriului național ale RTP pentru sprijinul trupelor româneşti dislocate în operații internaționale. Sunt create, de asemenea, extensii pentru reprezentanțele României la NATO, ACO şi UE. Serviciile oferite de aceste extensii sunt de voce, date şi VTC criptate şi necriptate pentru legăturile sociale.

2. Creşterea capabilităților de apărare ale Armatei României prin implementarea de tehnologii integratoare, pentru asigurarea de capabilități multifuncționale şi flexibile

Necesitățile de ordin operațional care pot fi definite pentru o Rețea Comună pentru Armata României sunt accesul la rețea pentru satisfacerea de criterii cum ar fi flexibilitatea, simplitatea şi securitatea, pe teritoriul național sau în afara acestuia, pentru a permite accesul utilizatorilor care exploatează rețeaua din:

- centre fixe prin intermediul infrastructurii militare, guvernamentale sau comerciale;
- centre fixe prin intermediul Modulelor de Comunicații şi Informatică Dislocabile;
- centre/puncte de comandă/unități mobile prin intermediul conexiunilor stabilite prin intermediul accesului îndepărtat.

Una dintre cerințele tehnice esențiale o constituie realizarea compatibilității cu cele mai importante standarde din domeniu, pentru a asigura interoperabilitatea. De asemenea, topologia rețelei va trebui să permită flexibilitate, viabilitate şi servicii corespunzătoare nevoilor utilizatorilor. Totodată, rețeaua trebuie să ofere suport pentru diferite servicii/aplicații/funcțiuni şi fluxurile informaționale specifice, care să permită operațiuni autonome şi independente, precum şi integrarea şi schimbul de date la cererea serviciilor şi aplicațiilor specifice.

Nu mai puțin importantă este utilizarea celor mai noi tehnologii integrate, cum ar fi: Stații radio definite prin software (Software Defined Radio), Protocolul de Interoperabilitate al Comunicațiilor Securizate (Secure Communication Interoperability Protocol), Comunicații tactice după anul 2000 (TACOMS Post 2000) etc.

Rețeaua comună pentru Armata României va oferi suport pentru:

- servicii de interconectare între rețele;
- servicii de bază (core services);
- servicii funcționale (functional areas services), cum ar fi pentru personal, cercetare, operații, logistică, planificare, geo-meteo, simulare etc.

Această abordare este similară cu cele utilizate de NATO pentru dezvoltarea NATO Bi-Strategic Command Automated Information System, Deployable CIS şi NATO General Purpose Communication System.

În scenariul descris este foarte importantă demararea unui proces evolutiv care să conducă la o capabilitate facilitată de rețea, într-o perioadă de timp acceptabilă. Având acest scop, trebuie gândite acțiuni de implementare a unei rețele comune prin exploatarea achizițiilor recente şi prin optimizarea şi integrarea sistemelor deja realizate sau care vor trebui introduse în exploatare în viitorul apropiat. Pornind de la aceste ipoteze privind scopul final, estimăm că se vor putea atinge următoarele cerințe:

• suport pentru servicii de bandă largă (servicii integrate multimedia);
• optimizarea benzii de transmisie avute la dispoziție;
• dezvoltarea / implementarea de rețele de acces;
• creşterea securității rețelei prin utilizarea de sisteme de criptare compatibile NATO şi implementarea de concepte NATO privind securitatea (de ex. securitate multinivel);
• dezvoltarea platformelor existente sau introducerea de noi platforme care să permită servicii de bază;
• creşterea integrării, realizându-se sprijinul acțiunilor din afara teritoriului național prin comunicații satelitare şi conectivități de mare capacitate către mijloacele mobile;
• mărirea interoperabilității între RMNC şi NGCS;
• creşterea funcțiunilor de automatizare şi control pentru înlocuirea forței de muncă.

Aceste cerințe conduc la realizarea obiectivelor finale:

• construirea unei rețele sigure şi cu o viabilitate ridicată;
• integrarea totală a componentelor rețelei atât strategice, cât şi tactice;
• gândirea arhitecturii rețelei şi tehnologiilor adoptate pentru a optimiza capabilitățile privind eficiența şi managementul;
• evoluția serviciilor.

Pornind de la situația actuală, se poate defini un plan secvențial al acțiunilor care pot conduce la realizarea unei rețele comune pentru Armata României.

Serviciile furnizate de rețea sunt împărțite în două categorii principale, având la bază împărțirea Bi-Strategic Command Automated Information System: servicii de bază (core services) şi servicii funcționale (functional area services). Serviciile de bază sunt destul de bine dezvoltate în cadrul rețelei, problema principală reprezentând-o, în opinia noastră, diseminarea acestor servicii pentru toți utilizatorii.

În zona serviciilor funcționale suntem în faza în care Armata României investeşte efort şi fonduri. Aceste activități sunt conduse de necesitatea obținerii unui schimb de informații în timp real între efectori şi senzori, precum şi de servicii specifice pentru diferite misiuni. Serviciile vor fi furnizate începând din zona magistrală, pentru zone specifice, cum ar fi cea a utilizatorilor naționali, a utilizatorilor NATO, a celor din diverse coaliții şi a participanților la misiuni externe.

Pentru viitorul apropiat, eforturile sunt concentrate pe integrarea sistemelor existente şi pe introducerea în rețeaua existentă a subsistemelor integrate sau a subsistemelor cu capabilități de integrare.

Armata României se află în procesul de testare şi finalizare a activităților de integrare a sistemului de război electronic (programul AZUR) şi a sistemului de control al armamentului, Hawk XXI. De asemena, există două programe principale ale categoriilor de forțe - SCOMAR – sistemul de supraveghere şi observare pentru Statul Major al Forțelor Navale şi SCCAN – sistemul de comandă-control pentru Statul Major al Forțelor Aeriene.

Pentru perioada imediat următoare, ambițiile sunt mari. Datorită cerințelor de capacități mari de trafic ale noilor sisteme informatice, trebuie concentrate eforturile pentru dezvoltarea infrastructurii existente, prin introducerea de purtătoare de mare viteză. Pentru unele zone vor fi realizate rețele zonale de fibră optică de mare capacitate. Pentru a mări capabilitățile de procesare, vor fi introduse comutatoare multiprotocol şi multiservicii. Totodată, efortul va fi axat pe:

• integrarea sistemelor existente prin porți specifice, care nu vor limita performanțele;

• utilizarea de stații radio definite prin software pentru toate serviciile şi toate tipurile de comunicații. Stațiile radio cu astfel de capabilități au început să fie deja utilizate;

• realizarea unui sistem de management al rețelei de ansamblu;

• în zona INFOSEC, protejarea informațiilor şi a sistemului, criptoarele IP urmând a fi utilizate ca soluție standardizată;

• integrarea senzorilor şi utilizarea senzorilor inteligenți.

3. Dezvoltarea şi utilizarea de comunicații numerice, mobile operative în vederea asigurării suportului pentru activitățile procesului de comandă-control

Ministerul Apărării Naționale a început diferite programe de modernizare, multe dintre ele la eşaloane inferioare datorită nivelului de angajare din momentul inițierii programelor. În prezent, această angajare implică eşaloane mai mari,

conştientizându-se faptul că, datorită lipsei de coordonare, nu pot fi integrate aceste sisteme decât cu greu la nivel brigadă.

Analizând situaţia la nivelul Statului Major General, Direcţia comunicaţii şi informatică, cu sprijinul Statului Major al Forţelor Terestre, a decis că singurul mod de a rezolva situaţia tuturor aspectelor privind integrarea îl constituie demararea unui proces de definire a sistemului C4ISTAR la nivel brigadă. Aceasta pentru că, un sistem C4ISTAR flexibil, multinivel şi operativ este potenţial cel mai important multiplicator al forţei din tot spaţiul de luptă.

Pentru dezvoltarea unui sistem C4ISTAR competitiv, abordarea arhitecturală recomandată în NATO C3 Systems Architecture Framework se consideră a fi soluţia cea mai bună. Ca tehnologie de bază a fost adoptată digitizarea spaţiului de luptă, iar ca idee de bază, conceptul C4ISTAR. Nu mai puţin importantă este coordonarea cu toate programele cu care interacţionează.

În realizarea acestui deziderat, Statul Major General a stabilit o Echipă Integrată de Proiect, formată din reprezentanţi ai Ministerului Apărării Naţionale şi ai unor companii cu experienţă în domeniul sistemelor C4ISTAR, având ca scop dezvoltarea elementelor de bază pentru un sistem C4ISTAR la nivel brigadă. De asemenea, această echipă realizează şi analizează lacunele de interoperabilitate şi de capabilităţi, precum şi o propunere privind calendarul de implementare.

Dezvoltarea şi utilizarea de comunicaţii mobile şi digitale operative pentru furnizarea către soldat de date de comandă-control şi cercetare sunt bazate pe: cerinţe operaţionale, constrângeri tehnologice, de timp şi bugetare.

Când vorbim despre cerinţele operaţionale, avem în vedere două grupe principale:

• prima este aceea care ia în consideraţie capabilităţile care trebuie furnizate de către sistem pentru a putea sprijini toate tipurile de acţiuni militare;

• a doua are în vedere cerinţele de interoperabilitate. În mod normal, una dintre cerinţele de capabilitate este cea de interoperabilitate, dar având în vedere experienţa din teatrele de operaţii, considerăm că această problemă trebuie tratată separat.

Sistemul C4I trebuie să furnizeze sprijin pentru comandă la toate nivelurile. Toate sistemele de arme trebuie să fie integrate. Mobilitatea este o caracteristică de bază pentru toate sistemele tactice. Protecţia este termenul în spatele căruia se află securitatea, contramăsurile electronice, criptarea. Suportul de comunicaţii trebuie să ofere suficientă capacitate pentru sprijinul comenzii şi serviciilor funcţionale. Nu în ultimul rând, sistemul trebuie să furnizeze interoperabilitate între zona naţională şi cea internaţională.

Timpul în care interoperabilitatea pentru sistemele de comandă-control era asigurată de interoperabilitatea comunicaţiilor a trecut. Noul context al

transformării spaţiului de luptă schimbă semnificaţia acestui cuvânt. Pentru moment, când vorbim despre interoperabilitatea sistemelor C4I, vorbim despre comunicaţii, dar şi despre partajarea informaţiilor, imaginea operaţională comună, aplicaţii de bază. Există informaţii foarte precise care trebuie partajate şi care sunt de o importanţă foarte mare pentru trupele care acţionează în teatre: urmărirea trupelor aliate şi analiza situaţiei.

Atunci când se dezvoltă un sistem C4ISTAR tactic, de nivel brigadă, există câteva constrângeri de ordin tehnologic care trebuie luate în considerare, deoarece este practic imposibilă achiziţionarea unui sistem total nou, cu vehicule noi, cu elemente de sprijin pentru luptă noi, aproape în toate situaţiile trebuind să fie utilizate unele dintre sisteme existente – este şi cazul sistemului de control al focului, de sprijin cu artilerie şi capabilităţi ISTAR.

La nivel tactic, mediul de comunicaţii este caracterizat de capacitate mică de trafic. Cu toate noile tehnologii, staţiile radio monocanal cu capacitate 16/64 Kbps continuă să fie cele mai utilizate mijloace de comunicaţii pentru trupele luptătoare. Există două mari subiecte pe care le considerăm ca având constrângeri tehnologice:

• sistemele de comandă-control, cele de sprijin pentru luptă şi sistemele de sprijin logistic utilizează baze de date diferite, ceea ce face integrarea într-un sistem C4I foarte dificilă – Programul MIP rezolvă problema la nivelul comandamentelor şi aplicaţiilor pentru comandă-control, iar JC3IEDM va extinde zona de acoperire ca model de date, dar se pare că nu va rezolva toate problemele;

• foarte importante sunt şi mecanismele de schimb de date, care depind şi de capacitatea de comunicaţii.

4. Perspective: programe şi proiecte esenţiale

Programele fundamentale care permit implementarea sistemelor C4ISTAR la nivel tactic sunt:

• dotarea punctelor de comandă ale brigăzii, diviziei şi forţelor terestre cu sisteme C4I;

• dotarea batalioanelor cu un sistem simplu de comandă-control (denumit şi Sistem de Management al Câmpului de Luptă = Battlefield Management System – BMS) – batalioanele luptătoare au nevoie să primească ordine de la eşaloanele superioare, să raporteze informaţii privind poziţia, alerte, starea logistică etc. având la dispoziţie un sistem C4I simplu şi rapid; toate acestea ţin cont că scopul principal al acestor batalioane este de a lupta şi nu de a introduce o cantitate mare de date într-un sistem software complex;

• dotarea batalioanelor de cercetare cu sisteme specifice C4I – cercetarea este o muncă specifică, care utilizează foarte multe mijloace de achiziţie şi

procesare a informațiilor, de la războiul electronic, la spionaj, iar sistemul C4I pentru batalioanele de cercetare este complet particularizat pentru misiunile ce trebuie executate;

• dotarea batalioanelor şi brigăzilor de sprijin (de ex. de artilerie) cu sisteme C4I specifice. De exemplu, optimizarea totală a efectelor focului de artilerie poate fi obținută doar cu un sistem C4I specific, având în vedere toate datele şi parametri de artilerie (localizarea armamentului, starea muniției, imagini 2D şi 3D, reguli de securitate, doctrină etc.). În paralel, sistemul C4I de artilerie trebuie să aibă funcțiuni suplimentare pentru a fi total operațional, cum ar fi manevra şi logistica.

Atunci când brigăzile vor fi disponibile, brigada luptătoare va fi echipată deja cu un sistem C4I pentru punctul de comandă ce va fi integrat într-un sistem C4ISTAR la nivelul diviziei, incluzând şi brigăzile de sprijin pentru luptă (cum ar fi cea de artilerie).

Un alt proiect care face parte din dezvoltarea C4ISTAR este Sistemul Avansat de Luptă Individual (SLIA). Scopul SLIA este de a creşte capacitățile individuale ale soldatului: de mişcare, detectare, angajare şi în lupta de aproape. SLIA se adresează capabilităților C4I, de supraveghere şi achiziție ținte, armament şi mobilitate, pentru a mări ritmul şi precizia angajărilor tactice în întregul spectru de conflicte.

SLIA este un sistem de luptă modular, integrat şi dezvoltabil care va echipa soldații forțelor terestre cu o gamă de facilități tehnologice avansate, fiecare interconectat la o platformă unică. Sistemul va interconecta fiecare grupă de soldați într-un spațiu digitalizat de luptă, ca un sistem de arme, fiecare om-platformă din această grupă contribuind la un nivel mai înalt, acela de Capabilități facilitate de rețea.

MODELAREA ŞI SIMULAREA – ELEMENTE FUNDAMENTALE ALE CONDUCERII ACŢIUNILOR MILITARE

General-locotenent prof. univ. dr. Teodor FRUNZETI
Comandantul (rectorul) Universităţii Naţionale de Apărare „CAROL I”

„Omul raţional se adaptează el însuşi la lumea înconjurătoare; cel iraţional persistă în încercarea de a adapta lumea ce îl înconjoară la el. Consecinţa este că toate progresele sunt dependente de cel iraţional."
“OM ŞI SUPEROM” ,
George Bernard Shaw, 1903

Modificările esenţiale ale mediului de securitate global, conţinutul şi fizionomia luptei moderne, structura funcţională de tip nou a eşaloanelor tactice şi rolul acestora în conflictele actuale, dar şi în câmpul de luptă al viitorului determină transformări majore în toate planurile. Noile conflicte militare generează schimbări în domeniul artei militare, în domeniul doctrinelor, al organizării, al înzestrării şi al instruirii. Având ca element comun – tehnologia, în evoluţia ei, toate aceste schimbări îşi propun optimizarea raportului om-tehnică în condiţiile digitizării câmpului de luptă, cu scopul fundamental de apropiere a victoriei într-un eventual conflict.

Când perfecţionarea continuă, multifuncţională şi structurală a diferitelor eşaloane este o realitate, când supleţea, manevrabilitatea, ritmul înalt de acţiune, adaptabilitatea şi capacitatea de a acţiona întrunit sunt cerinţe actuale ale celor mai multe structuri ale armatelor moderne, când transformarea NATO pentru a face faţă noilor provocări ale secolului XXI este o realitate, putem constata cu uşurinţă

preocupările permanente ale armatelor moderne privind completarea eforturilor întreprinse pentru perfecţionarea tehnologiilor militare cu eforturi similare, în plan analitic, prin revigorarea cercetărilor operaţionale. Diversificarea preocupărilor privind creşterea calităţii instruirii, a învăţământului militar superior şi a activităţilor de cercetare ştiinţifică evidenţiază tendinţele şi orientările armatelor moderne privind întrebuinţarea modelării şi simulării ca o alternativă viabilă şi eficientă în domeniul conducerii acţiunilor militare, asistării deciziilor şi evaluării alternativelor şi rezultatelor, implementării noilor tehnici, tactici şi proceduri de conducere a trupelor, realizării cooperării prin desfăşurarea unor exerciţii în comun, utilizând procedurile NATO, de comandă şi stat major.

În acest context, operaţiile militare reprezintă obiectul principal al activităţii din domeniul Modelare şi Simulare (M&S), aşa după cum rezultă explicit din planurile master ale SUA şi NATO. Astfel, v*iziunea NATO asupra Modelării şi Simulării (M&S),* stipulează că *M&S va asigura mijloacele gata disponibile, flexibile şi eficiente, pentru a pune în valoare în mod drastic operaţiile NATO în întreaga arie de aplicare a lor: planificarea apărării, antrenament, sprijin operaţional, cercetare, dezvoltare tehnologică şi achiziţii de armament.*

Similar, viziunea asupra modelării şi simulării stipulează că aceasta va sprijini antrenamentul forţelor, dezvoltarea doctrinei şi tacticii, evaluarea performanţelor unităţilor, sprijinul operaţional pentru planificarea, executarea şi analiza operaţiilor şi a exerciţiilor, posibilitatea efectuării repetiţiei generale în vederea îndeplinirii misiunilor şi analize de sprijin ale dimensiunilor politice, militare şi economice ale securităţii naţionale, pentru dezvoltarea politicii de apărare.

În termeni generali, modelarea desemnează *reprezentarea unui sistem sau proces printr-un alt sistem, denumit model,* care păstrează caracteristicile relevante ale originalului şi este mai uşor de studiat. Scopul modelării îl reprezintă obţinerea unor concluzii relevante asupra originalului, pe baza studierii modelului. Modelarea poate fi realizată pe cale analitică şi pe cale experimentală. Din definiţia prezentată se poate aprecia că modelarea este, din punct de vedere formal – matematic, o operaţie care asociază unui anumit original, un anume model şi conţinutul operaţiei este dependent de scopul modelării, care determină implicit ce caracteristici ale originalului sunt considerate relevante în raport cu el şi care introduce o nouă noţiune – aceea de *nivel de rezoluţie*. Rezoluţia[1], înseamnă gradul de detaliere şi de precizare utilizat în reprezentarea aspectelor lumii reale în construcţia modelului.

Definiţia modelului utilizată de NATO[2] a fost inspirată după cea folosită de armata SUA, potrivit căreia modelul este "*o reprezentare a unui sistem, entităţi, fenomen sau proces*. *Modelele software ale entităţilor specifice sunt compuse din*

algoritmi şi date". Algoritmul reprezintă un set stabilit de reguli şi procese bine definite şi mai puţin ambigue pentru soluţionarea unei probleme într-un număr finit de paşi iar datele sunt proprietăţi ale unei entităţi care sunt exprimate prin valorile parametrizate, discrete care descriu atributele acesteia. Modelul este, în mod obiectiv, limitat, el nu poate să cuprindă în structura sa toată multitudinea de proprietăţi ale fenomenului. "Contradicţia fundamentală a modelului constă în aceea că el nu coincide cu scopul propus, dar serveşte la cunoaşterea acestuia, fapt care nu întotdeauna se obţine la prima variantă, ci, de regulă, prin perfecţionarea permanentă a modelului, prin negarea dialectică a unui model de către altul."[3]

Conceptul de modelare integrată a luptei şi a operaţiei a fost propus relativ recent în modelarea şi simularea militară şi răspunde unor cerinţe fundamentale ale planurilor master, atât din perspectiva alinierii la cadrul tehnic comun de modelare şi simulare, cât şi din nevoia de a asigura consistenţa modelelor care reprezintă aceeaşi realitate (lupta, operaţia), dar urmăreşte ţinte diferite (evaluare, antrenament, planificare, sprijin operaţional).

Modelarea integrată a luptei este un proces interactiv care începe cu reprezentarea directă a conflictului, continuă cu evaluarea şi simularea lui, revine în punctul iniţial pentru validarea continuă printr-o nouă reprezentare directă, validată, ca un model complet integrat (un set de modele analitice şi euristice ale conflictului, împreună cu uneltele asociate de evaluare şi simulare), se contiună cu o completă evaluare şi optimizare, şi cu o simulare detaliată, şi se opreşte în cadrul aplicaţiilor finale.

În principiu, un *model integrat al luptei trebuie să permită efectuarea întregii game teoretice şi experimentale ale modelului* (analiză, sinteză, evaluări, optimizări şi simulări). Dar aceasta impune existenţa unui model matematic al luptei, reclamând deci folosirea cercetării operaţionale. Întrebarea de fond care se pune acum este de a şti dacă este posibilă modelarea matematică a oricărui conflict. Ea are un răspuns afirmativ şi generează, la rândul ei, o altă întrebare fundamentală, aparent nouă, şi anume „care sunt trăsăturile relevante ale unui conflict?". Un răspuns complet la această întrebare a fost dat de vechea, dar încă actuala monografie a colonelului Dupuy, care prezintă o teorie a luptei elaborată de Historical Evaluation and Research Organization (HERO). Aceasta scoate în evidenţă următoarele componente (submodele) ale unui model al luptei: *modelul potenţialului de luptă, al rezultatului luptei, procedurile scenariului luptei, regulile pentru vitezele de înaintare, pentru pierderile în personal şi armament (blindate, artilerie şi alte arme), ratele de epuizare a forţelor şi spijinul aerian.* În teoria HERO a luptei aceste modele sunt numai euristice, dar fiecare dintre ele poate fi convertit într-un model analitic echivalent, denumit model dual.

Este necesară o discuţie aparte cu privire la modelarea analitică a scenariului operaţei, care a fost inspirată, în plus, de implementarea scenariului în componenta Heuristical Combat Evaluator (HCE) a programului FORCES. Aceasta a fost „văzută" ca un arbore de joc al ramificării evenimentelor de luptă ale operaţiei şi a fost implementată în Verificatorul de Traseu – nucleul tehnologiei HCE – proiectat ca o unealtă de sprijin a interacţiunii soldat-maşină care asigură un control simplu, dar eficace, al ramificării jocului sub controlul jucătorului responsabil, asigurarea fezabiltăţii cursului acţiunilor.

Această reprezentare a scenariului sugerează modelarea lui cu ajutorul grafurilor, dar modelul implementat nu este un arbore, deoarece acesta are o ramificaţie potenţial explozivă. Ca urmare, modelul implementat este un multigraf, având pe fiecare direcţie de acţiune câte un graf orientat, conex, fără bucle, care modelează programul de înlănţuire a acţiunilor pe direcţie. În felul acesta, controlul de supervizare al jucătorului a fost mutat de la procesul de ramificare.

Dezvoltarea Modelului Conceptual al Spaţiului Misiunii al operaţiilor militare este o problemă mereu actuală, care obligă la reevaluarea periodică a procesului de dezvoltare, în vederea armonizării lui cu noile obiective. *Elaborarea unui model conceptual al spaţiului misiunii al operaţiei are ca punct de pornire precizarea clară a misiunii forţelor participante la operaţie.*

În termeni generali, acesta poate fi reprezentat sub forma unei liste de sarcini esenţiale pe care forţele participante la operaţie trebuie să le îndeplinească, în conformitate cu ordinele de luptă primite. Aproape întotdeauna, această listă cuprinde, ca sarcini prioritare, nimicirea sau anihilarea forţelor adversarului, cucerirea mediului ambiant natural ocupat de el şi crearea de condiţii favorabile pentru operaţiile ulterioare. *Dar conţinutul principal al modelului îl reprezintă precizarea entităţilor (forţelor) participante la operaţie şi a acţiunilor şi interacţiunilor utilizate de ele pentru îndeplinirea misiunii.* Noţiunea „cheie", aici, este cea de „*scenariu al operaţiilor*", prin care se reprezintă în model concepţia operaţiei. În practica simulărilor actuale, scenariul operaţiei este un model logic, numit „model agregat", care reprezintă modul de înlănţuire a acţiunilor, de luptă sau de sprijin, planificate, dar o modelare mai eficientă a lui poate fi realizată printr-un graf orientat, prin care se oferă posibilitatea realizării unui model matematic adecvat al operaţiei.

Pasul următor al modelării este dat de *reprezentarea adecvată a acţiunilor operaţiei* şi constituie, în fond, un proces de reiterare a modelării, la nivelul acţiunilor, adică de realizare a unor modele conceptuale ale spaţiului misiunii (MCSM) adecvate pentru fiecare acţiune planificată. Sau, altfel spus, un MCSM al operaţiei este, de fapt, o reţea de MCSM-uri asociate acţiunilor operaţiei a cărui topologie este determinată de scenariul operaţiei. Realizarea unui MCSM al

unei acţiuni necesită precizarea forţelor participante la acţiune, a modului în care ele acţionează pentru îndeplinirea misiunii încredinţate, a regulilor care dirijează începerea şi oprirea acţiunii, precum şi a modului de apreciere a rezultatelor cantitative şi calitative (logice) cu care ea se încheie.

Pentru corelarea lor cu misiunea operaţiei, modelarea trebuie să includă, de regulă, o reprezentare adecvată a pierderilor şi recuperărilor, iar în cazul acţiunilor terestre şi a ritmurilor de înaintare. În acest scop pot fi folosite fie modele analitice deterministe, din familia ecuaţiilor lui Lanchaster, sau stocastice, în cazul eşaloanelor mici sau al prezenţei incertitudinilor asupra parametrilor modelelor deterministe, fie euristici tactico-operative, bazate pe experienţe de război, care le oferă credibilitate mai mare în faţa utilizatorilor.

Ultimul pas al modelării îl constituie reprezentarea adecvată a rezultatelor finale ale operaţiei care se obţin prin cumularea rezultatelor similare ale acţiunilor, ponderate de importanţa lor pentru operaţia în ansamblu, şi raportarea lor la grila de evaluare utilizată pentru aprecierea gradului de îndeplinire a misiunii.

În elaborarea modelului conceptual al spaţiului misiunii operaţiei se întâlnesc două tendinţe contradictorii. *Prima* este de a realiza o reprezentare cât mai fidelă a spaţiului misiunii şi este justificată prin dorinţa de a realiza un înalt realism operaţional. *Cea de-a doua* tendinţă constă în simplificarea modelului, cu scopul obţinerii unui model fezabil, apt să soluţioneze problemele specifice utilizării sale: dezvoltarea doctrinei şi tacticii, evaluarea performanţelor unităţii, sprijinul operaţional pentru planificarea, executarea şi analiza operaţiei, analize de sprijin ale securităţii naţionale pentru dezvoltarea politicii de apărare. În principiu, simplificarea constă în înlocuirea unor submodele ale operaţiei printr-un sistem de parametri raportaţi la context, care produc în model efecte similare cu cele ale submodelelor înlocuite.

În final, remarcăm că fiecare conflict poate fi reprezentat printr-un set de modele ale sale, dependent de trăsăturile originalului care au fost ignorate în procesul de modelare, şi că fiecare model individual prezintă avantaje specifice în raport cu obiectivele modelării, în felul acesta realizându-se o integrare chiar în interiorul modelului. Astfel, modelarea integrată a luptei poate acoperi toate tipurile de simulări prezentate, prin modele duale corespunzătoare lor, realismul operaţional şi gradul de abstractizare nu vor mai fi invers corelate, cu consecinţe pozitive asupra satisfacerii de către model a cerinţelor pentru succes ale utilizatorului.

Este cunoscut faptul că pregătirea acţiunilor militare reprezintă o activitate cu o însemnătate covârşitoare pentru buna desfăşurare a acestora. Pregătirea eficientă probează, în mare măsură, poate chiar în primul rând, capacitatea de conducere a comandamentelor. Acestea trebuie să prevadă, să planifice, să

organizeze şi să coordoneze acţiunile marilor unităţi (unităţi), pe baza principiilor unităţii de comandă, al promovării spiritului de echipă, al asigurării concordanţei dintre subiectul, obiectul şi scopul conducerii, apropierii conducerii de execuţie. Ca mijloace de instruire, tehnologiile de simulare şi comunicaţiile adecvate pot reduce semnificativ activităţile de supraveghere şi control necesare în cazul experimentărilor operaţionale ori al exerciţiilor, creând în plus posibilitatea de colectare, procesare şi integrare automată a bazelor de date, precum şi a informaţiilor şi concluziilor legate de activitatea de experimentare propriu-zisă, ulterior putând fi analizate, criticate, valorificate, interpretate sau chiar resimulate, pentru obţinerea rezultatelor maxime.

Modernizarea echipamentelor de luptă a determinat, printre altele, şi apariţia unor tehnici şi procedee de instruire, dintre care simularea a devenit cea mai larg întrebuinţată, suficient de agreată în multe ţări şi foarte mult stimulată de tehnologiile avansate. Procedeul de simulare a fost adoptat în extrem de multe domenii de activitate, inclusiv în cel militar, fiind foarte eficient. În prezent, putem remarca trecerea de la simularea în scop de instruire la simularea în scop de decizie, în sensul că, prin simularea unei variante a cursului acţiunilor militare, se pot estima efectele acestora, respectiv se poate verifica dacă o decizie poate duce sau nu la realizarea obiectivului propus, se pot aduce corecturile necesare astfel ca, înainte ca decizia să se transforme în directive şi ordine de acţiune, aceasta poate fi îmbunătăţită succesiv, până la varianta optimă.

Folosirea modelelor şi protocoalelor digitale în procesele de simulare, a celor care folosesc modele practice de instruire, simulând urmările posibile ale unor acţiuni planificate, dar încă neexecutate, ar putea să permită instruirea operaţională combinată (prin simulare, realitatea adevărată şi realitatea virtuală), integrând toate armele şi serviciile, precum şi componente din diferite ţări. Acest sistem poate permite instruirea combinată a subunităţilor situate în diferite zone sau facilităţi de instruire, indiferent de dislocarea acestora, precum şi modelarea echipamentelor şi materialelor adecvate diverselor tipuri de misiuni şi situaţii posibile.

Studierea experimentală a unui model este denumită şi *simulare* şi este preferată în situaţiile în care studierea pe cale analitică este imposibilă sau prea laborioasă. Modelul sistemului sau procesului astfel studiat este denumit model de simulare şi este, în cel mai fericit caz, un model matematic. Rezultă, astfel, unitatea organică dintre modelare şi simulare, precum şi faptul că simularea oferă întotdeauna posibilitatea studierii unui model, atunci când studierea sa analitică nu este aplicabilă.

Cuvântul simulare derivă din latinescul "*simulatio*", care înseamnă capacitatea de a reproduce, a reprezenta sau a imita ceva. În ştiinţă, termenul

simulare a fost folosit prima dată de către J. von Neumann şi S. Ulam, în anii 1940-1944, cu ocazia lucrărilor de cercetare în domeniul fizicii nucleare efectuate în SUA împreună cu grupul de cercetători ai şcolii „Los Alamos" care au realizat prima bombă atomică. Folosirea termenului de simulare este justificată în acest caz, prin scopul particular al modelării, şi anume reproducerea în decursul timpului, cu ajutorul modelului de simulare, a comportamentului relevant al originalului.

Se poate aprecia că simularea desemnează tehnica de studiere experimentală a unui model al operaţiei, în scopul obţinerii unor concluzii relevante asupra originalului, prin imitarea ducerii operaţiei cu ajutorul modelului şi observarea, colectarea, înregistrarea, prelucrarea datelor astfel obţinute. Ca *metodă de studiu a realităţii*, simularea îşi găseşte un loc bine conturat în procesul de selectare a metodelor de luare a deciziei, între metodele intuitive şi cele analitice, şi poate fi utilizată separat (ca variantă independentă) sau în completare cu oricare din celelalte metode.

Simularea operaţiilor desemnează acea tehnică de *studiere experimentală* a unui model al operaţiei în scopul obţinerii unor concluzii relevante asupra originalului, prin imitarea ducerii operaţiei cu ajutorul modelului şi observarea, colectarea, înregistrarea şi prelucrarea datelor astfel obţinute. Folosirea, în acest caz, a simulării este consecinţa directă a particularităţilor modelului.

Simulările militare au fost clasificate, în decursul timpului, după diferite criterii, în funcţie de natura originalului, de scopul urmărit prin simulare, de particularităţile modelului de simulare şi de caracteristicile constructive ale suportului tehnologic al simulării. Din punctul de vedere al scopului urmărit, prin simulare se disting următoarele tipuri de utilizări: *antrenamentul individual sau în grupuri de diferite mărimi care s*usţine antrenamentul în organizarea de luptă şi oferă oportunităţi pentru exersarea deprinderilor de stat major; *cercetarea şi analiza unor probleme militare complexe; planificarea misiunii şi sisteme pentru repetiţia generală în vederea îndeplinirii ei; simularea sistemelor de arme pentru antrenamentul operatorilor.*

O clasificare autorizată[4], larg utilizată a modelelor şi simulărilor distinge trei tipuri de simulări: reală, virtuală şi constructivă. Ea este însă problematică întrucât nu sunt suficient de clare limitele dintre categoriile sale şi pentru că exclude categoria de simulări care implică personal simulat care operează asupra unui echipament real. Cu alte cuvinte, cele trei categorii sunt descrise astfel: s*imulare reală* – reprezintă o simulare care implică personal real operând asupra sistemelor reale; s*imulare virtuală* – reprezintă o simulare care implică personal real operând asupra unui sistem simulat (aceasta introduce conceptul „omul în buclă" – Human in the loop – ca având un rol central în simulare, exercitând

controlul asupra procedurilor de operare, de decizie sau de comunicare); s*imulare constructivă* – reprezintă simulările care implică personal simulat, operând asupra unui sistem simulat; cuprinde, de asemenea, şi un personal real care stimulează simularea (introduce stimuli), dar care nu este implicat în determinarea răspunsului acesteia. Această taxonomie a fost preluată şi de către NATO[5]. Simularea constructivă oferă abilităţi pentru analiza conceptelor, prognoza rezultatelor posibile şi solicită organizaţii de dimensiuni mari. Forţa ei constă în oferirea unor oportunităţi pentru a face măsurători, a genera statistici şi a executa analize.

Simularea are potenţialul de a înlocui anumite medii de instruire, de a spori valoarea, calitatea şi veridicitatea instruirii şi de a amplifica procesul de instruire. În consecinţă, activităţile pot fi parcurse, în interiorul sistemului de simulare, fără întrerupere, datorită siguranţei oferite de mediul informatic. În acelaşi timp se ţine cont şi de limitele simulării, care se referă, în principal, la proporţiile antrenamentelor, care totuşi se desfăşoară în afara câmpului real de luptă, fără muniţie reală - aspecte care conduc la anumite limite ale instruirii.

Se acţionează pentru menţinerea unui echilibru între instruirea reală şi cea simulată cu folosirea celor mai bune avantaje ale fiecăreia dintre ele, în funcţie de situaţie. În anumite, situaţii instruirea prin simulare poate fi parte de sine stătătoare a ciclului de instruire integrată ansamblului sau poate fi utilizată secvenţial pe anumite niveluri ale palierului instruirii. Folosirea simulatoarelor la nivelul instruirii individuale şi de echipă poate crea uneori premise pentru întrebuinţarea acestora în cadrul instruirii colective ori, conjunctural, în alte medii de instruire.

Un exemplu edificator în acest sens este operatiunea "Iraqi Freedom", unde, conform celor afirmate de către generalul Franks, înainte de începerea ostilităţilor, trupele au beneficiat de un număr semnificativ de exerciţii majore în teren, precedate de o serie de exerciţii asistate de calculator şi urmate de mai multe repetiţii, toate acestea oferind posibilitatea statelor majore să lucreze împreună pentru o perioadă mai lungă de timp. Armonizarea lucrului în cadrul comandamentelor de unităţi şi mari unităţi ar trebui să reprezinte una dintre priorităţile noastre, conştientizând, în acelaşi timp, faptul că ***"operaţiile sunt operaţii"***, toate celelalte nefiind altceva decât, cu riscul de a mă repeta, ***"operaţii administrative"***, care copleşesc comandamentele şi pun comandanţii în situaţii neprevăzute. De fapt, ceea ce ne dorim este ca, pentru fiecare scânteiere de inteligenţă, pentru fiecare probă de rafinament al gândirii tactice, să dispunem de un mijloc de analiză şi evaluare a rezultatelor.

Simularea oferă mijloace pentru micşorarea presiunii bugetare şi posibilitatea ca anumite echipamente să fie îmbunătăţite, judicios exploatate, perfecţionate, asigurând creşterea calităţii acestora şi, implicit, a calităţii sistemului de instruire, în ansamblu, cu determinări asupra calităţii armatei în întregul ei.

Acest trend este caracteristic marii majorităţi a armatelor moderne, el continuă şi se poate constata o reală accentuare a implementării simulării în noile echipamente şi instalaţii, încă de la faza de proiect şi folosirea software-ului simulării în cadrul sistemelor operaţionale.

Una dintre tendinţele actuale constă în utilizarea reţelelor de simulatoare, în care echipamentele reale sunt legate de simulatoare. Această tehnică este utilizată deja cu succes atât în armata SUA cât şi în alte armate şi permite personalului să se antreneze în locaţiile lor de reşedinţă şi să evite deplasările de trupe pentru nevoi de antrenament. Cercetarea în acest domeniu presupune cunoştinţe multiple, în special din domeniile: automatică, ştiinţa calculatoarelor şi tehnologia informaţiilor, ştiinţe militare, geografie. Este de remarcat faptul că şi la noi s-a verificat experimental posibilitatea distribuirii simulării, la nivelul armatei existând un grup de lucru preocupat de realizarea modelului funcţional şi identificarea tehnologiilor necesare distribuirii simulării între aplicaţiile care utilizează protocoale diferite.

Este din ce în ce mai evidentă cerinţa majoră care stă în faţa modelării şi simulării militare actuale, care decurge din nevoia integrării totale a tuturor sistemelor utilizatorilor militari (senzori, sisteme de comandă şi control, sisteme de arme, sisteme de instruire, antrenament, planificare şi sprijin operaţional). Se impune, astfel, integrarea sistemelor M&S în setul de unelte analitice şi informatice ale utilizatorului. Implementarea simulării distribuite va duce, pe de o parte, la mărirea încrederii, susţinerea reciprocă a participanţilor şi creşterea performanţelor în timp real. Pe de altă parte, utilizarea programelor de simulare distribuită trebuie să fie transparentă pentru toţi utilizatorii.

O primă reglementare cu privire la realizarea unui cadru tehnic comun Common Techical Framework (CFT) pentru M&S a fost făcută în cadrul Modeling and Simulation Master Plan al Departamentului Apărării SUA, urmărind să se asigure utilizarea eficientă şi efectivă a modelelor şi simulărilor, prin facilitarea interoperabilităţii şi reutilizării.

În conformitate cu acest obiectiv, CFT constă în: o arhitectură comună de nivel înalt – High Level Architecture – HLA – faţă de care să se conformeze toate modelele şi simulările; modelele conceptuale ale spaţiului misiunii – CMMS – care să asigure o bază pentru dezvoltarea unor reprezentări consistente şi autorizate a simulărilor; standarde de date care să asigure o reprezentare comună a datelor pentru toate modelele, simulările şi sistemele C4I cu care ele interacţionează.

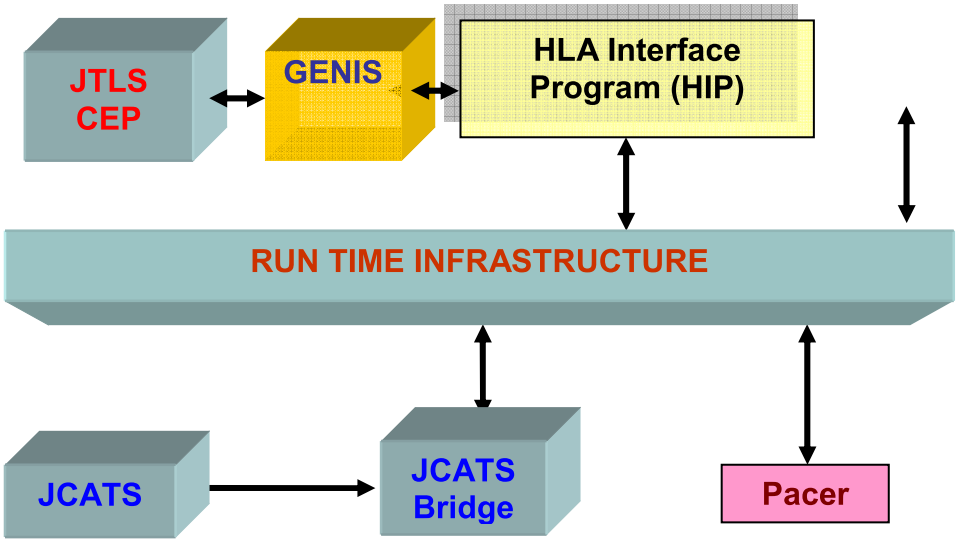
În ceea ce priveşte HLA (arhitectura de înalt nivel), aceasta este o arhitectură tehnică dezvoltată pentru a facilita interoperabilitatea sistemelor de simulare. Permite distribuirea simulării între diferite sisteme de simulare pentru a fi elaborate şi executate o gamă largă de aplicaţii, într-un mod standardizat. De

exemplu, aceste aplicaţii pot sprijini analizele, experimentele, achiziţiile de tehnică şi tehnologie, instruirea şi învăţământul.

De asemenea, permite combinarea sistemelor de simulare existente cu noi sisteme, mixând limbaje de programare şi sisteme de operare diferite. Arhitectura a fost inspirată din câteva protocoale de simulare anterioare ca DIS – Simulare Interactivă Distribuită – (Distributed Interactive Simulation) şi ALSP – Protocol de Simulare la Nivel Unificat – (Aggregate Level Simulation Protocol). Aceste tehnologii individuale au jucat un rol important în cadrul diferitelor domenii de simulare, dar nu au fost în totalitate capabile să îndeplinească cerinţele comunităţii M&S, în special interconectarea simulărilor.

Se pot exemplifica cele afirmate prin prezentarea federaţiei unei Arhitecturi de Înal Nivel (HLA), federaţia JTLS (Sistemul de simulare a acţiunilor militare la nivel teatru de operaţii - Joint Theater Level Simulation) – JCATS (Sistemul de simulare la nivel tactic în context întrunit - Joint Conflict and Tactical Simulation), acestea reprezentând principalele simulări de tip constructiv în cadrul NATO. Obiectivele acesteia constau în sprijinul instruirii de tip întrunit pentru eşaloane multiple, cerinţă care se adresează modelării multi-rezoluţie (Multi-Resolution Module - MRM) în condiţiile administrării unor resurse limitate.

Dezvoltarea modelului conceptual a fost decisiv pentru atingerea obiectivelor federaţiei, acesta bazându-se pe scenarii care descriu „lumea reală”. Arhitectura federaţiei JTLS – JCATS este prezentată în figura de mai jos.



Arhitectura Federaţiei JTLS – JCATS

Evenimentele şi incidentele sunt produse de un program pentru generarea evenimentelor de luptă (Combat Events Program – CEP) din JTLS care serveşte ca „motor" pentru jocul de război şi care comunică cu sistemul GENIS, componentă a Sistemului de Control Grafic al Intrărilor (GIAC – Graphical Input Aggregate Control System).

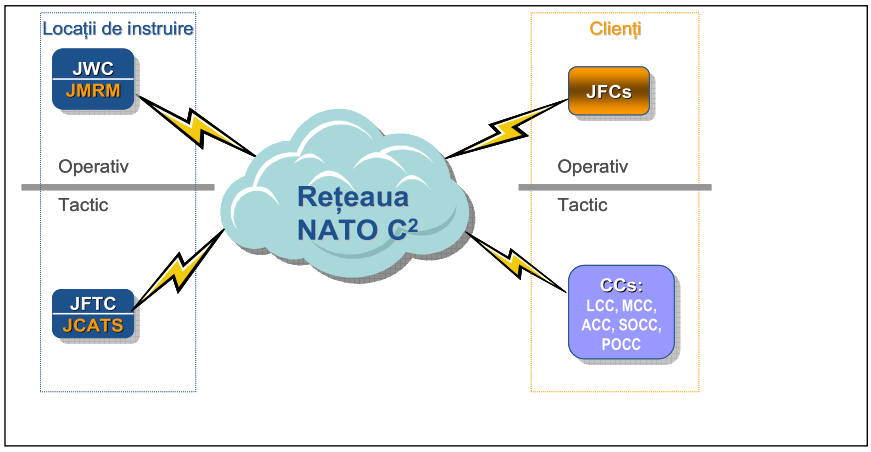
Interfaţa arhitecturii de înalt nivel (HLA) transmite şi primeşte baza de date pentru jocul de război pentru şi de la federaţie prin intermediul infrastructurii de sincronizare a timpului de lucru (Run Time Infrastructure - RTI). Infrastructura de sincronizare (RTI) realizează şase categorii de servicii: managementul federaţiei pentru arhitecturi mai largi, ca de exemplu crearea şi îmbinarea cu alte federaţii; managementul protocoalelor, pentru transmiterea şi recepţionarea unor clase specifice de baze de date; managementul entităţilor, pentru transmiterea şi recepţionarea bazei de date existente, a evenimentelor şi incidentelor dorite; gestionarea activităţilor în timp, asigurându-se condiţiile de cauzalitate dintre sisteme; gestionarea dreptului de proprietate, pentru transferul atributelor de la o federaţie la alta; gestionarea distribuirii bazei de date, pentru asigurarea unei filtrări optime a informaţiilor, dincolo de serviciile oferite prin protocoalele dintre aplicaţiile interconectate.

Punctul forte al federaţiei JTLS – JCATS constă în capacitatea acesteia de a transmite controlul entităţilor simulate de la o simulare la alta, permiţând entităţilor să fie modelate la oricare nivel al rezoluţiei. ***Modelarea multi-rezoluţie*** (***Multi-resolution Modeling - MRM)*** este necesară pentru a evalua diferenţele dintre cele două simulări. Acest model reprezintă de fapt un sistem integrat care va fi capabil să sprijine integrarea exerciţiilor multi-eşalon, la nivel teatru de operaţii, cu structuri mici şi acţiuni individuale de luptă, fiind astfel îmbunătăţite.

Modelarea multi-rezoluţie nu este numai o funcţie de reprezentare a obiectelor. Funcţionalitatea JTLS şi JCATS nu este aceeaşi în toate domeniile şi aceasta oferă oportunităţi pentru implementarea modelării multi-rezoluţie, în timp ce, mai important este că oferă o funcţionalitate sporită pentru utilizator. Obiectivele modelării multi-rezoluţie sunt: sprijinul instruirii simultane a forţelor, în cadrul unor scenarii complexe, la mai multe niveluri, în context întrunit; prezentarea, în detaliu, a modelelor JTLS şi JCATS; asigurarea posibilităţii desfăşurării exerciţiilor, întrebuinţând simularea distribuită; asigurarea unui cost redus al cheltuielilor necesare exerciţiilor; sprijinirea desfăşurării atât a exerciţiilor care folosesc baze de date clasificate, cât şi a celor care folosesc baze de date neclasificate; asigurarea unei funcţionalităţi complementare; asigurarea unui controlul al configurării federaţiei pentru utilizatori.

La nivelul NATO, prin proiectul SNOW LEOPARD (SL – figura de următoare) se doreşte crearea unei reţele NATO Joint pentru educaţie şi instruire,

cu capabilităţi la nivel strategic, operativ şi tactic, prin conectarea reţelelor şi capabilităţilor existente la nivel naţional. Acest proiect va consta într-o reţea distribuită între organizaţiile, naţiunile şi partenerii NATO, cu scopul de a participa la creşterea instruirii, educării şi experimentării distribuite. Capabilitatea NATO SNOW LEOPARD este în curs de formare. Snow Leopard va fi în măsură să ofere instruire pentru Forţa Rapidă de Răspuns a NATO, comandamente multinaţionale întrunite, precum şi naţiunilor membre şi partenere NATO, în concordanţă cu întregul spectru de misiuni de îndeplinit, folosind metodele şi procedeele de instruire reală, virtuală şi constructivă, precum şi mediile specifice exerciţiilor pentru repetarea misiunii.



Arhitectura proiectului SNOW LEOPARD

În concluzie, putem constata că atât în domeniul conducerii militare, al creaţiei tehnice şi tehnologice, cât şi în cel acţional, este necesar ca resursa umană specializată să facă o permanentă investiţie de inteligenţă, acţionând creativ şi inovativ. Instruirea trupelor trebuie să vină în completarea unor concepţii ale operaţiilor care pun accentul pe neprevăzut şi contracararea sa. Pe timpul instruirii, trupele şi statele majore trebuie puse în situaţii cât mai puţin familiare şi forţate astfel să gândească creativ. Chiar dacă omul este decidentul, tehnologia şi în special simularea îl ajută să domine virtual realitatea până când angajează forţele şi mijloacele reale. Dacă putem afirma că în programele de simulare este concentrată ştiinţa, tot astfel putem spune că ele nu pot înlocui arta, imaginaţia omului, a decidentului. Unul dintre elementele importante ale instruirii este, de fapt, grija faţă de om, căutându-se a se identifica cele mai realiste proceduri de evitare a fratricidului.

Pentru realizarea unei calităţi corespunzătoare a simulării este necesară încorporarea în model a experienţei de război. *Experienţa[6] de război* este înmagazinată în experienţa personală a comandanţilor şi statelor majore; datele înregistrate despre războaiele anterioare; „documentaţia" de război; studiile şi analizele specifice cercetărilor operaţionale; arhivele militare. Ea se introduce în model prin structura potrivită a acestuia, urmată de un proces adecvat de „acordare" şi „calibrare".

Militarii de carieră continuă încă să fie sceptici cu privire la capacitatea simulării pe calculator, de a reprezenta corect procesele de luptă. Ei au, totuşi, un rol activ în creşterea calităţii modelării, pentru obţinerea celor mai bune modele cu putinţă. Pentru aceasta este necesar ca ei să se convingă de avantajele oferite de simulare şi să realizeze că simularea nu îi împiedică, ci, dimpotrivă, îi ajută. Pe de altă parte, modelatorii trebuie să-şi înfrângă tentaţia pentru modele „elegante", dar nerealiste, în favoarea unor modele „murdare", dar care reflectă experienţa profesională. Poate, mai devreme sau mai târziu, vom înţelege că, într-adevăr, pentru noi militarii, *totul, cu excepţia războiului, este simulare.*

Note bibliografice

[1] DOD 5000.59 - MODELING AND SIMULATION (M&S) MASTER PLAN, DoD, October 1998.

[2] NATO MODELING AND SIMULATION MASTER PLAN, Version 1.0, Document AC/323 (SGMS) D/2,7 -2004.

[3] Cam. (r) dr. Vasile GRAD, Ion STOIAN, Emil-Carol KOVACS, Vasile DUMITRU, *Cercetare operaţională în domeniul militar*, Editura Sylvi, Bucureşti, 2000, p.78.

[4] DOD 5000.59-MODELING AND SIMULATION (M&S) MASTER PLAN, DoD, October 1995.

[5] NATO MODELING AND SIMULATION MASTER PLAN, Version 1.0, Document AC/323 (SGMS) D/2,7 August 2004.

[6] Ben-Itzhak, U., *Introducing War Experience into Staff Trainer,* NATO PfP/PWP „Simulators and Simulation-Powerful Means Enabling Allied Forces to Reach Interoperability", Brno, Czech Republic, May 5-7, 1999.

SISTEMUL C4I PENTRU FORŢELE TERESTRE. PREZENT ŞI PERSPECTIVE

General-maior dr. Dan GHICA- RADU
Locotenent-colonel Ştefan PREDA

În cadrul sistemului militar, de-a lungul timpului, au existat multe încercări de a defini cu acurateţe ce trebuie să facă un comandant pentru a-şi conduce trupele, pentru a exercita actul de comandă. În timp, s-a ajuns la definiţia conform căreia *comanda* reprezintă autoritatea şi responsabilitatea cu care un comandant/şef este investit în mod legal pentru a o exercita asupra unei structuri militare, incluzând autoritatea pentru utilizarea tuturor resurselor puse la dispoziţie, planificarea, conducerea şi coordonarea utilizării forţelor alocate în scopul îndeplinirii misiunilor primite.

Pe măsură ce războiul a devenit mai complex, conceptul de „*comandă*" a evoluat, devenind „*comandă şi control*" (C2). *Controlul* a devenit parte intrinsecă a actului de comandă, reprezentând autoritatea exprimată de un comandant asupra activităţilor sau a unor părţi din activităţile structurilor subordonate sau a altor structuri care nu sunt, în mod obişnuit, sub comanda sa, care include responsabilitatea de a da ordine şi directive.

Dezvoltarea tehnologică din a doua jumătate a secolului trecut a avut implicaţii majore în ceea ce priveşte fenomenul militar, rolul comunicaţiilor devenind vital în exercitarea comenzii şi controlului, dar şi în gestionarea tot mai complexelor şi sofisticatelor sisteme de armament. Astfel, s-a ajuns la formula *C3* (*comandă, control şi comunicaţii*).

Prin creşterea ponderii componentei informaţionale s-a impus, de asemenea, ca vitală, gestionarea unei noi laturi, tot mai decisive, a acţiunii militare, *confruntarea informaţională*, care implică producerea şi diseminarea informaţiilor

militare, fapt ce a condus la formula *C3I (comandă, control, comunicaţii şi infromaţii militare)*.

În etapa actuală, prelucrarea vastului volum de informaţii şi necesitatea luării deciziilor în ritm deosebit de rapid (pentru a devansa oponentul) au determinat omniprezenţa calculatoarelor, ceea ce a condus la forma actuală de *C4I (comandă, control, comunicaţii, calculatoare şi informaţii militare)*.

Sistemul de comandă, control, comunicaţii, calculatoare şi informaţii (C4I) reprezintă un ansamblu de sisteme integrate de doctrine, proceduri, structuri organizatorice, personal, echipament, facilităţi şi comunicaţii destinate să sprijine exercitarea procesului de comandă şi control în toate fazele (stările) operaţiei.

Sistemul C4I este destinat să asigure transmiterea informaţiilor între structurile organizatorice şi mijloacele tehnice de prelucrare din spaţiul de luptă, dincolo de orizontul vizibil şi invizibil. Toate sistemele de comunicaţii şi informatice militare, de la semnalizatoarele antice la cele mai recente sisteme bazate pe computere, nu sunt decât dezvoltări tehnice cu acelaşi scop – transmiterea informaţiilor între şi în cadrul structurilor organizatorice luptătoare.

Obiectivele fundamentale ale sistemelor C4I

a. *Realizarea unităţii de efort*. Sistemele C4I trebuie să ajute forţele luptătoare şi de sprijin, să combine ideile şi aprecierile comandanţilor şi personalului cu funcţii importante în cadrul comandamentelor şi structurilor organizatorice subordonate. Astfel, se permite exprimarea opiniilor cât mai multor experţi/specialişti în activitatea de elaborare a deciziilor, comanda şi controlul operaţiilor în timp real sau aproape real şi, în final, îndeplinirea cu succes a misiunilor primite.

b. *Exploatarea tuturor capacităţilor forţei*. Sistemele C4I trebuie să fie planificate ca extensii ale simţurilor şi proceselor specific umane şi să ajute personalul militar în formarea percepţiilor reale, să reacţioneze corespunzător la acestea şi să elaboreze decizii. Acestea permit personalului de stat major să acţioneze eficient pe timpul operaţiilor cu ritm înalt de desfăşurare. Sistemele C4I trebuie să aibă timp de răspuns cât mai mic, să fie uşor de înţeles şi de exploatat, în special pe timpul rezolvării unor situaţii care implică un nivel ridicat de stres.

c. *Localizarea corectă a informaţiilor critice*. Sistemele C4I trebuie să aibă capacitatea de a răspunde rapid la cererile de informaţii şi, de aceea, informaţiile trebuie stocate şi menţinute acolo unde sunt necesare. Astfel, se reduc la minim întârzierile în transmiterea sau obţinerea informaţiilor şi se micşorează nivelul de solicitare al reţelelor de comunicaţii.

d. *Fuziunea informaţiilor*. Sistemele C4I trebuie să asigure o imagine complexă şi precisă a spaţiului de luptă în funcţie de cerinţele personalului de stat major. Aceasta se realizează prin fuziunea informaţiilor – reducerea la minim a

volumului de informaţii util şi plasarea lor, în mod convenabil, în cadrul sistemului pentru a fi utilizate în funcţie de cerinţele operaţiei. Astfel, cu informaţii concise, precise, oportune şi semnificative se îmbunătăţeşte unitatea de efort şi se reduce nivelul de incertitudine, permiţând forţei să acţioneze ca un ansamblu unitar, să exploateze, în mod avantajos, condiţiile din spaţiul de luptă modern şi să lupte mai inteligent.

Sistemul C4I asigură comandantului mijloacele necesare pentru exercitarea autorităţii şi conducerii forţelor subordonate şi a celor primite în sprijin, în scopul îndeplinirii misiunii. Statul major utilizează informaţiile în procesul de elaborare a deciziilor şi de coordonare a acţiunilor care vor influenţa, în primul rând, forţele adversarului şi cele proprii în avantajul celor din urmă. Pentru aceasta este necesară o circulaţie optimă a informaţiilor, deci constituirea unor fluxuri informaţionale corecte. Pe timp de război sau în situaţii de criză, sistemele C4I trebuie să asigure un flux de date continuu pentru a oferi informaţii, în timp real, în spaţiul de luptă, în orice loc, în orice moment, la cererea utilizatorilor. Datorită diversificării formelor şi procedeelor de ducere a acţiunii militare şi a supratehnologizării spaţiului de luptă modern, sistemele de tip C4I vor trebui să aibă aceeaşi eficienţă, indiferent de structura şi misiunile forţei luptătoare sau de tipul de acţiune militară în care sunt angajate.

Datorită schimbărilor de profunzime petrecute în ultimii ani în mediul de securitate globală, forţele luptătoare sunt nevoite să participe la acţiuni militare care nu au o desfăşurare liniară în cadrul aceluiaşi tip de acţiune, sau în acelaşi mediu fizic. Trecerea rapidă de la acţiuni cu caracter ofensiv la cele cu caracter defensiv, de la acţiuni militare decisive la operaţii militare altele decât războiul, de la acţiuni militare sincrone la acţiuni militare asincrone obligă comandamentele la efectuarea de schimbări dese în concepţii şi planuri de acţiune care solicită de regulă, un alt tip de flux informaţional. În plus, probabilitatea crescută ca o forţă să participe în timp relativ scurt la acţiuni în diferite regiuni sau zone de pe glob determină modificări esenţiale în conţinutul bazelor de date cu referire la informaţiile despre mediu, societate, cultură etc.

Perfecţionarea tehnologiilor utilizate în asigurarea mobilităţii trupelor, perfecţionarea sistemelor de armament şi senzori contribuie la reducerea timpului de acţiune, sporirea controlului spaţiului de luptă, la creşterea ritmului de ducere a operaţiilor şi la generarea unui volum mare de informaţii. Dacă nici cel puţin aceste elemente nu sunt gestionate corespunzător se pot crea situaţii care vor conduce la afectarea reacţiilor luptătorilor şi, în cele din urmă, ale subunităţilor şi unităţilor.

Sistemele C4I asigură subsistemele de sprijin pentru schimbul informaţional şi elaborarea deciziilor în cadrul procesului de comandă şi control al marilor unităţi şi unităţilor.

Pentru a putea desfăşura operaţiile cu eficienţă, comandamentul unităţii şi marii unităţi, precum şi componentele luptătoare şi de sprijin din compunerea acesteia trebuie să dispună de informaţii. Aceste informaţii trebuie să fie relevante, esenţiale, oportune şi prezentate într-o formă accesibilă pentru a fi înţeleasă şi utilizată rapid de către luptător şi a acţiona optim pentru îndeplinirea misiunilor. Sistemul de sprijin al comenzii şi al controlului reprezintă instrumentul principal la dispoziţia comandantului structurii de forţe, utilizat pentru colectarea, transmiterea, prelucrarea şi diseminarea/distribuţia acestor informaţii.

Operaţiile multinaţionale sunt deosebit de complexe şi presupun angajarea unor structuri militare diverse, solicitate să acţioneze în mod unitar. Forţele multinaţionale pot avea unele particularităţi în organizarea şi funcţionarea sistemelor C4I, limbaj, tehnologie, doctrină, standarde de operare care pot crea confuzii. Acestea din urmă pot conduce la creşterea cerinţelor informaţionale şi a nivelului de incertitudine. Cu cât eşaloanele între care se realizează interfaţarea sunt mai mici, cu atât creşte nivelul de incertitudine şi nivelul cerinţelor la adresa sistemelor C4I. Comandantul trebuie să urmărească cu atenţie sporită structura acesteia, înainte de începerea operaţiilor, pentru a evita unele confuzii în cadrul forţelor proprii. După ce comandantul stabileşte organizarea specifică a comenzii şi controlului pentru o operaţie multinaţională, sunt stabilite cerinţele de schimb informaţional pentru sistemele C4I, în funcţie de unele principii prezentate în continuare.

Trebuie totuşi avut în permanenţă în atenţie faptul că sistemele C4I şi resursele aferente la dispoziţia comandantului sunt limitate şi, de aceea, trebuie gestionate cu atenţie şi eficienţă. Utilizarea raţională începe cu preocuparea şi analiza echilibrată de către comandantul forţei a infrastructurii de comandă şi control bazate pe nevoile prestabilite pentru informaţii importante - minimum de informaţii esenţiale pentru elaborarea deciziei şi îndeplinirea misiunii. Aceasta permite ca resursele limitate ale sistemului C4I, forţele şi resursele aferente să fie utilizate în modul cel mai eficient prin instituirea unui control şi management riguros. Planificarea şi exploatarea resurselor sistemelor C4I se pot eficientiza prin mai multe activităţi.

a. *Echilibrarea raportului scop-forţe-mijloace* solicită angajarea complementară, planificată a tuturor forţelor şi sistemelor implicate în activităţi informaţionale. Forţele şi mijloacele tehnice care constituie sistemul de sprijin al comenzii şi controlului trebuie organizate pe misiuni pentru a colecta, transmite,

prelucra şi proteja informaţiile proprii, concomitent cu desfăşurarea operaţiilor specifice războiului de comandă şi control care vizează degradarea capacităţilor similare ale adversarului.

b. Managementul resurselor de comunicaţii şi informatice presupune planificarea şi realizarea infrastructurii de transport al informaţiilor în concordanţă cu volumul şi orientarea fluxurilor de informaţii preconizat sau estimat.

c. Managementul spectrului electromagnetic reprezintă un factor esenţial în procesul de planificare şi utilizare raţională a resurselor disponibile. Repartiţia şi utilizarea frecvenţelor sunt fundamentale pentru utilizarea mijloacelor radioelectrice. Resursele spectrului electromagnetic sunt gestionate prin legislaţia internaţională şi sunt considerate ca resurse naţionale. Frecvenţele trebuie să fie coordonate şi gestionate pe baza unor principii unice la nivel strategic, operativ şi tactic, printr-o varietate de căi administrative şi tehnice naţionale şi internaţionale.

d. Prioritatea informaţiilor este, de asemenea, importantă pentru stabilirea cerinţelor privind dimensionarea reţelelor C4I şi a centrelor de sprijin din sistem - de exemplu: angajarea, mijloacelor din sistemul C4I pentru transmiterea informaţiilor de cercetare reduce capacitatea de vehiculare a reţelei de către alţi utilizatori care au nevoie de deciziile comandantului forţei pe timpul planificării şi ducerii operaţiei.

e. Nivelul de pregătire al personalului implicat în realizarea şi exploatarea sistemelor C4I, reprezintă unul din aspectele cele mai importante datorită impactului pe care nivelul abilităţilor de operare al acestora îl are asupra intenţiei de eficientizare a utilizării resurselor sistemului.

f. Simplitatea în exploatare se adresează, în mod deosebit, utilizatorului final care, în cele mai multe cazuri, nu este un specialist, iar, din această cauză cu cât modul de operare este mai simplu, dar, în acelaşi timp şi eficient, cu atât va creşte gradul de utilizare eficientă a resurselor sistemului.

La nivelul Forţelor Terestre, plecând de la aspectele menţionate mai sus, sistemul C4I actual este organizat şi structurat astfel încât să asigure nevoile de legătură pentru comanda şi controlul operaţional şi administrativ al forţelor, având o componentă staţionară şi una mobilă.

Regulile generale de angajare a sistemelor C4I sunt următoarele:

a) de la eşalonul superior către eşaloanele subordonate şi cu două eşaloane mai jos;

b) de la eşalonul care sprijină la eşalonul sprijinit;

c) de la structura care întăreşte către cea întărită;

d) de la stânga spre dreapta între unităţile vecine.

În cazul unor situaţii speciale se pot elabora şi aplica alte reguli care să corespundă tuturor cerinţelor informaţionale specifice.

În proiectarea, organizarea şi realizarea sistemului C4I al Forţelor Terestre s-a avut şi se are în vedere asigurarea următoarelor fluxuri informaţionale, pentru nevoile de conducere, cooperare şi înştiinţare**,** după cum urmează:

✓legătura cu eşalonul superior;

✓ legăturile pentru conducerea administrativă a forţelor subordonate: organele militare teritoriale, instituţiile militare de învăţământ, unităţi, subunităţi şi formaţiuni subordonate;

✓legăturile pentru comanda şi controlul operaţional al forţelor subordonate: comandamente operaţionale de nivel tactic tip divizie**,** brigadă, comandamente de mari unităţi şi unităţi subordonate nemijlocit;

✓legăturile cu eşaloanele cu care se cooperează: comandamente NATO, Comandamentul Operaţional Întrunit, Statul Major al Forţelor Aeriene, Statul Major al Forţelor Navale, Ministerul Administraţiei şi Internelor, organe S.R.I., S.P.P. şi S.T.S., organe ale Administraţiei Publice centrale sau locale, agenţii, instituţii şi societăţi economice civile, care au responsabilităţi şi participă la susţinerea efortului naţional de apărare.

Pentru exercitarea oportună şi eficientă a actului de comandă şi control, sistemul de comunicaţii şi informatică utilizează toate mediile de transmitere (fibră optică, cablu de campanie, unde electromagnetice, segment satelitar), care necesită un spectru larg de tehnologii (sisteme radio şi radioreleu, reţele celulare, sisteme satelitare, magistrale radioreleu, sisteme de comutaţie, sisteme de management, sisteme de comandă-control etc.). Structura, tehnologiile şi echipamentele utilizate converg către realizarea unui sistem de comunicaţii şi informatică integrat.

La pace, comanda şi controlul operaţional şi administrativ al Forţelor Terestre se execută din sediile de dislocare la pace, prin infrastructura de comunicaţii militară naţională şi exploatarea elementelor din Centrele de Comunicaţii şi Informatică de Garnizoană.

În situaţii de criză şi la război, în sediile de dislocare la pace, sistemul de comunicaţii şi informatică se amplifică, cu forţele, mijloacele şi echipamentele mobile din dotarea unităţilor, subunităţilor şi formaţiunilor de comunicaţii, informatică, mentenanţă şi logistică din organica structurilor subordonate. Din locaţiile temporare, comanda şi controlul operaţional şi administrativ se execută prin exploatarea elementelor Centrelor de Comunicaţii şi Informatică ale Punctelor de Comandă şi elementelor Centrelor de Comunicaţii şi Informatică de Sprijin.

Din perspectiva capacităţii de asigurare a nevoilor, sistemul C4I actual foloseşte: reţele radio, comunicaţii bazate pe infrastructura tehnologiei informatice (MILNET) şi infrastructura RTP/RMNC.

Statul Major al Forţelor Terestre şi o parte din marile unităţi şi unităţile subordonate au asigurate legături prin reţele securizate şi reţelele radio de garnizoană ale Statului Major General şi au organizate reţele radio de garnizoană cu marile unităţi şi unităţile direct subordonate. Pentru instrucţie, structurile din Forţele Terestre au organizate reţele de instrucţie, conform caracteristicilor de lucru alocate prin dispoziţiunile pe linie de comunicaţii şi informatică.

În teatrele de operaţii sunt organizate reţele radio de informare de luptă şi reţele de comunicaţii aliate.

Din perspectiva utilizării infrastructurii tehnologiei informatice, Forţele Terestre dispun de reţele informatice securizate şi nesecurizate, toate unităţile având în acest moment capabilitatea de a transmite şi primi fişiere prin „dial-up”.

Dotarea structurilor militare din Forţele Terestre cu tehnică modernă de comunicaţii şi informatică, interoperabilă cu cea existentă în armatele statelor membre NATO, s-a realizat conform programelor de înzestrare, ea vizând asigurarea, cu prioritate, a unităţilor şi subunităţilor nominalizate pentru a fi puse la dispoziţia NATO. În acest sens, pentru structurile destinate să îndeplinească misiuni NATO, înzestrarea a fost orientată către realizarea reţelei mobile de campanie, în cadrul căreia echipamentele de comunicaţii radio pe unde scurte şi ultrascurte constituie infrastructura de comandă-control la nivelul eşaloanelor mici (grupă, pluton, companie, batalion), deoarece permit instalare uşoară, mobilitate ridicată şi exploatare oportună. Forţele Terestre au în înzestrare staţii radio cu salt de frecvenţă, în diverse variante constructive, hand-held, portative şi vehiculare, care asigură dotarea parţială a structurilor nominalizate în cadrul obiectivelor forţei, participante la iniţiative regionale şi misiuni internaţionale.

Pentru asigurarea comunicaţiilor voce cu structurile care execută misiuni internaţionale, se utilizează echipamente de comunicaţii prin satelit, portabile sau în cadrul modulelor de comunicaţii desfăşurabile şi reţelele/direcţiile radio organizate.

Pe lângă echipamentele şi capabilităţile menţionate mai sus, există însă un număr semnificativ de echipamente de comunicaţii analogice, uzate fizic şi moral, iar calitatea legăturilor este afectată de lipsa unor canale cu parametri unici, care să respecte standardele internaţionale, normele EUROCOM şi standardele existente în cadrul NATO.

Pentru conducerea structurilor care au aceste tipuri de echipamente s-a adoptat, de regulă, o structură ierarhică, iar calitatea legăturii este afectată de lipsa unor canale cu parametri adaptabili, definiţi conform standardelor internaţionale.

Acest tip de sistem de comunicaţii are o fiabilitate scăzută, generată de modul strict ierarhizat de organizare a acestuia, de siguranţa în funcţionare redusă a mijloacelor tehnice utilizate şi absenţa canalelor de rezervă.

Ca urmare a resurselor financiare limitate şi a derulării procesului de restructurare s-a optat pentru varianta modernizării instalaţiilor de comunicaţii şi informatică de pe tehnica de luptă, prin implementarea de tehnică performantă, interoperabilă NATO şi perpetuarea unui sistem de comunicaţii de tip hibrid, care să permită eliminarea progresivă a tehnicii analogice, în cea mai mare parte realizată după o concepţie rusească, şi care să asigure un minim de fluxuri informaţionale la nivelul eşaloanelor existente. Participarea tot mai accentuată a unităţilor şi subunităţilor din Forţele Terestre la exerciţii, aplicaţii şi misiuni internaţionale, sub egida ONU, OSCE şi NATO, a scos în evidenţă limitele tot mai evidente privind posibilităţile sistemelor existente şi necesitatea actualizării concepţiei de asigurare a suportului tehnic necesar derulării procesului de comandă şi control.

Insuficienta dotare cu tehnică de comunicaţii şi informatică poate îngreuna îndeplinirea la timp şi de calitate a sarcinilor. Aceasta trebuie compensată printr-o repartiţie judicioasă, în scopul asigurării strictului necesar de materiale şi tehnică de lucru, pentru desfăşurarea activităţii şi dotarea ritmică a structurilor implicate la parametri optimi de funcţionare.

În perspectivă, Forţele Terestre au în vedere continuarea modernizării sistemului C4I existent, iar acest lucru se realizează prin sisteme de comunicaţii şi informatice integrate, pentru structurile luptătoare, de sprijin de luptă şi de sprijin logistic de nivel batalion, puncte de comandă de moderne, mobile şi cu capabilităţi C4I avansate, capabilităţi informatizate şi integrate de conducere a focului, sisteme integrate de senzori şi capabilităţi de informatică medicală.

În concluzie, sistemul C4I al Forţelor Terestre asigură, la pace, cu anumite limitări, nevoile de legătură pentru comanda şi controlul administrativ. Pe timp de criză şi la război, sistemul poate asigura nevoile de legătură pentru comanda şi controlul operaţional, limitat în spaţiu şi timp, pe anumite direcţii şi numai cu angajarea infrastructurii naţionale sau extinderea infrastructurii militare (RMNC), cu sprijin din partea structurilor centrale sau aliate. Continuarea modernizării sistemelor C4I în Forţele Terestre rămâne o prioritate, urmărindu-se realizarea deplină a interoperabilităţii tehnice cu sistemele C4I ale celorlalte categorii de forţe ale Armatei României şi armatele statelor membre NATO şi UE.

Bibliografie

1. Dumitru Cristea, Roceanu Ion, *Războiul bazat pe rețea, provocare a erei informaționale în spațiul de luptă*, Editura Universității Naționale de Apărare „Carol I", Bucureşti, 2005.

2. Dumitru Cristea, *Sisteme C4I*, Editura Militară, Bucureşti, 2005.

3. Lt. col. Hurmuz Paul, *Sisteme de comandă, control, computere, comunicații şi informații pentru eşaloanele operative din Armata României*, Teză de doctorat, AISM, 2003.

4. Nejat Ince, *Planning and Architectural Design of Modern C4I Systems*, 1997.

5. Intelligence and Electronic Warfare Operations (FM 34-1), US, 1994.

6. Allied Joint Operations Doctrine(AJP-01), 1997.

7. Allied Joint Intelligence and Security Doctrine(AJP-2), Final Draft, 2001.

8. FM 6-0, Command and Control(Final Draft), US, 2000.

SISTEMUL DE COMANDĂ ŞI CONTROL AERIAN NAȚIONAL (SCCAN)

Colonel (r) prof. univ. dr. Gheorghe BOARU

Introducere

Obținerea *supremației aeriene* sau a unei situații aeriene favorabile (fie şi doar local, temporar sau doar pe anumite direcții) a devenit un obiectiv important pentru strategii militari. În aceste condiții, controlul spațiului aerian de interes devine tot mai important.

Având în vedere vulnerabilitățile şi amenințările, rezultă faptul că forțele aeriene vor desfăşura acțiunile de luptă într-un spațiu de operare militară tot mai complex, corespunzător unui timp de evaluare, analiză şi decizie foarte scurt. Sistemul de Comandă şi Control Aerian Național (SCCAN) trebuie să ofere o capacitate de reacție care să permită sincronizarea acțiunilor forțelor aeriene aflate pe teritoriul/în spațiul aerian al României, cu acțiunile forțelor aeriene ale Alianței, să evite surprinderea, cu posibilitatea desfăşurării acțiunilor defensive în timp real (supraveghere, darea misiunilor, controlul spațiului aerian, etc.) şi să asigure realizarea surprinderii adversarului, prin respingerea rapidă a agresiunii aeriene cu forțe naționale şi forțe din cadrul apărării colective a NATO.

Modalitatea cea mai eficientă de asigurare a unității de efort în apărarea aeriană şi a securității aeriene a României se realizează prin centralizarea controlului tuturor operațiunilor specifice de către un singur comandant, care îşi

exercită autoritatea asupra lor într-un cadru bine definit şi delimitat, existent încă din timp de pace.

Modernizarea şi integrarea Sistemului de Apărare Aeriană a României presupune un proces de adaptare, în special pentru realizarea unei flexibilităţi corespunzătoare în apărarea colectivă, pentru satisfacerea nevoilor apărării aeriene extinse a NATO şi a managementului situaţiilor de criză. În acest context, se apreciază că integrarea acţională a forţelor şi mijloacelor de apărare aeriană ale Forţelor Aeriene, Forţelor Terestre şi Forţelor Navale, în cadrul Sistemului de Comandă şi Control Aerian Naţional –SCCAN, constituie o soluţie viabilă şi de perspectivă pe termen lung.

1. Realizarea sistemului naţional integrat de apărare aeriană

Realizarea sistemului naţional integrat de apărare aeriană este reclamată de existenţa unor mijloace specializate de apărare aeriană din dotarea tuturor categoriilor de forţe ale armatei, care trebuie conduse unitar la nivel naţional, zonal sau sectorial, pentru creşterea eficienţei şi scăderea riscurilor de angajare reciprocă (evitarea fratricidului) pe timpul acţiunii în zonele comune.

Respectarea cerinţelor de bază pentru realizarea integrării acţionale a forţelor care au misiunea specifică de apărare aeriană conferă sistemului de apărare aeriană următoarele caracteristici: modularitate organizatorică şi structurală, mobilitate, flexibilitate, complementaritate acţională, credibilitate operaţională, reacţie oportună şi sustenabilitate.

Datorită caracteristicilor mediului aerian (tridimensionalitate, fără delimitări laterale naturale), în dispunerea forţelor şi mijloacelor se are în vedere pe lângă stratificarea apărării aeriene (combaterea şi nimicirea mijloacelor de atac aerian, în toată gama de înălţimi) şi necesitatea asigurării unei zone de angajare a ţintelor adânc eşalonată pe căile apropiate şi nemijlocite de acces la obiectivele apărate aerian.

Sincronizarea eforturilor de apărare aeriană în cadrul Sistemului de Apărare Aeriană al României revine, în egală măsură, tuturor statelor majore ale categoriilor de forţe ale armatei.

2. Integrarea apărării aeriene a României în sistemul de apărare aeriană NATO – *NATINADS (NATO Integrated Air Defence System)*

În condiţiile actualului mediu internaţional de securitate, NATO a definit şi a validat concepţia cu privire la realizarea Sistemului Integrat de Apărare Aeriană NATO – NATINADS care cuprinde principiile şi concepţiile directoare pentru îndeplinirea misiunii de apărare aeriană colectivă a Alianţei şi asigură generarea capabilităţilor destinate managementului situaţiilor de criză şi conflict.

Amplificarea rolului şi misiunilor NATO pentru menţinerea păcii şi rezolvarea situaţiilor de conflict determină un proces de adaptare a NATINADS, în cadrul apărării colective, pentru satisfacerea nevoilor apărării aeriene extinse şi creşterea contribuţiei la managementul situaţiilor de criză. În acest context, integrarea spaţiului aerian românesc în cel al Alianţei trebuie realizată cu respectarea principiilor şi concepţiilor directoare ale Alianţei, pentru îndeplinirea misiunii de apărare aeriană colectivă. Sistemul de Apărare Aeriană a României trebuie să contribuie simultan la securitatea militară a ţării, la apărarea colectivă a Alianţei şi să asigure capabilităţi pentru managementul situaţiilor de criză.

3. Întrebuinţarea sistemelor de comandă şi control integrate pentru supravegherea şi controlul spaţiului aerian

Sistemul de supraveghere radar a spaţiului aerian al României reprezintă principala sursă de informaţii pentru Sistemul de apărare aeriană naţional, precum şi al Alianţei, în această zonă. Integrarea reală în sistemul de apărare aeriană al Alianţei – ***NATINADS*****,** a impus analiza stării actuale a sistemului naţional de supraveghere radar a spaţiului aerian şi adaptarea acestuia corespunzător acestei cerinţe.

Scopul general al supravegherii spaţiului aerian îl constituie prevenirea surprinderii în cazul unei agresiuni din aer şi asigurarea suveranităţii României în spaţiul aerian propriu, precum şi transmiterea informaţiilor necesare pentru avertizarea timpurie şi alarmarea în sistemul de apărare aeriană integrată a ROMÂNIEI şi a NATO *(NATO Integrated Air Defence System – NATINADS)*.

Amploarea spaţială şi informaţională a acţiunilor de supraveghere a spaţiului aerian necesită organizarea şi funcţionarea tuturor forţelor

specializate într-un sistem unic care să confere noi valenţe dimensiunii acţiunilor sale.

Din punct de vedere acţional, supravegherea spaţiului aerian acoperă cea mai mare şi mai dinamică parte a componentelor informaţionale şi electromagnetice ale dimensiunii verticale a operaţiei. Creşterea rapidă a ponderii acestor componente, mai ales în cadrul operaţiilor aeriene, este o caracteristică majoră a noilor tipuri de conflicte care se prefigurează în viitor.

Din punct de vedere spaţial, acţiunile de supraveghere a spaţiului aerian acoperă întreaga zonă de ducere a operaţiei atât pe teritoriul naţional, cât şi în exterior, în adâncimea dispozitivului advers, în limita posibilităţilor tehnicii din înzestrare. Ducerea cu succes a operaţiilor de apărare aeriană necesită informaţii despre acţiunile inamicului aerian anterior pătrunderii acestuia în zonele de apărat, iar pentru reuşita loviturilor executate de aviaţie în spaţiul advers este necesară, în limita posibilităţilor, cunoaşterea situaţiei aeriene pe traseul de zbor şi din zonele obiectivelor de lovit.

Din punct de vedere temporal, locul supravegherii spaţiului aerian este dat de caracterul de permanenţă al acestor acţiuni desfăşurate (cu intensităţi diferite) încă din timp de pace, continuând, la dimensiuni sporite, pe timpul pregătirii şi ducerii operaţiilor.

Ca urmare toate operaţiile sunt precedate şi includ supravegherea spaţiului aerian, indiferent de caracterul şi anvergura conflictului armat.

Utilizarea spaţiului aerian trebuie să fie optimizată, iar riscul privind pierderile de mijloace aeriene proprii poate fi redus prin restricţionarea libertăţii de acţiune a aeronavelor. Este esenţial ca toţi utilizatorii spaţiului aerian să cunoască măsurile luate şi mijloacele prin care se asigură reducerea la minim a riscurilor privind combaterea mijloacelor aeriene proprii, mărind, în acelaşi timp, la maxim, libertatea lor de acţiune. Aceste măsuri şi mijloace sunt cunoscute, în general, sub denumirea de control al spaţiului aerian.

4. Implementarea Sistemului de Comandă şi Control Aerian Naţional – SCCAN. Compatibilitatea şi interoperabilitatea cu viitorul sistem de comandă şi contol aerian al Alianţei Nord-Atlantice – ACCS

Forţele Aeriene trebuie să participe pe timp de pace, în situaţii de criză şi la război la operaţiile de apărare aeriană integrată sub comandă

NATINADS pentru menținerea controlului asupra spațiului aerian național, ca parte integrantă a spațiului aerian NATO, şi pentru extinderea acestuia asupra spațiului de interes militar strategic. De asemenea, trebuie să asigure pregătirea şi desfăşurarea în teatru a forțelor aeriene „*sub comanda NATO*" şi să participe la îndeplinirea responsabilităților naționale privind generarea şi susținerea logistică a forțelor proprii, precum şi la apărarea teritoriului României, populației şi forțelor aflate pe acesta. În consecință, Sistemul de Comandă şi Control Aerian Național (SCCAN) este necesar să fie în deplină concordanță cu rolul şi misiunile Forțelor Aeriene atât pe plan național, cât şi în NATO.

SCCAN, ca parte a Sistemului de Comandă şi Control (C2) al Armatei României, furnizează capabilitățile de comandă şi control specifice acțiunilor în spațiul aerian pentru a îndeplini obiectivele apărării colective în cadrul NATO, securității naționale şi rezolvării crizelor în spațiul aerian. SCCAN funcționează ca o combinație de structuri organizaționale, personal specializat, proceduri şi echipamente specifice destinate funcțiilor de planificare, conducere operațională, control şi coordonare a acțiunilor aeriene militare.

Pentru a asigura unitatea acțiunilor forțelor specializate în ducerea acțiunilor militare în spațiul aerian, SCCAN trebuie să permită şi integrarea elementelor de supraveghere aeriană şi mijloacelor de apărare aeriană ale Forțelor Terestre şi Forțelor Navale.

La baza dezvoltării SCCAN au stat următoarele cerințe operaționale principalele:

- capacitatea de reacție în timp real pentru respingerea unei agresiuni aeriene;
- răspunsul pentru nevoile operaționale ofensive şi de sprijin;
- interoperabilitatea cu alte sisteme de conducere;
- prelucrarea unor cantități mari de informații cu caracter dinamic;
- distribuția electronică şi simultană a datelor;
- asistarea computerizată în procesul elaborării deciziilor.

SCCAN îndeplineşte următoarele funcții:

- *supravegherea şi recunoaşterea* (Surveillance and Recognize – S&R), care va asigura capabilitatea de a produce şi de a distribui imaginea aeriană unică recunoscută utilizatorilor, managementul senzorilor,

procesarea şi afişarea datelor senzorilor, schimbul de date cu alte sisteme din înzestrarea altor categorii de forţe ale armatei;

- *managementul spaţiului aerian* prin capabilitatea de planificare şi control al spaţiului aerian;

- *controlul traficului aerian*, prin care să se asigure servicii de informare aeronautică, de dirijare de apropiere şi îndepărtare faţă de aerodrom, servicii în situaţii de urgenţă şi de alertare, căutare şi salvare. Să includă capabilitatea de coordonare şi control a zborurilor militare şi civile;

- *managementul forţelor aeriene* prin capabilitatea de a planifica, repartiza misiuni şi a coordona forţe şi resurse la nivel operativ şi tactic;

- *controlul misiunilor aeriene* ofensive, defensive şi de sprijin, la nivel tactic;

- *managementul resurselor de comandă şi control (C2),* să asigure capabilitatea de planificare, utilizare, dislocare şi control al resurselor de comandă şi control aerian.

Sistemul de Comandă şi Control Aerian Naţional – SCCAN – are în structură următoarele elemente:

- *Centrul de Operaţii Aeriene (COA)* care este colocat cu *Centrul de Raportare şi Control de Bază (CRCBz),* aflat sub comanda NATO, destinat pentru supravegherea spaţiului aerian, realizarea imaginii aeriene recunoscute şi comanda armelor;

- *Centrul de Raportare şi Control de Rezervă*, destinat să preia în timp real, funcţiile de supraveghere aeriană şi control arme şi în timp scurt, toate funcţiile CRCBz;

- *centrele de operaţii ale bazelor aeriene;*

- *centrul de operaţii al rachetelor sol-aer şi punctele de comandă ale batalioanelor de rachete sol-aer* care asigură execuţia descentralizată pentru combaterea ţintelor aeriene, cu rachetele sol-aer;

- *centrul de operaţii pentru război electronic* care asigură execuţia descentralizată pentru protecţia electronică.

Supravegherea spaţiului aerian se realizează în regim automatizat, prin procesarea datelor furnizate de radarele digitale aparţinând Forţelor Aeriene. Schema de conectare a acestor radare va fi directă la Posturile de Fuziune Senzori PFS/CRC şi PFS independente. Imaginea aeriană recunoscută (RAP – Recognaise Air Picture) se materializează în afişarea integrată a situaţiei aeriene din spaţiul de interes şi este produsă în CRC.

Cerinţele operaţionale privind supravegherea aeriană, definite pentru Sistemul de Asigurare a Suveranităţii Aeriene – ASOC iniţial (Air Soveregnity Operatons Center) rămân valabile şi pentru sistemul SCCAN. Acestea se completează cu următoarele cerinţe operaţionale:

- imaginea aeriană recunoscută (RAP) este realizată independent la CRC Bz. şi CRC Rz.şi se realizează pe baza următoarelor surse de date:
- radare digitale militare şi civile, cuplate direct la CRC Bz. şi CRC Rz.;
- sisteme de recunoaştere amic-inamic-IFF (Identification Friend or Foe), modulele NATO şi modulul naţional securizat;
- planuri de zbor;
- alte surse, incluzând şi informaţiile de la radarele analogice digitizate sau introduse de operator;
- radarele tridimensionale de mare înălţime (FPS-117) şi radarele tridimensionale de joasă şi medie înălţime (GAP FILLER) conectate direct la PFS/CRC Bz. şi la PFS/CRC Rz.;
- imaginea aeriană recunoscută (RAP) se formează din surse de date plot, furnizate, în principal, de către radarele de tip FPS-117 şi de alte tipuri de radare (GAP FILLER etc.) cu ieşire în format digital;
- caracteristica multitracking a sistemului de formare a imaginii aeriene recunoscute permite urmărirea ploturilor/traiectelor şi eliminarea ploturilor/traiectelor paralele;
- capacitatea minimă a PFS: 48 de surse plot/traiect;
- asigurarea integrării datelor de la aeronavele de avertizare timpurie;
- asigurarea recepţionării, identificării ploturilor/traiectelor la nivelul PFS/CRC Bz. şi PFS/CRC Rz.;

SCCAN permite distribuţia imaginii aeriene recunoscute (RAP), produsă la nivelul PFS/CRC Bz. şi PFS/CRCRz. Distribuţia RAP se face integral sau filtrat către alţi utilizatori şi componente ale SCCAN.

SCCAN asigură comanda şi controlul operaţional al spaţiului aerian naţional şi al acţiunilor care se desfăşoară în acest perimetru, cu excepţia controlului traficului aerian civil. Sistemul sprijină operaţiile în timp de război, de criza, precum şi în timp de pace. Acest sistem vine, de asemenea, în sprijinul activităţilor desfăşurate de personalul care se ocupă de operaţiile aeriene în vederea controlului în timp real al misiunilor de apărare aeriană, începând cu stabilirea obiectivelor pentru operaţiile aeriene până la

controlul în timp real al misiunilor executate şi evaluarea rezultatelor misiunilor.

Structura sistemului SCCAN include un CRC Bz., localizat în Centrul pentru Operaţii Aeriene Baloteşti (AOC – Air Operation Centre), aflat sub comanda NATO şi un CRC Rz., aflat sub comanda naţională, localizat în incinta Centrului 71 Operaţii Aeriene Câmpia Turzii. În condiţii normale de pace, CRC Bz. produce Imaginea aeriană recunoscută (RAP). Imaginea RAP este, de asemenea, distribuită Centrului NATO pentru Operaţii Aeriene Combinate – CAOC 7 Larissa (Combined Air Operations Centre), către cele două CRC învecinate (Ungaria şi Bulgaria) prin Link 1 şi către toate componentele din cadrul sistemului de comandă control (baze aeriene, centru de bruiaj, punctul de comandă al brigăzii de rachete, şi către punctele de comanda ale batalioanelor de rachete sol-aer). Prin intermediul CRC Bz. se asigură, de asemenea, o interfaţă Link 11 cu o aeronavă de avertizare timpurie AWACS (Airborne Warning and Control System) NAEW&FC(NATO Airborne EarlyWarning) în scopul îmbunătăţirii capacităţii de descoperire şi de înştiinţare asupra acţiunilor aeriene, în special, la înălţimi mici şi foarte mici. O imagine aeriană filtrată (FAP – Filtered Air Picture) este apoi distribuită nodurilor naţionale româneşti prin intermediul reţelei de extindere largă (WAN – Wide Area Network) pusă la dispoziţie de România. Imaginea FAP constă din imaginea RAP generată de CRC Bz., filtrată în funcţie de conţinut şi arie geografică.

Imaginea RAP include date din următoarele surse:

- radarele FPS-117;
- radarele tip „GAP FILLER;
- radiolocatoarele de distanţă mică pentru dirijare la aterizare;
- radarele de supraveghere aeriană ale aviaţiei civile;
- datele civile şi militare privind planurile de zbor obţinute prin sistemul FDEx;
- datele de la două ASOC vecine, cu statut NATO, transferate prin Link 1;
- datele de la o aeronava AEW NATO transferate prin Link 11.

Nodurile naţionale care au capacitatea de a recepţiona imaginea FAP prin WAN includ următoarele:

- centrele de operaţii ale bazelor aeriene – COBA (WOC – Wing Operations Centre);
- centrul de operaţii al rachetelor sol-aer CORSA (SAM – Surface to Air Missile);
- unităţile combatante SAM (SAMFU – Surface to Air Missile Fight Unit);
- centrul de operaţii de război electronic – CORE (EWOC – Electronic Warfare Operations Centre).

În cazul în care CRC Bz. nu mai este disponibil, CRC Rz. va genera imaginea aeriană locală (LAP) pentru toate nodurile româneşti conectate la WAN. În condiţii normale pe timp de pace, CRC Rz. va funcţiona ca facilitate de rezervă şi de instruire, gata să intre în funcţiune pentru generarea LAP. Transferul conducerii acţiunilor aeriene de la CRC Bz la CRC Rz se va face manual.

Achiziţia sistemului SCCAN a necesitat o abordare integrată, simultan pe toate subsistemele componente: informatic, comunicaţii, infrastructură şi securitate.

1. Subsistemul de comunicaţii şi informatic este parte componentă a sistemului integrat de comandă şi control, procesează şi afişează date, asigură suportul care furnizează conexiuni între centrele C2, precum şi între acestea şi punctele de execuţie. Software-ul este liantul care uneşte toate resursele şi datele într-un sistem unic integrat.

Serviciile oferite de subsistemul de comunicaţii şi informatic (CIS – Communications and Information System) sunt servicii de reţea (RTP/RMNC) şi utilizator, clasificate, la rândul lor în: operaţional, administrativ, informaţional.

Fluxul informaţional este asigurat instantaneu atât pe verticală - în structura ierarhică de comandă şi control, cât şi pe orizontală – în cadrul relaţiilor de cooperare – în întreaga structură organizatorică a Forţelor Aeriene. Toate nivelurile ierarhice de comandă sunt capabile să-şi extragă imediat toate informaţiile de care au nevoie.

Sistemul de comunicaţii şi informatic (CIS) pentru Sistemul de Comandă şi Control Naţional (SCCAN) este structurat, astfel:

A. Reţeaua de comunicaţii şi informatică COM- SCCAN.

B. Servicii de procesare date (aplicaţii informatice).

C. Servicii de voce VCSS (Voice Communication Switching).

COM-SCCAN împreună cu VCSS-SCCAN şi sistemele informatice de comandă şi control (CCIS-SCCAN) se constituie în sistemul integrat de comunicaţii şi informatică (CIS-SCCAN) pentru comanda şi controlul forţelor aeriene.

Infrastructura de comunicaţii şi informatică a avut la bază:

a) realizarea proiectului tehnic de sistem;

b) realizarea, pe baza proiectului tehnic de sistem avizat de beneficiar, a lucrărilor de instalare, testare, punere în funcţiune şi mentenanţă;

c) şcolarizarea personalului tehnic SMFA pentru exploatarea şi întreţinerea echipamentelor.

Pentru reţeaua de comunicaţii şi informatică specifică /COM-SCCAN/ sunt impuse câteva cerinţe specifice:

- fiabilitate, viabilitate şi operativitate;
- legături şi comunicări facile între sursele şi utilizatorii de informaţii;
- utilizare în paralel şi simultan a două medii de transmisiuni diferite;
- redundanţă la nivel de echipamente în nodurile esenţiale;
- politici de alocare şi/sau reconfigurarea rapidă a resurselor;
- mentenabilitate ridicată;
- compatibilitate cu sistemele de telecomunicaţii NATO;
- management integrat al reţelei.

Tehnologiile de comunicaţii folosite pentru implementarea COM-SCCAN sunt:

- TDM (Time Division Multiplex);
- TDMoIP (Time Division Multiplex over IP);
- VoIP (Voice over IP);
- ISDN (Integrated Services Digital Network);
- ATM (Asynchronous Transfer Mode).

Subsistemul de comunicaţii radio sol-aer VHF/UHF.

Sistemul de acces reţea este organizat modular, asigurând următoarele 3 funcţiunide bază:

1. Interfeţe între nivelele serviciilor de utilizator, de reţea şi de transport;
2. Servicii de reţea;
3. Managementul interfeţelor şi al serviciilor de reţea.

Reţelele radio HF organizate cu staţii HARRIS sunt destinate pentru iniţierea si dezvoltarea unei reţele de comandă pentru nevoile operaţionale, utilizată ca backup a reţelei RTP/RMNC.

Subreţeaua tactică de comunicaţii de arie largă din cadrul RMNC pentru legături operative ale SCCAN trebuie să aibă topologia de reţea, iar tehnologia care stă la baza comunicaţiei între noduri este omogenă. Fiecare nod constituie un subsistem al RTP/ RMNC, astfel: BALOTEŞTI, OTOPENI, FETEŞTI, BOBOC, BACĂU, CÂMPIA TURZII şi CHITILA. Accesul conexiunilor terminale de tipul locaţii-senzor FPS, locaţii-senzor GAP-FILLER, locaţii-RSA şi locaţii radio – Poliţie Aeriană, se face prin intermediul nodurilor de acces.

Suportul tehnic de comunicaţii şi informatică a asigurat realizarea funcţiilor SCCAN prin următoarele aplicaţii definite:

- *aplicaţii de generare date radar, prelucrare, producere şi distribuţie a imaginii aeriene recunoscute* – RAP, inclusiv realizarea compatibilităţii cu sistemul NATO - NAEW(Airborne Early Warning);
- *aplicaţii ce asigură comunicaţii vocale pentru conducerea aviaţiei;*
- *aplicaţii ce asigură managementul echipamentelor;*
- *aplicaţii ce asigură planificarea zborurilor civil-militare;*
- *aplicaţii de comandă şi control SAM.*

2. Subsistemul Infrastructură şi securitate are următoarele elemente de bază:

- MAOC-ASOC (Main Air Operation Centre) cu nivel de clasificare NATO CONFIDENTIAL;
- Remote ODC, cu nivel de clasificare NATO CONFIDENTIAL NAOC-ASOC (National Operation Centre) cu nivel de clasificare NATO CONFIDENTIAL;
- SAMFU-IU, fără nivel de clasificare încă (va fi acreditat la nivel NATO CONFIDENTIAL);

- Radarele 3D, 2D, cu nivel de clasificare SECRET DE SERVICIU;
- FDEx. (Flight Data Exchange), cu nivel de clasificare SECRET DE SERVICIU – nu face parte din SCCAN.

În configuraţia sa finală, SCCAN trebuie să asigure:

- integrarea datelor furnizate de radarele digitale, militare şi civile şi a datelor provenite de la alţi senzori, la nivel local, naţional şi colectiv (al Alianţei);
- producerea imaginii aeriene recunoscute la nivel naţional (Recognized Air Picture – RAP), precum şi distribuirea sa, în mod diferenţiat şi filtrat, a utilizatorilor autorizaţi;
- comanda şi controlul la distanţă a radarelor digitale;
- evaluarea ameninţărilor în spaţiul aerian, stabilirea şi transmiterea de niveluri de avertizare şi alarmare;
-controlul tactic al misiunilor defensive, ofensive şi de sprijin;
- comanda centralizată şi execuţia descentralizată, în funcţie de complexitatea operaţiei aeriene, dar şi de descentralizarea conducerii, în anumite situaţii.

Putem aprecia că SCCAN constă în extensia programelor actuale şi implementarea sistemului NATO pentru planificarea şi conducerea operaţiilor aeriene ICC (***I****ntegrated* ***C****ommand and* ***C****ontrol*) şi a sistemului automat de informaţii meteo NAMIS (***N****ATO* ***A****utometed* ***M****eteorological* ***I****nformation* ***S****ystem*) şi trebuie să asigure informatizarea/automatizarea conducerii acţiunilor aeriene militare prin integrarea facilităţilor de comandă, control, comunicaţii, computere, informaţii şi interoperabilitate, supraveghere şi recunoaştere. De asemenea, trebuie să asigure schimbul de date şi informaţii, rapid şi securizat, să fie interoperabil cu sistemul actual NATINADS şi cu viitorul sistem de comandă şi control ACCS (***A****ir* ***C****ommand and* ***C****ontrol* ***S****ystem*) dezvoltat în prezent de NATO, să fie suficient de adaptabil şi deschis pentru a sprijini concepte operaţionale evolutive, în funcţie de transformarea structurilor militare în Alianţă şi în Armata României sau de schimbările mediului de operare.

SCCAN, prin utilizarea software-ului NATO ICC, va coordona utilizarea spaţiului aerian cu aviaţia civilă şi crearea zonelor aeriene cu regim special necesare pentru suportul acţiunilor defensive şi ofensive, precum şi pentru coordonarea folosirii spaţiului aerian cu alte acţiuni

militare (apărarea aeriană din organica Forţelor Terestre şi tragerile de artilerie din poligon).

5. Sistemul Integrat de Comandă şi Control Aerian al Alianţei Nord-Atlantice – ACCS (*Air Command and Control System*)

La începutul anilor ’90, Sistemul NATO Integrat de Apărare Aeriană-NATINADS era caracterizat de o mare diversitate a platformelor tehnice utilizate în centrele de comandă şi control. Sistemele dezvoltate sau achiziţionate de fiecare stat membru NATO, prin fonduri proprii, se găseau la nivele tehnologice diferite, cu capabilităţi diferite şi nu asigurau atât de necesara interoperabilitate la nivelul Alianţei.

În această situaţie, s-a decis realizarea unui sistem unic, integrat, care să opereze pe o platformă hardware şi software unică şi care să fie dezvoltat ulterior pe baza unei concepţii unitare.

Astfel, a luat fiinţă unul dintre proiectele majore şi prioritare ale Alianţei, Programul ACCS – Sistemul Integrat de Comandă şi Control Aerian (Air Command and Control System).

Sub aspect operaţional, ACCS va asigura integrarea elementelor statice şi dislocabile de comandă control ale statelor NATO europene, combinând funcţiile de planificare şi executare a operaţiilor aeriene ofensive şi defensive. Totodată, ACCS reprezintă un element cheie pentru implementarea noilor generaţii de echipamente de comandă şi control şi comunicaţii ale NATO, precum şi pentru includerea capabilităţilor de apărare împotriva rachetelor balistice.

ACCS va schimba date cu capabilităţile de apărare aeriană, sistemele de control trafic aerian, aeronavele pilotate sau cele fără pilot, navele marinei militare, sistemele din spaţiu şi alte sisteme. Misiunile de bază acoperite de sistem sunt cele de control trafic aerian, supraveghere aeriană, controlul misiunilor aeriene, managementul spaţiului aerian, managementul forţei şi managementul resurselor C2. Este în studiu echiparea unor centre de comandă control în variantă mobilă, care vor avea aceleaşi capacităţi cu cele fixe.

Sistemul ACCS este proiectat pentru a rezolva automat următoarele funcţii ale comenzii şi controlului aerian:

- *conducerea forţelor (Force Management – FM)* - activitatea de planificare, execuţie şi conducere a acţiunilor aeronavelor cu sau fără pilot şi a armelor sol-aer;

- *controlul misiunilor aeriene (Air Mission Control – AMC)* – monitorizarea misiunilor în desfăşurare, dirijarea avioanelor de vânătoare şi repartiţia ţintelor aeriene unităţilor subordonate;

- *managementul spaţiului aerian (Airspace Management – ASM)* – dezvoltarea şi menţinerea structurii spaţiului aerian. Pe timp de război, importanţa managementului spaţiului aerian creşte, pentru utilizarea la maxim a spaţiului, concomitent cu reducerea la maxim a riscului de fratricid;

- *controlul traficului aerian (Air Traffic Control – ATC)* – coordonarea cu controlul misiunilor, zona de control radar, serviciu de refacere-plecare, coordonarea traficului civil/militar; alarmarea serviciului Căutare şi salvare (***SAR*** *– Search and Rescue).*

- *supravegherea (Surveillance – S)* – managementul, producerea şi distribuţia imaginii aeriene recunoscute (*Recognised Air Picture – RAP*); recepţionarea şi distribuţia traiectelor de la forţele terestre, navale şi submarine;

- *managementul resurselor de comandă şi control (C2 Resource Management – C2RM)* – managementul senzorilor, modulelor ACCS şi comunicaţiilor operaţiilor aeriene şi include alocarea, desfăşurarea, configurarea, execuţia şi monitorizarea.

În aprilie 2004, la momentul aderării la NATO, România a găsit programul ACCS în plină derulare. Cerinţele operaţionale şi arhitectura sistemului fuseseră deja definite şi se aflau în faza avizării şi aprobării de către forurile Alianţei.

România a întreprins numeroase demersuri la diferite niveluri de reprezentare pentru a fi inclusă în lista de replicare, iar recentele hotărâri ale Comitetului Director, care coordonează programul ACCS, crează premizele reconsiderării actualei configuraţii a sistemului. Rămâne ca aceste eforturi să fie continuate printr-o adevărată ofensivă politico-militară în cadrul Alianţei, la toate nivelurile de reprezentare, pentru ca România să fie inclusă cu o entitate de tip

ARS (*ACC – RPC – SFP: Area Control Centre-Rap Production Center-Sensor Fusion Post)* în programul realizării ACCS.

6. Realizarea compatibiltății şi interoperabilității dintre SCCAN şi ACCS

Analiza Forțelor Aeriene în perspectiva anului 2015 trebuie să ia în considerare contextul în care la acea dată, ambele sisteme, cel național şi cel NATO, vor fi operaționale în România.

Ca țară membră NATO şi ca parte integrantă a NATINADS, România trebuie să răspundă cerințelor de apărare colectivă a spațiului aerian al Alianței. Aceasta este o cerință implicită, asumată odată cu accederea în NATO şi va rămâne o obligație pentru țara noastră, indiferent dacă va fi sau nu va fi inclusă pe lista țărilor cu entități ACCS. În acelaşi timp, poziția geostrategică a României, la limita estică a Alianței, potențialul operațional oferit şi investițiile însemnate făcute până în prezent pentru modernizări şi achiziții de noi senzori şi de echipamente de comandă şi control, îndreptățesc solicitarea țării noastre de a figura în arhitectura ACCS cu un element de tip ARS. Odată demonstrată importanța celor două sisteme pentru România, trebuie considerate cerințele operării lor simultane, respectiv:

- *complementaritatea*, prin evitarea suprapunerilor şi a consumului inutil de resurse;

- *compatibilitatea,* prin asigurarea interoperabilității şi a capacității de „comunicare" între cele două sisteme.

Prima cerință a fost îndeplinită încă din faza proiectării arhitecturii SCCAN, care a ținut cont de configurația ACCS şi de funcțiunile pe care acesta le va îndeplini.

Cea de-a doua cerință, a interoperabilității, trebuie evaluată prin prisma compatibilităților tehnice, de pregătire şi procedurale.

Compatibilitatea tehnică este asigurată prin respectarea următoarelor cerințe:

- dezvoltarea SCCAN în conformitate cu standardele specifice NATO, care stau şi la baza dezvoltării ACCS;

- asigurarea, prin echipamente ICC, furnizate de agenția NATO specializată, a funcției de planificare a operațiilor aeriene în SCCAN;

- conectarea senzorilor naţionali direct atât la CRC bază şi ulterior la ARS, pentru susţinerea cerinţelor NATO, cât şi la CRC rezervă, numai pentru cerinţele naţionale.

Astfel, România, prin funcţiunile oferite de finalizarea SCCAN, va avea operaţional un sistem care va respecta toate cerinţele minimale ale ACCS.

Compatibilitatea în pregătire va fi asigurată prin adoptarea unui sistem de instruire a personalului şi a unor standarde de evaluare similare cu cele din cadrul Alianţei.

Compatibilitatea procedurală va fi asigurată prin implementarea procedurilor standard NATO şi prin armonizarea reglementărilor naţionale cu cele operează în cadrul Alianţei.

7. Implicaţiile implementării SCCAN asupra procesului de transformare şi modernizare a sistemului de securitate aeriană al României

În eforturile de consolidare a capacităţilor de răspuns la noile ameninţări, România, ca stat membru NATO, aliat al SUA, dar şi de membru al UE, va trebui să realizeze o reconfigurare a forţelor sale aeriene care să-i permită să îndeplinească noi tipuri de operaţii desfăşurate la distanţă, la pace, criză şi război, să facă faţă cu succes provocărilor viitoare din mediul regional şi global.

Concepţia privind apărarea aeriană integrată a României prezintă soluţii de eficientizare a efortului de apărare aeriană a României, printr-o abordare conceptuală nouă şi unitară, care vizează măsuri organizatorice şi structurale pentru realizarea unor entităţi modulare şi complementare de forţe specializate pentru acţiuni în spaţiul aerian, din compunerea tuturor categoriilor de forţe ale armatei, care să fie integrate acţional în Sistemul de Comandă Control Aerian Naţional (SCCAN).

Apreciem că Sistemul de Comandă Control Aerian Naţional (SCCAN) trebuie să includă subsisteme de supraveghere aeriană, de identificare şi control aerian, la care să fie racordate toate sistemele de arme, indiferent cui aparţin, pentru a beneficia de date reale, oportune şi identificate, privitor la dinamica situaţiei aeriene. Un asemenea Sistem de Comandă Control Aerian Naţional permite instituirea şi respectarea cu strictețe a regulilor de angajare a sistemelor de arme, fapt ce elimină fratricidul.

Considerăm că în dinamica securităţii colective la nivel NATO, *Concepţia privind apărarea aeriană integrată a României* prezintă soluţii, oportunităţi, responsabilităţi şi acţiuni de integrare a apărării aeriene a României în Sistemul Integrat de Apărare Aeriană NATO (NATINADS) care, în noul context geostrategic, are o dimensiune extinsă şi definită conceptual, organizatoric şi acţional.

Pornind de la cele două dimensiuni de integrare a apărării aeriene a României, se defineşte, pe de o parte, necesitatea şi preocupările de eficientizare a folosirii forţelor prin acţiuni oportune şi coordonate la nivel naţional, iar pe de altă parte, oferă posibilitatea soluţionării problematicii de integrare a apărării aeriene a României în sistemul NATINADS.

Având în vedere problematica securităţii aeriene, ca parte a securităţii naţionale, evoluţia previzionată a mediului regional şi global de securitate, rolul din ce în ce mai puternic al forţelor aeriene în câmpul de luptă modern, precum şi procesul de transformare şi modernizare a Armatei României şi al Forţelor Aeriene se impune o continuă perfecţionare a sistemului de securitate aeriană SCCAN, reevaluare a obiectivelor, strategiilor, concepţiilor, planurilor şi programelor pentru a le adapta la noile condiţii de la început de secol XXI.

PERSPECTIVE PRIVIND REALIZAREA SISTEMULUI DE COMANDĂ ŞI CONTROL ÎN FORŢELE NAVALE

Comandor Tiberiu CHODAN

1. EVOLUŢIA ACTUALĂ A MEDIULUI DE SECURITATE REGIONAL ŞI MONDIAL

Problematica securităţii maritime este foarte complexă. Aceasta a fost subiectul care a dominat dezbaterile forumurilor liderilor navali din NATO şi Europa, în ultima perioadă. Cheia soluţionării riscurilor, ameninţărilor şi provocărilor din domeniul securităţii maritime o reprezintă cooperarea, interoperabilitatea, schimbul de informaţii şi acţiunea preventivă. Conducerea forţelor în condiţiile evoluţiei mediului de securitate impune existenţa unui sistem de comandă şi control, în concordanţă cu transformarea noilor structuri de forţe.

"Misiunea dedusă" de modernizare a sistemului de comandă control ca orice misiune trebuie să aibă, de regulă, un singur scop din care rezultă sarcinile şi obiectivele. Transformarea Forţelor Navale, odată cu cea a întregului organism militar, impune, în mod logic, asumarea acestei noi "misiuni implicite" – modernizarea sistemului de comandă control, care are în vedere, ca prioritate importantă, realizarea cerinţelor de interoperabilitate.

2. DELIMITĂRI CONCEPTUALE

Conducerea Forţelor Navale presupune atât exercitarea actului de comandă, cât şi a controlului. Din punct de vedere teoretic, scolastic, aceasta se exercită în două domenii şi la trei nivele. **COMANDA** reprezintă autoritatea investită pentru **direcţionarea şi coordonarea** unei structuri militare. Obiectivul comenzii este de a obţine eficienţă operaţională şi/sau administrativă maximă.

Direcţionarea reprezintă procesul de planificare a luării deciziilor, de stabilire a priorităţilor, de formulare a instrucţiunilor şi de impunere a deciziilor.

Coordonarea reprezintă stabilirea în timpul operaţiilor, conform evoluţiei situaţiei, a unei coordonări în spaţiu timp şi pe misiuni a acţiunilor planificate pentru a obţine cel mai bun rezultat; în mediul naval, termenul coordonare poate include anumite funcţii de control.

CONTROLUL reprezintă autoritatea exercitată asupra unei părţi dintre activităţile structurilor subordonate, sau asupra altor structuri aflate temporar în subordine, ceea ce presupune responsabilitate în executarea ordinelor sau directivelor. Toată autoritatea comandantului sau numai o parte din aceasta poate fi transferată sau delegată.

Comanda deplină reprezintă autoritatea şi responsabilitatea militară a unui comandant şi constă în darea ordinelor subordonaţilor. Termenul „comandă”, aşa cum este folosit în cadrul NATO, implică un grad mai scăzut de autoritate decât în situaţia în care se foloseşte numai în sens naţional. Nici un comandant NATO sau al unei coaliţii nu dispune de o comandă deplină asupra forţelor destinate acestuia, deoarece statele care destină forţe pentru NATO vor delega numai controlul şi comanda operaţională. Acest termen acoperă toate aspectele acţiunilor (operaţiilor) şi administraţiei militare şi se aplică numai în cadrul naţional.

3. SISTEMUL DE COMANDĂ ŞI CONTROL

Exercitarea comenzii presupune existenţa unei **structuri ierarhice** şi a unui **sistem de comandă şi control**.

Orice sistem de comandă şi control este structurat ierarhic şi include mijloacele necesare distribuirii ordinelor, compilării şi diseminării informaţiilor. În cazul Forţelor Navale, ierarhizarea exercitării comenzii este structurată, doar din punct de vedere teoretic pe două nivele distincte –

operativ şi administrativ. În fapt, acestea se întrepătrund în funcţie de scopul şi de importanţa misiunii de îndeplinit, compunerea şi dispunerea forţelor destinate îndeplinirii acesteia, raionul, zona sau teatrul de acţiune.

Structura special creată şi desemnată în Forţele Navale pentru exercitarea conducerii operaţionale, pe timp de pace în situaţie de criză şi la război atât la nivel tactic, cât şi operativ este Comandamentul Operaţional Naval.

În mod normal, în cadrul unor forţe mari sau când acestea sunt dispersate, acolo unde este necesară descentralizarea procesului de luare a deciziilor, anumite funcţii de direcţionare, coordonare şi control pot fi delegate subordonaţilor. Cu toate acestea o comandă centralizată este cea mai directă cale prin care un comandant face uz de experienţa şi de capacitatea sa.

În cadrul Sistemului Naţional de Apărare, Statul Major al Forţelor Navale este direct subordonat Statului Major General şi asigură conducerea tuturor structurilor Forţelor Navale.

Forţele Navale duc acţiuni militare independent, întrunit cu celelalte categorii de forţe ale armatei, sau în compunerea unor grupări multinaţionale.

În acest lanţ de comandă, Forţele Navale acţionează pentru apărarea şi promovarea intereselor şi drepturilor suverane ale României, la mare şi pe fluviu, independent sau în cooperare cu alte forţe, în cadrul creat de aderarea la NATO, UE sau organizaţii regionale.

De asemenea, Forţele Navale contribuie activ la realizarea măsurilor de securitate maritimă regională îndeosebi pe timp de pace, prin participarea la iniţiative regionale şi la operaţii maritime de securitate, ocupând în acest domeniu un loc central, alături de Poliţia de Frontieră şi Autoritatea Navală Română.

Exercitarea comenzii pe cele două domenii, operaţional, respectiv administrativ, apare mai evidentă în situaţii de criză şi război, deoarece complexitatea problemelor de rezolvat impune partajarea responsabilităţilor unor structuri specializate. Continuitatea actului de comandă se realizează prin măsurile stabilite pentru trecerea de la situaţia de pace la cea de criză sau război, care prevăd completarea statelor de organizare şi alte măsuri graduale destinate realizării funcţionalităţii structurilor pentru a fi capabile să îndeplinească misiunile primite.

În exercitarea comenzii operaţionale a acţiunilor militare, îndeplinirea cu succes a oricărei misiuni impune parcurgerea a şapte paşi: analiza situaţiei, însuşirea misiunii, stabilirea cursului acţiunii, elaborarea planului de acţiune, transmiterea ordinului de acţiune, desfăşurarea acţiunii şi analiza post acţiune.

Comanda operaţională/OPCOM reprezintă autoritatea conferită unui comandant de a atribui misiuni sau sarcini comandanţilor din subordine, de a angaja unităţi, de a schimba destinaţia unor forţe şi de a păstra sau a delega comanda operaţională şi/sau tactică, atât cât este necesar. OPCOM nu include responsabilitatea administrativă sau logistică. De asemenea, OPCOM poate fi folosită pentru a desemna forţele unui comandant. În mod normal, OPCOM se exercită la nivel strategic.

Controlul operaţional/OPCON, care se exercită la nivelul Forţelor Navale de către CON reprezintă autoritatea delegată unui comandant: pentru a conduce forţele din subordine, astfel încât să îşi poată îndeplini misiunile sau sarcinile specifice, care sunt de regulă limitate de scop, timp şi locaţie; pentru a angaja unităţile respective; pentru a păstra sau a delega controlul tactic/TACON al acestor unităţi. OPCON nu include controlul administrativ sau logistic. Controlul operaţional este subordonat comenzii operaţionale şi are autoritate limitată. În cadrul OPCON nu se pot realoca sau redirecţiona forţe.

4. SISTEMUL INTEGRAT DE COMUNICAŢII ŞI INFORMATICĂ

În cazul particular al Forţelor Navale acţiunea în spaţiul complex al Mării Negre, precum şi în afara acestuia, conferă particularităţi şi importanţă crescută informaţiei şi infrastructurii de transport şi prelucrare a acesteia. În acest sens este necesară asigurarea Forţelor Navale cu un sistem integrat de comunicaţii şi informatică şi cu suportul logistic aferent, care să asigure managementul şi procesarea informaţiei în scopul transferului oportun al acesteia, nealterată şi nedeconspirată, de la furnizori la utilizatori, respectiv între corespondenţi.

Sistemul Integrat de Comunicaţii şi Informatică al Forţelor Navale va asigura atât fluidizarea informaţiei, cât şi participarea la acţiuni comune în cadrul Alianţei prin existenţa unor mijloace de comunicaţii radio şi informatice securizate, moderne.

Realizarea sistemului integrat de comunicaţii şi informatică pentru Forţele Navale este cuprins în programul de înzestrare şi a fost reorganizat în două subprograme "NAVCIS etapa I" şi "Achiziţii în sprijinul NAVCIS".

Sistemul de Comunicaţii şi Informatică al Statului Major al Forţelor Navale este un sistem ierarhic complex, compus din subsisteme de comunicaţii radio, TI, radioreleu, precum şi din infrastructura corespunzătoare centrelor de comandă şi control, interconectate flexibil prin linii de comunicaţii prestabilite sau, în funcţie de nevoi, stabilite temporar, sprijinit de elemente administrative şi proceduri organizatorice specifice.

Pentru susţinerea activităţii de management a informaţiei s-a prevăzut asigurarea infrastructurii de comunicaţii corespunzătoare, necesare acoperirii fluxurilor de informaţii din Forţele Navale, care este alcătuită din două **componente**:

● **Componenta terestră** asigură:

- monitorizarea şi exploatarea spaţiului aerian în folosul forţelor proprii (protecţia acestora), monitorizarea spaţiului maritim (cu componentele de suprafaţă şi submarină), fluvial şi terestru (îndeosebi în Delta Dunării), în vederea îndeplinirii misiunilor principale de combatere a ameninţărilor în aceste medii;
- necesarul de transfer informaţii al CON şi SCOMAR, cu structuri externe acestora;
- legăturile de grup, la dislocarea în teren a subunităţilor (companii/plutoane infanterie marină sau grupe de transport logistice);
- legăturile individului/grupei (staţie radio individuală UUS – handheld);
- acoperirea radio în gama UHF a teritoriului Dobrogei, prin retranslatarea legăturilor radio conform unei matricie de redistribuire radio predefinită.

● **Componenta navală** asigură capabilităţile de comunicaţii externe vocale, imagine şi date, prin canale radio, cu ajutorul modem-urilor radio, dispozitivelor de securizare a vocii, precum şi a dispozitivelor de criptare a datelor, între nave, navă – litoral, în vederea dezvoltării interoperabilităţii şi capacităţii de a acţiona în cadrul grupului/grupării de nave proprii (cu dotare similară) sau NATO.

5. INTEGRAREA SISTEMULUI DE COMANDĂ ŞI CONTROL

Conducerea Forţelor Navale presupune o serie de cerinţe specifice sistemului de comandă control, date de specificitatea realizării legăturilor cu fiecare tip de nave, aeronave sau cu submarinul, a procedurilor diferite utilizate în funcţie de situaţii, distanţe şi misiuni ceea ce face mai dificilă acoperirea completă a necesităţilor de conducere.

Centrul de comandă şi control comun CON/SCOMAR de nivel operativ (CCCOp) reprezintă infrastructura principală de sprijin a activităţii de conducere a Forţelor Navale. Integrează totalitatea informaţiilor recepţionate şi sintetizează rezultatele integrării în formate standard pe care le pune la dispoziţie structurilor proprii şi a celor din cadrul forţelor armate prin interconectare directă cu sistemele de comandă şi control ale acestora.

Centrul de comunicaţii şi informatică de nivel operativ (CCICOp) reprezintă infrastructura principală de transfer a informaţiilor între componentele Forţelor Navale şi beneficiarii din cadrul celorlalte categorii de forţe.

Acest centru asigură:

- acoperirea necesarul de transfer informaţii al CON şi SCOMAR, cu structuri externe acestora;
- intrarea/ieşirea în/din SCOMAR (legătura cu senzori externi şi sisteme similare);
- reţelele radio ale Forţelor Navale (cu navele proprii şi aliate);
- reţelele/legăturile speciale (HF/UHF DATA LINK; SATCOM, NGCS).

De maximă importanţă în domeniul schimbului de informaţii este realizarea unor linii de comunicaţii sigure, stabile şi securizate, care să permită un flux continuu pentru schimbul internaţional de informaţii în timp real. În consecinţă, exercitarea comenzii şi controlului este legată de cerinţa interoperabilităţii comunicaţiilor, ca o condiţie indispensabilă şi primordială.

Dotarea Forţelor Navale cu un sistem care să asigure realizarea şi utilizarea NATO – REP – Recognized Environmental Picture (Imagine recunoscută a mediului), pentru a furniza un tablou complet şi unitar al condiţiilor geospaţiale, meteorologice, oceanografice etc., pentru planificarea şi conducerea operaţiilor întrunite într-o zonă şi la un anumit

moment de timp presupune funcționarea integrată a tuturor categoriilor de senzori.

Misiunea principală a sistemului este generarea imaginii navale unice în sistemul de comandă control al unei nave, transferul acesteia în rețeaua DATA LINK, conținând sistemul similar din CCICOP, transferul acesteia în centrul de comandă şi control (CIS CCCOp), utilizarea pe console dedicate şi fuzionarea în aplicații specializate cu date furnizate de către sistemele SCOMAR, STASA sau MCCIS; transferul via DATA LINK a imaginii astfel obținute la nave sau aeronave.

Aceasta se realizează prin integrarea în CIS CCCOp a datelor provenite din toate sursele pentru obținerea unei imagini unice asupra amenințărilor posibile existente la un moment dat, imagine vehiculată între consolele CIS CCCOP în vederea planificării şi ducerii operației, respectiv distribuită conform celor arătate anterior.

6. CONCLUZIE

Funcționarea sistemului de comandă control este un element vital pentru Forțele Navale, motiv pentru care realizarea lui reprezintă o prioritate. Prin asigurarea fondurilor necesare pentru programele de înzestrare, acest sistem este fezabil şi poate fi finalizat în următorii 8-10 ani.

SISTEMELE DE COMANDĂ ŞI CONTROL – PREZENT ŞI PERSPECTIVE

Colonel prof. univ. dr. Gelu ALEXANDRESCU
Colonel (r) prof. univ. dr. Gheorghe BOARU

Introducere

Pacea mondială, mult dorită, nu a fost adusă nici de Secolul XXI şi probabil că nici nu se va instala prea curând. Poate nici nu există pace mondială sau poate pacea trebuie redefinită aşa cum şi războiul a fost redefinit. Astăzi se desfăşoară conflicte militare între coaliții de state şi un regim politic dintr-o altă țară. Declarațiile de război specifice secolului XX sunt în afara legilor internaționale, dar interesele de tot felul fac posibilă existența în permanență a unor focare de conflict. Atunci când procesul de gestionare a crizelor eşuează, conflictele militare sunt iminente. Modificările esențiale ale mediului de securitate, aderarea României la NATO şi promovarea intereselor naționale impun ca deseori forțele militare româneşti să participe la astfel de conflicte.

Conflictele militare actuale aduc modificări majore în toate planurile domeniului militar (artă militară, doctrine, organizare, pregătire, înzestrare, acțiune etc.), dar toate aceste transformări au un element comun: progresul tehnologic. În decursul istoriei noastre zbuciumate, progresul tehnologic a influențat direct toate planurile domeniului militar. O lege a luptei armate ne spune că este o strânsă concordanță între nivelul tehnologic al forțelor militare şi modul în care acestea acționează. În ultimele decenii, însă, forțele militare au influențat semnificativ, la rândul lor, progresul tehnologic prin finanțarea directă a cercetării în domeniul tehnologiilor de vârf. Această finanțare s-a făcut pe baza unor noi concepte acționale pe care forțele armate doreau să le întrebuințeze, dar care nu aveau suportul tehnic necesar.

Creşterea rolului componentei informaţionale asociată acţiunii militare în dauna componentei energetice a determinat schimbări majore în plan teoretic şi acţional. Acum, într-o acţiune militară este esenţial să controlezi informaţia din mediul de confruntare şi să deţii cel puţin superioritatea informaţională. Dorinţa militarilor de a concentra efecte şi nu forţe a impus progresul sistemelor informaţionale şi a sistemelor informatice de sprijin a deciziei şi, ulterior, transformarea acestora în sisteme integrate de comandă şi control. La rândul lor, sistemele integrate de comandă şi control au evoluat de la sisteme de comandă, control şi comunicaţii până la sisteme de comandă, control, comunicaţii, calculatoare, informaţii despre inamic şi teren, supraveghere şi recunoaştere.

Pentru a ne putea pronunţa asupra perspectivelor în dezvoltarea sistemelor de comandă şi control trebuie mai întâi să analizăm războiul informaţional şi una dintre ţintele sale – sistemul de comandă şi control. Comparând diferite concepte ale războiului informaţional sau ale operaţiilor informaţionale din analiza doctrinelor SUA, Marii Britanii şi României, precum şi elemente din doctrina NATO putem înţelege eventualele diferenţe. În acest fel se pot stabili factorii cei mai importanţi care determină sau influenţează dezvoltarea sistemelor de comandă şi control şi putem chiar să deducem perspectivele lor de dezvoltare sub impactul factorilor respectivi.

1. Sistemul de comandă şi control - ţintă a Războiului informaţional şi Operaţiilor informaţionale. Viziuni ale specialiştilor militari străini şi români

Conceptul războiului informaţional îşi are rădăcinile în faptul că informaţia şi tehnologia informaţiei devin din ce în ce mai importante în securitatea naţională şi în confruntarea militară. Ca urmare, viitoarele conflicte vor putea fi caracterizate de lupta pentru controlul şi dominarea informaţiei deoarece cei ce vor stăpâni tehnicile războiului informaţional vor avea un avantaj asupra celorlalţi. Pornind de la această bază, Marin C. Libicki a dorit să demonstreze că războiul informaţional nu poate fi considerat ca o tehnică separată de purtare a războiului clasic şi, în schimb, pot fi distinse şapte forme de război informaţional, deoarece toate acestea implică interzicerea accesului, protecţia, manipularea şi degradarea informaţiilor: războiul de comandă şi control (*command and control warfare*); războiul bazat pe informaţii militare (*intelligence based warfare*); războiul electronic (*electronic warfare*); războiul psihologic (*psychological warfare*); războiul de tip „hacker” (*„haker” warfare*); războiul informaţional economic (*economic information warfare*); războiul cibernetic (*cyberwarfare*).

Subliniind dificultatea definirii războiului informaţional, acelaşi autor a considerat că războiul informaţional ar trebui privit ca un mozaic eterogen al celor

şapte forme de manifestare, ce pot cuprinde domenii vaste ale activităţii umane (domeniul politic, economic, cultural, social etc.), mult în afara responsabilităţilor organismelor militare. Ca urmare, războiul informaţional este foarte puţin descris în publicaţiile militare oficiale. În schimb, există mai multe doctrine ale operaţiilor informaţionale, ce abordează acţiunile specific militare în domeniul nostru de interes.

În doctrina SUA, războiul informaţional este definit ca fiind „operaţiile informaţionale desfăşurate în situaţii de criză sau de conflict pentru îndeplinirea sau promovarea obiectivelor specifice ce vizează un adversar sau adversari specifici". Operaţiile informaţionale sunt definite ca fiind acţiunile executate „pentru a afecta informaţiile şi sistemele informaţionale ale adversarului, concomitent cu apărarea propriilor informaţii şi sisteme informaţionale". Ele vizează informaţii şi sisteme informaţionale pentru a afecta un proces bazat pe informaţii, indiferent dacă acesta este uman sau automat.

Specialiştii militari britanici au dezvoltat *conceptul campaniei informaţionale*, definită ca fiind emiterea coordonată de informaţii de către întreaga activitate guvernamentală în scopul influenţării decidenţilor în sensul necesar determinat de obiectivele politice, concomitent cu protejarea propriilor decidenţi. Elementul central al conceptului se bazează pe faptul că orice acţiune sau inacţiune transmite un mesaj, din care audienţa partizană, neutră şi ostilă derivă şi agregă deducţii, care, la rândul lor, determină acţiuni ale acestora.

Contribuţia Ministerului Apărării britanic la campania informaţională constă în folosirea coordonată a oricărei capacităţi militare pentru a influenţa audienţa ţintă (la orice nivel) şi pentru a o împiedica să-şi impună voinţa, folosind operaţiile informaţionale şi operaţiile media. Operaţiile informaţionale sunt definite ca fiind acţiuni coordonate executate pentru a influenţa un adversar sau potenţial adversar, în sprijinul obiectivelor politice şi militare, prin subminarea voinţei, coeziunii şi capacităţii sale de a decide ca urmare a afectării informaţiilor, sistemelor informaţionale şi proceselor sale bazate pe informaţii, concomitent cu protejarea decidenţilor şi proceselor decizionale proprii.

Începând cu anul 2006, Armata României foloseşte Doctrina operaţiilor informaţionale SMG/FOP – 3.15, potrivit căreia operaţiile informaţionale sunt acţiuni sincronizate şi coordonate, planificate şi desfăşurate în vederea obţinerii efectelor dorite asupra voinţei, puterii de înţelegere şi capacităţii/mijloacelor adversarului, potenţialului adversar sau altor entităţi aprobate de Autoritatea Naţională de Comandă, în sprijinul îndeplinirii obiectivelor comandantului, prin afectarea informaţiilor şi proceselor bazate pe informaţii ale acestora, concomitent atât cu valorificarea propriilor informaţii, cât şi cu protecţia şi întărirea propriilor sisteme bazate pe informaţii. Ele au drept scop afectarea sau influenţarea

elementelor cheie de care depinde eficienţa factorilor de decizie sau liderilor de opinie: voinţa de a acţiona; puterea de înţelegere şi percepţia lor privind situaţia respectivă; capacitatea şi/sau mijloacele de care dispun pentru a acţiona în consecinţă.

Publicaţia NATO Allied Joint Doctrine AJP-01(B) /2002 defineşte operaţiile informaţionale ca fiind acele acţiuni executate în sprijinul unor obiective politice sau militare pentru a influenţa decidenţii prin afectarea informaţiilor, proceselor bazate pe informaţii, sistemelor de comandă şi control şi a sistemelor de comunicaţii şi informatice folosite de aceştia, concomitent cu exploatarea şi protejarea propriilor informaţii şi/sau sisteme informatice.

În concluzie, conceptul războiului informaţional este folosit în mod explicit doar de armata SUA pentru a diferenţia operaţiile informaţionale desfăşurate pe timp de pace faţă de cele desfăşurate în situaţii de criză sau de conflict. Ca urmare, termenul „război" ar trebui tradus şi interpretat în sensul de „confruntare" ce are în vedere simultan atât aspectul atacului, cât şi aspectul apărării.

De asemenea, ţintele vizate de operaţiile informaţionale diferă în cele patru doctrine analizate. Dacă suntem de acord că unul dintre rolurile doctrinelor este acela de a stabili limite în care comandanţii pot folosi forţele şi mijloacele din dotare, rezultă diferenţe semnificative de abordare conceptuală a operaţiilor informaţionale.

Definiţiile date operaţiilor informaţionale sunt diferite. Această diferenţă subliniază caracterul dinamic şi vast al conceptului. De asemenea, diversitatea se datorează şi unor unghiuri diferite de abordare a problemei apărute atunci când progresul tehnologic a depăşit modalităţile clasice de ducere a războiului, specifice mileniului II.

Doar doctrina britanică abordează conexiunea dintre decizia politică şi acţiunile militare desfăşurate în sau cu impact în mediul informaţional, precum şi sincronizarea ori coordonarea elementelor de putere naţională atunci când acestea desfăşoară acţiuni în sau cu impact în mediul informaţional.

2. Sisteme de comandă şi control folosite pentru conducerea acţiunilor militare

„Comandă şi control" (C2) este termenul folosit în prezent pentru conducerea forţelor militare. Acest termen este relativ recent şi înlocuieşte termenul „comandă" sau termenul „conducere" folosite în trecut. Conceptul de „comandă" a apărut înaintea altor concepte, cum ar fi „politică" sau „management industrial", şi a evoluat separat faţă de acestea din cauza caracteristicilor diferite ale războiului în comparaţie cu alte acţiuni umane. Evoluţia conceptului de

„comandă" a fost influenţată îndeosebi de trei factori: timpul, consecinţele grave ale erorilor şi preocuparea pentru reducerea confuziei pe timpul acţiunilor militare.

Studiind publicaţiile militare străine, am găsit mai multe definiţii legate de termenul „comandă şi control". Astfel, în NATO se folosesc doi termeni strâns legaţi, folosiţi împreună, de regulă, dar care nu sunt sinonimi. Comanda este autoritatea investită într-o persoană. Ea poate fi descrisă ca fiind procesul prin care un comandant îşi impune intenţiile şi voinţa sa asupra subordonaţilor în scopul executării unei anumite acţiuni. Ea conţine autoritatea şi responsabilitatea pentru desfăşurarea şi alocarea de forţe în scopul îndeplinirii misiunilor primite de comandant. Controlul este autoritatea exercitată de un comandant. Ea poate fi descrisă ca fiind procesul prin care un comandant, asistat de către statul său major, organizează, direcţionează şi coordonează activităţile forţelor alocate.

Analizând cele două concepte descrise mai sus, putem trage mai multe concluzii. În primul rând, comanda este o „autoritate şi o responsabilitate", pe când controlul este doar o „autoritate". Termenul de autoritate trebuie înţeles ca „având dreptul...", iar cel de responsabilitate ca „purtând răspunderea ...". Rezultă că autoritatea de control poate fi delegată de către „titular" unei alte persoane sau structuri din subordine. În acelaşi timp, comanda nu poate fi delegată pentru că responsabilitatea rămâne mereu a comandantului. În al doilea rând, comanda este o „autoritate investită", pe când controlul este o „autoritate exercitată". În al treilea rând, comanda se referă la forţe (comandantul alocă forţe şi le dă misiuni), iar controlul se referă la activităţi (comandantul organizează, direcţionează şi coordonează activităţile forţelor subordonate).

Armata americană foloseşte definiţii mai nuanţate şi oarecum diferite. Astfel, comanda este definită ca fiind autoritatea pe care un comandant din forţele armate o exercită în mod legal asupra subordonaţilor în virtutea rangului sau a numirii (desemnării). Comanda include autoritatea şi responsabilitatea pentru folosirea eficace a resurselor disponibile şi pentru planificarea întrebuinţării, organizarea, direcţionarea, coordonarea şi controlul forţelor militare pentru îndeplinirea misiunii primite. De asemenea, ea include responsabilitatea pentru sănătatea, moralul şi disciplina personalului din subordine. Controlul este definit ca fiind autoritatea exercitată de un comandant asupra unei părţi dintre activităţile subordonaţilor.

Se observă o diferenţă importantă între conceptul NATO şi cel american. În opinia noastră, această diferenţă subliniază faptul că, având în vedere caracterul alianţei, un comandant „NATO" are un grad mai mic de autoritate faţă de forţele din subordine decât un comandant „naţional".

Analizând acţiunile militare desfăşurate în era industrială, putem concluziona că nu a existat un singur model conceptual de comandă şi control.

Există cel puţin şase diferite abordări conceptuale, arătate în figura 1, care odată puse în practică, au avut succes pe câmpul de luptă.

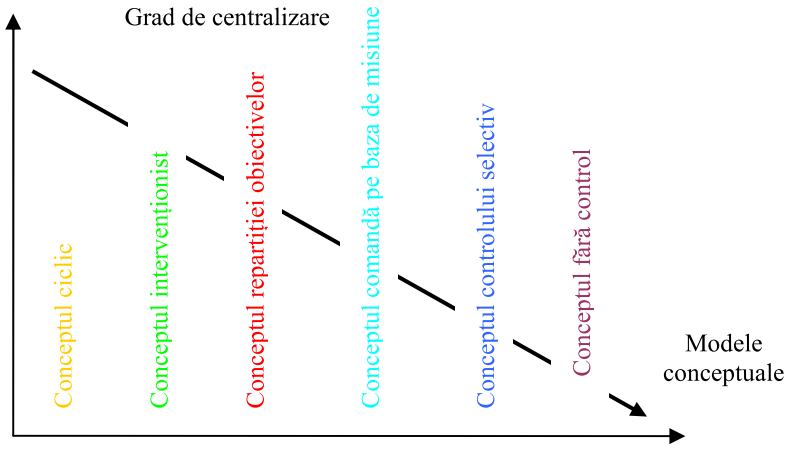


Figura 1. Gradul de centralizare al diferitelor concepte C2

Diferenţele majore dintre cele şase concepte sunt legate direct de gradul de centralizare pe care acestea îl impuneau. Aprofunzând aceste concepte, se pot deduce cei mai importanţi factori ce au influenţat evoluţia diferitelor concepte: fizionomia acţiunilor militare (acţiuni statice sau război manevrier); continuitatea comunicaţiilor între eşaloane (secvenţială sau continuă); competenţa profesională a comandanţilor şi forţelor subordonate.

Cea mai mare parte a filozofiei şi practicii în domeniul comenzii şi controlului a fost dezvoltată şi perfecţionată în era industrială. Actualele principii ale comenzii şi controlului sunt valabile nu numai în domeniul militar, ci şi în domeniul civil. Aceste principii sunt: descompunerea, specializarea, ierarhizarea, optimizarea, coordonarea, planificarea centralizată şi execuţia descentralizată. Cea mai modernă abordare a mecanismului de comandă şi control în era industrială a fost una de tip liniar. Comandanţii au descompus spaţiul de luptă, au împărţit acţiunile militare în faze, au folosit specializarea, optimizarea şi planificarea centralizată pentru a eficientiza acţiunea forţelor subordonate şi au folosit execuţia descentralizată şi alte procese ciclice pentru a se asigura că eforturilor lor sunt suficient de flexibile faţă de situaţia des schimbătoare a confruntărilor armate.

Dacă în ceea ce priveşte termenii de comandă şi de control nu sunt diferenţe mari, definirea şi utilizarea termenului „sistem de comandă şi control” este diferită. În doctrina NATO Allied Joint Doctrine AJP – 01 (B), se arată că pentru exercitarea autorităţii de comandă şi control, comandantul şi statul său

major folosesc proceduri standardizate şi Sistemul de Comunicaţii şi Informatică al Alianţei. Împreună, aceste două procese (de comandă şi de control) formează un sistem de comandă şi control, pe care comandantul, statul major şi subordonaţii lor îl folosesc să planifice, direcţioneze, coordoneze, controleze şi să susţină acţiuni militare.

În armata americană, termenul de „comandă şi control" este definit ca fiind exercitarea autorităţii şi direcţionarea forţelor din subordine (organice sau subordonate temporar) de către un comandant în scopul îndeplinirii misiunii. Sistemul de comandă şi control reprezintă acele facilităţi, mijloace, comunicaţii, proceduri şi persoane esenţiale unui comandant pentru planificarea, direcţionarea şi controlul acţiunii forţelor subordonate.

Specialiştii militari au diferite opinii atunci când explică „ce este şi din ce se compune un sistem C2 modern". În unele cazuri, sistemul C2 este văzut ca un simplu sistem tehnic destinat să ajute comandantul şi statul său major în desfăşurarea proceselor de comandă şi de control. În alte cazuri, sistemul C2 este văzut ca un sistem complex, alcătuit din două părţi principale: pe de o parte sistemul tehnic şi, pe de altă parte, comandantul, statul major şi procedurile de lucru. O altă variantă explică un sistem C2 ca fiind o sumă de subsisteme C2 sau de noduri C2.

O altă abordare foloseşte teoria conducerii organizaţiilor şi teoria sistemelor informaţionale. Astfel, orice organizaţie are un sistem decizional, un sistem informaţional şi un sistem operaţional. Alţi specialişti militari au descompus sistemele C4I2 şi le-au analizat pe subsisteme, astfel: subsistemul de comandă şi control; subsistemul de reţele locale şi extinse de calculatoare; subsistemul de informaţii; interoperabilitatea.

Toate variantele prezentate anterior sunt corecte şi logice atât timp cât sunt privite din perspectiva pe care au avut-o autorii lor. Logica analizelor făcute ne direcţionează către o abordare a sistemelor C2 dintr-o perspectivă evoluţionistă.

3. Perspective în dezvoltarea sistemelor de comandă şi control

Din punct de vedere conceptual, viitorul sistemelor C2 se bazează pe integrarea deplină a proceselor de comandă şi de control în sistemul informatic. Pentru că decizia rămâne atributul omului, este esenţial ca viitorul sistem C2 să permită folosirea a trei categorii de decizii:

1.„Decizia evidentă" care va apare în condiţiile în care toate informaţiile necesare sunt cunoscute şi nu există nici un grad de incertitudine. Ea poate fi chiar şi automatizată cel puţin la nivelul unor reguli de angajare.

2. „Decizia simplă” este aceea pentru care un set de variante corespunzătoare şi criteriul de selecţie între ele este bine cunoscut şi înţeles. Acest tip de decizie poate fi automatizată parţial.

3. „Decizia complexă” nu poate fi automatizată şi este aceea pentru care nu se cunosc variantele corespunzătoare şi criteriul de selecţie între ele. Ea se rezolvă prin metoda cursurilor de acţiune.

Pentru ca viitoarele sistemele C2 să fie eficiente, ele trebuie să permită noi modalităţi de colaborare între personalul de stat major şi noi modalităţi de interacţiune a acestuia cu mijloacele informatice şi cu sursele de informaţii. Pentru îndeplinirea acestui deziderat va trebui creată o gamă largă de tehnologii de interacţiune om-maşină care să mărească viteza şi eficienţa interacţiunii dintre utilizator şi calculator.

Simularea în timp real

Un număr mare dintre sarcinile şi activităţile unui comandament pot fi executate mai uşor şi mai bine folosind tehnologiile de simulare. Până în prezent, aceste tehnologii au fost folosite doar pentru desfăşurarea unor analize şi antrenamente. Nu există programe de simulare construite în mod specific pentru a fi folosite pe timpul acţiunilor de luptă. În viitor însă, eficacitatea comandamentelor va fi îmbunătăţită prin utilizarea programelor de simulare proiectate să faciliteze dezvoltarea şi analiza cursurilor de acţiune, revederea planului de acţiune şi monitorizarea desfăşurării acţiunii militare propriu-zise.

Viitoarele programe de simulare special proiectate pentru a fi folosite pe timpul acţiunilor militare ar putea fi denumite simulări în timp real – STR. Pe baza unei puteri de calcul suficient de mare, STR va facilita analiza în timp real a implicaţiilor pe care le ar avea punerea în aplicare a unei anumite decizii. Practic, STR va simula evoluţia în timp a cursurilor de acţiune şi va furniza, în timp util, diferite informaţii în legătură cu fiecare curs de acţiune simulat. Pe baza acestor informaţii, comandantul va lua decizia corectă în momentul oportun.

Efectele benefice ale introducerii STR sunt multiple. Cele mai importante sunt legate de îmbunătăţirea cunoaşterii situaţiei, prevenirea supraîncărcării cu informaţii şi micşorarea ciclului decizional.

Cu ajutorul STR, statul major va putea analiza adecvat mai multe cursuri de acţiune în aceeaşi unitate de timp. Pe timpul rulării simulărilor vor fi evidenţiate automat problemele legate de sincronizarea forţelor. Apoi, rezultatele simulărilor vor fi folosite ca un criteriu de evaluare şi selecţie a cursurilor de acţiune. Un alt avantaj al folosirii STR îl reprezintă posibilitatea reducerii numărului de persoane implicat în analiza cursurilor de acţiune. STR va putea rula pe un singur calculator şi va necesita un singur operator.

Pe timpul revederii planului de acţiune, diferite funcţiuni ale unei forţe (sprijin cu foc, sprijin aerian nemijlocit, mobilitate şi contra-mobilitate etc.) vor putea fi revăzute în detaliu mult mai uşor în scopul coordonării forţelor subordonate şi a înţelegerii depline a planului de acţiune aprobat. Revederea planului cu ajutorul STR prezintă un avantaj major în sensul că participanţii de la eşaloanele subordonate nu trebuie să se deplaseze la punctul de comandă al eşalonului superior. Este suficientă conectarea mai multor monitoare aparţinând subordonaţilor la calculatorul de la eşalonul superior pe care rulează STR.

Un program software de tip „agent de monitorizare" observă imediat dacă apar deviaţii semnificative de la planul iniţial şi avertizează comandantul dacă succesul planului iniţial este în pericol şi dacă va fi necesară o nouă decizie.

O bună parte dintre tehnologiile necesare pentru proiectarea şi construcţia unui STR există în prezent. Totuşi, mai sunt multe probleme de rezolvat atât din punct de vedere conceptual, cât şi tehnologic.

Există două variante de reprezentare a spaţiului virtual în care va avea loc acţiunea militară. Varianta 2D (două dimensiuni) este avantajată de cerinţele hardware mai mici şi de obişnuinţa actualelor comandamente de a lucra pe hărţi plane. Varianta 3D (trei dimensiuni) ar permite o abordare mult mai completă şi mai intuitivă a simulării, dar va necesita platforme hardware puternice şi antrenarea intensă a comandamentelor pentru utilizarea hărţilor tridimensionale.

Aplicaţiile software de tip „agent de monitorizare" vor necesita interogarea asincronă şi în orice moment a bazei de date STR. Dar această bază de date este dinamică, ea fiind permanent modificată de rularea simulării. În scopul menţinerii integrităţii bazei de date STR este necesară dezvoltarea unei tehnologii noi de management dinamic al bazelor de date care să permită completarea şi interogarea simultană a bazei de date STR.

Pentru a face o predicţie cât mai riguroasă a rezultatului unei acţiuni militare, entităţile din simulare trebuie să se comporte la fel ca şi unităţile reale pe care le reprezintă. Practic, viitorul mod de acţiune al unei entităţi militare este strâns legat de performanţa sa anterioară în acţiuni militare similare şi de o serie de factori unici pentru fiecare entitate în parte (moral, calitatea personalului, nivel de pregătire, experienţă etc.). Acelaşi lucru este valabil şi pentru forţele inamice. Rezultă că este necesară dezvoltarea unei tehnologii care să nuanţeze în funcţie de factorul uman comportamentul, totuşi diferit, a unor entităţi de acelaşi tip.

În concluzie, există câteva modalităţi prin care simularea poate fi integrată într-un sistem C2. Simulările pot fi folosite în toate fazele unei acţiuni militare. Beneficiul cel mai mare se va obţine atunci când actualele proceduri de stat major vor fi înlocuite cu altele noi, revoluţionare. În prezent, există o serie de tehnologii ce pot fi dezvoltate pentru a fi incluse într-un sistem STR. Celelalte tehnologii

necesare pot fi demonstrate în viitorul apropiat. Pe baza ritmului actual de dezvoltare tehnologică se poate estima că primul sistem de simulare în timp real poate fi operațional în anul 2010.

Perspective tehnologice

Pentru ca viitoarele sistemele C2 să fie eficiente, ele trebuie să permită noi modalități de colaborare între personalul component şi noi modalități de interacțiune a acestuia cu mijloacele informatice şi cu sursele de informații.

Pentru îndeplinirea acestui deziderat va trebui creată o gamă largă de tehnologii de interacțiune om-maşină (împreună cu dispozitivele fizice necesare) care să mărească de 10 ori viteza şi eficiența interacțiunii dintre utilizator şi calculator. Tehnologiile necesare includ: recunoaşterea vocii în conversația liberă, recunoaşterea în mod continuu a scrisului de mână, urmărirea persoanelor şi a mimicii feței folosind camere neobservabile, realitatea virtuală şi grafica 3D, integrarea dispozitivelor de tip „handheld" cu alte dispozitive de introducere sau afişare a datelor, lucrul în echipă şi afişarea în comun a rezultatelor etc.

În plus, înregistrarea automată a acțiunilor desfăşurate va face mai eficientă prezentarea şi evaluarea respectivelor acțiuni. Acest tip îmbunătățit de înregistrare multi-mod va asigura o memorare instituțională a activității dintr-un comandament, ce va putea fi accesată în orice moment. De asemenea, ea poate fi folosită la crearea de programe „macro" sau de „agenți inteligenți" pentru automatizarea unor sarcini cu caracter de rutină. Luarea notițelor va fi uşurată de tehnologia „notițelor comune publice". Practic, toate şedințele vor fi înregistrate, urmărite şi procesate pentru a permite indexarea, răsfoirea şi rezumarea ulterioară a lor.

Toate facilitățile enumerate anterior vor fi create cu ajutorul unor instrumente flexibile de proiectare şi dezvoltare a aplicațiilor software. Acestea vor permite dezvoltatorilor de soft să creeze noi programe sau să le adapteze pe cele vechi atunci când situația o va impune. Ca urmare, vor fi necesari mai puțini oameni pentru configurarea sistemelor şi crearea interfețelor suplimentare de acces la noi baze sau surse de date.

Până în prezent au fost demonstrate următoarele tehnologii software: JANUS – recunoaşterea vocală; NPEN++ – recunoaşterea scrisului de mână; MULTIMODAL TOOLKIT – controlul interfețelor de acces; ARIADNE MAP TOOL – vizualizarea obiectelor pe fondul unei hărți; PEBBLES – lucrul în echipă şi afişarea comună a datelor; ALICE – crearea şi afişarea spațiilor 3D; CSPACE – înregistrarea în format electronic a şedințelor şi crearea documentelor „evolutive" (prin actualizare sau creare de versiuni noi). Aceste tehnologii urmează a fi dezvoltate şi integrate în viitoarele sisteme C2.

Perspective în domeniul afişării datelor

Una dintre principalele teme abordate de către proiectanţii sistemelor C2 o reprezintă tehnica de afişare a informaţiilor. S-au desfăşurat analize şi experimente intense pentru a determina acele tehnici de afişare care să permită înţelegerea imediată a situaţiilor des schimbătoare din acţiunile militare moderne. Cea mai recentă inovaţie în acest domeniu se numeşte „blobology" – tehnica petei de cerneală.

Actualele monitoare folosesc un sistem de afişare bidimensional, static şi saturat cu fel de fel de grafice. Pentru reprezentarea forţelor se folosesc simbolurile standard, utilizate şi în cele două războaie mondiale. De fapt, actualele simboluri mai mult induc în eroare comandanţii în privinţa adevăratei puteri de luptă a forţelor reprezentate prin simboluri. Privind un simbol, comandantul este nevoit să-şi imagineze compunerea, dispunere, puterea de luptă şi alţi factori legaţi de forţele reprezentate de acel simbol.

Nevoia pentru crearea unei tehnici superioare de afişare a informaţiilor va fi şi mai stringentă în viitor, atunci când comandanţii vor fi inundaţi de informaţii provenind dintr-o multitudine de surse. Prin urmare, din punct de vedere uman, există doar două soluţii practice pentru gestionarea unui flux imens de date şi informaţii. Prima soluţie se referă la automatizarea procesului pentru mărirea vitezei de lucru. A doua soluţie se referă la afişarea intuitivă a informaţiilor pentru mărirea densităţii de informaţii din câmpul vizual.

În urma schimbării modelului de reprezentare a forţelor şi terenului, afişarea intuitivă şi expresivă a informaţiilor va duce la înţelegerea lor mai rapidă şi mai uşoară de către observatorul uman. Nu va fi nevoie de reducerea fluxului de informaţii, ci de afişarea lui într-o altă manieră.

Ca urmare, percepţia oamenilor va fi amplificată prin mărirea resurselor mentale disponibile, reducerea timpului de căutare, îmbunătăţirea abilităţii de recunoaştere a obiceiurilor (şabloanelor), creşterea numărului de deducţii efectuate şi mărirea sferei posibil a fi monitorizată.

În ultimii ani, tehnica „petei de cerneală" a fost dezvoltată în mai multe etape.

Prima variantă a folosit simbolurile militare convenţionale. A doua variantă a fost îmbunătăţită prin folosirea mai multor atribute ale unei forţe, cum ar fi zona de descoperire şi zona de lovire. Astfel, se putea răspunde instantaneu la întrebări de genul „ce pot vedea şi ce nu?" sau „ce pot lovi şi ce nu?". A treia variantă a încorporat mai mulţi factori ce pot influenţa reprezentarea forţelor cu ajutorul petelor. A patra variantă a tehnicii de afişare aduce o îmbunătăţire majoră în domeniu prin includerea unor atribute la nivel de entitate. Aceasta permite trecerea de la reprezentarea dedusă în urma interpolării unor date (centrul de

greutate, teren, formă de luptă etc.) la o reprezentare bazată pe poziția raportată în timp real a tuturor entităților din compunere.

Reprezentarea cu ajutorul entităților componente prezintă avantaje față de modelul tradițional. Dispunerea unor elemente ale puterii de luptă şi orientarea acestora poate fi evidențiată mai uşor. Grafica poate fi adaptată în funcție de situație sau de cerințele utilizatorului. Anumite detalii sau combinații de detalii pot fi selectate pentru afişare. Spațiul liber şi cel ocupat de către forțe este arătat cu mai multă precizie. Practic, comandantul poate interacționa cu datele reale ale forțelor subordonate, fără ca acestea să fie alterate prin rezumarea sau prezentarea făcută de altă persoană sau alt program.

În concluzie, efectele vizuale au un impact profund asupra abilității oamenilor în explorarea datelor, asimilarea informațiilor şi producerea cunoştințelor. Beneficiile şi consecințele unei corecte implementări ar fi: mărirea vitezei de înțelegere, îmbunătățirea calității deciziilor adoptate, mărirea ritmului acțiunilor militare, îmbunătățirea procesului decizional în condiții de oboseală şi lipsă de experiență, folosirea unei structuri de comandă şi control mai mică şi mai mobilă, precum şi sporirea comunicării şi colaborării pe timpul planificării şi execuției acțiunilor militare.

Identitatea digitală

Securitatea informației în viitorul sistem C2 este o provocare majoră. Deoarece magistralele informaționale depăşesc barierele, uşile zăvorâte nu mai sunt suficiente pentru a proteja unul dintre cele mai valoroase bunuri – informația. Toate organizațiile recunosc nevoia de a răspunde la creşterile explozive de trafic ale informațiilor în format electronic atât din preocuparea pentru protecția datelor proprii, cât şi din dorința de a instrumenta acest nou mediu pentru avantaje competitive.

Securitatea informației este cheia acestor două cerințe. Este nevoie de acelaşi grad de siguranță şi încredere în informațiile electronice, ca şi în cele tradiționale. Răspunsul la această provocare poate fi dat de identitatea digitală. Aceasta este reprezentarea digitală a identității umane în interacțiunea cu alte maşini sau alte persoane în cadrul rețelelor distribuite. Identitatea digitală trebuie să aibă gradul de complexitate şi de robustețe pe care îl implică utilizarea sa în cadrul unui sistem C2. Altfel spus, anumite sisteme reclamă o identitate digitală mai robustă decât altele deoarece gradul de încredere în informația transmisă poare varia semnificativ în funcție de tipul sistemului.

Implementarea conceptului de identitate digitală în cadrul unor sisteme informatice implică, în primul rând, dezvoltarea unor aplicații software dedicate managementului identității digitale. Cu toate că astfel de aplicații sunt mai

complexe decât cel mai sofisticat sistem de management al parolelor, realizarea acestora conduce la beneficii majore în managementul, securitatea şi productivitatea sistemelor.

Dezvoltarea tehnologiilor privind identitatea digitală va schimba lumea calculatoarelor, aşa cum a făcut-o cu câțiva ani în urmă dezvoltarea rețelelor. La fel ca în cazul acestora, introducerea conceptului de identitate digitală pare să conducă la o creştere dramatică a complexității sistemelor, dar, odată integrată în aplicații, această complexitate devine transparentă pentru utilizatori, producând o creştere rapidă a scalabilității şi productivității.

Una dintre cele mai importante implementări ale identității digitale este semnătura digitală. Conceptul şi utilitatea semnăturii digitale au fost definite şi recunoscute cu câțiva ani înainte de apariția primei realizări practice, schema inițială pentru semnătură digitală rămânând şi astăzi una dintre cele mai practice şi versatile tehnici disponibile. Cercetările ulterioare au condus la apariția altor tehnici, dintre care unele oferă avantaje semnificative relativ la funcționalitate şi implementare; toate aceste realizări au însă la bază criptografia asimetrică cunoscută şi sub denumirea de criptografie cu chei publice.

Semnătura digitală a unui mesaj este o configurație de digiți (cifre) depinzând de o anumită cheie secretă deținută numai de semnatar (cheia privată) şi de conținutul mesajului semnat. Semnătura trebuie să poată fi supusă unui mecanism de verificare sigur, astfel încât nici una dintre părți să nu poată nega acțiunile efectuate în timpul tranzacției, iar orice litigiu să poată fi rezolvat echitabil de către o terță parte, fără ca aceasta să cunoască cheia privată a semnatarului.

Perspective în domeniul achizițiilor

În anul 1994, Secretarul de Stat al Apărării SUA, domnul Wilhelm Perry, a semnat o directivă care a schimbat sistemul de achiziții al armatei americane. Parte a Legii de reformă a achizițiilor (Acquisition Reform Act), noua directivă ministerială orienta categoriile de forțe armate către produsele comerciale „de pe raft” (Commercial-Off-The-Shelf), pentru a reduce costurile aferente achizițiilor prin eliminarea cheltuielilor de proiectare de la zero a unor sisteme care aveau numai specificații militare. Prin această directivă, directorii programelor de înzestrare au fost obligați să studieze permanent piața liberă de produse şi servicii pentru a descoperi acele produse comerciale civile ce pot fi cumpărate şi folosite în domeniul militar. Scopul administrației americane era de a transfera costurile cercetării, dezvoltării şi testării produselor în sarcina producătorilor.

O imediată consecință a noii politici americane a fost pierderea influenței pe care armata americană o avea în sectorul electronicii şi a tehnicii de calcul. Dacă

în anii ’70, armata americană cumpăra mai mult de 30% din producţia acestui sector, în anii ’90, cota a scăzut sub 0,5%. Astfel, dezvoltarea noilor generaţii de produse electronice a fost dirijată de nevoile consumatorilor civili şi de tendinţele pieţei mondiale, transformând sectorul militar într-un simplu spectator.

O a doua consecinţă a fost crearea unui paradox. Pe de o parte, directorii programelor de achiziţii au fost încântaţi de costul scăzut la achiziţie al produselor electronice de ultimă generaţie. Pe de altă parte, utilizatorii produselor cumpărate au fost nemulţumiţi de uzura morală rapidă a acestora, ca urmare a apariţiei pe piaţă a unei noi generaţii. În plus, noua generaţie de componente nu putea fi folosită în vechile sisteme din cauza problemelor de compatibilitate şi a caracteristicilor constructive.

Acest paradox s-a accentuat pe măsura trecerii timpului ca urmare a spiralei din ce în ce mai strânse a evoluţiei tehnologice. Dacă în anii ‘90 ritmul de schimbare era de 3-4 ani, astăzi noile generaţii de procesoare apar o dată la 6 luni. În aceste condiţii, cum ar fi posibilă menţinerea în dotare timp de 10 sau 15 ani a unor sisteme ce devin arhaice după 2-3 ani şi pentru care piesele de schimb nu se mai produc?

Însă cea mai mare problemă a produselor „de pe raft” o reprezintă îndeplinirea cerinţelor indispensabile mediului militar în care aceste produse ar urma să fie folosite. În realitate, sunt foarte puţine produse din domeniul tehnicii de calcul şi al comunicaţiilor, care se vând pe piaţa civilă şi care îndeplinesc, în acelaşi timp, specificaţiile militare fără a necesita o modificare constructivă. Mai mult, în faza de testare la unităţi a unor produse propuse pentru achiziţionare, nimeni nu este de acord cu diminuarea parametrilor cheie de performanţă stabiliţi de viitorii utilizatori pentru respectiva clasă de produse.

Începând cu anul 2000, administraţia americană a trecut la implementarea unei noi strategii în domeniul achiziţiilor de produse de pe piaţa civilă. Aşa-numita strategie de „adoptare, adaptare şi dezvoltare” permite achiziţia la preţuri competitive şi în timp scurt a produselor „de pe raft” după ce acestea suportă unele modificări sau adaptări pentru a îndeplini specificaţiile militare. Practic, sistemul de lucru este destul de simplu.

Mai întâi, unele produse comerciale de pe piaţă se adoptă de către instituţiile specializate din domeniul militar (în sensul că se stabileşte posibilitatea şi oportunitatea folosirii lor de către forţele armate).

Apoi, producătorul adaptează produsele pentru a îndeplini specificaţiile militare. După introducerea lor în dotare urmează dezvoltarea lor în scopul atingerii unei durate de viaţă de 10-15 ani în serviciu. Există trei opţiuni ce pot fi luate în calcul: upgrade-ul, reconstrucţia sau „cumpărarea înapoi” (buy-back). Fiecare

opţiune are avantaje şi dezavantaje. Selecţia fiecărei opţiuni se poate face pentru fiecare produs în funcţie de raportul cost-eficienţă şi de alte criterii.

Câteva concluzii

Sistemele C2 moderne sunt foarte scumpe. Viitoarele sisteme C2 vor fi şi mai scumpe, iar spirala tehnologică este din ce în ce mai strânsă. Platformele hardware şi mijloacele de comunicaţii au un ciclu de viaţă din ce în ce mai mic din cauza, în special, uzurii morale. Din această cauză, speranţele noastre sunt legate de domeniul software. Modernizarea sau crearea de noi aplicaţii software poate duce la mărirea duratei de folosinţă a platformelor hardware şi a mijloacelor de comunicaţii. Dar şi domeniul software este un domeniu scump pentru că încorporează produsele cele mai de vârf ale inteligenţei umane.

Mai mult, „integrarea" este cuvântul cel mai folosit în prezent de către factorii de decizie militari. Şi în domeniul sistemelor C2 integrarea reprezintă şi va reprezenta una dintre direcţiile cele mai importante de acţiune. Costul integrării este cu atât mai mare cu cât sistemele C2 de integrat sunt mai diferite. Rezultă că este necesară centralizarea politicii în domeniul sistemelor C2 pentru a reduce costurile ulterioare legate de integrare.

În opinia noastră, decizia pentru achiziţia oricărui sistem C2 trebuie luată la un eşalon militar cât mai înalt, iar acest eşalon trebuie să răspundă şi de modernizările ulterioare, până la scoaterea respectivului sistem din funcţiune.

BIBLIOGRAFIE

1. Doctrina operaţiilor informaţionale SMG/FOP – 3.15, 2006.
2. AJP – 01 (B) Allied Joint Doctrine, NATO HQs, 2002.
3. AJP – 3 Allied Operations, NATO HQs, 2001.
4. Joint Doctrine for Information Operations, JP 3-13, 1998.
5. Joint Doctrine for Command and Control Warfare, JP 3-13.1, 1996.
6. Field Manual FM 106, Information Operations, 2003.
7. Joint Doctrine for Operations Security JP 3-54, 1997.
8. Joint Doctrine for Psychological Operations JP 3-53, 1996.
9. Joint Doctrine for Military Deception JP 3-58, 1996.
10. Joint Doctrine for Electronic Warfare JP 3-51, 2000.
11. Information Operations, Joint Warfare Publication 3-80, UK, 2002.
12. *NATO Glossary of Terms and Definitions AAP – 6,* 2002.

13. *Department of Defense Dictionary of Military and Associated Terms*, 2003.
14. Alberts D., Gratska J., *Network Centric Warfare – Developing and Leveraging Information Superiority,* 1999.
15. Boaru Gh., Pungă A., *Războiul informaţional în viziunea unor specialişti militari străini şi români,* Sesiune de comunicări ştiinţifice, UNAp „Carol I", 2007.
16. Boaru Gh., Pungă A., *Implicaţiile războiului de comandă şi control asupra planificării acţiunilor militare,* Sesiune de comunicări ştiinţifice, UNAp„Carol I", 2006.
17. Boaru Gh., Pungă A., *Etica atacului reţelelor de calculatoare din compunerea sistemelor de comandă şi control moderne,* Sesiune de comunicări ştiinţifice, Universitatea Naţională de Apărare„Carol I", 2006.
18. Boaru Gh., Pungă A., *Comunicarea în confruntarea informaţională,* Sesiune de comunicări ştiinţifice, Universitatea Naţională de Apărare„Carol I", 2006.
19. Boaru Gh., *Războiul informaţional şi operaţiile informaţionale*, Editura UNAp. 2004.
20. Libicki Marin C., *What is Information Warfare?,* 1995.
21. Roceanu I., *Fundamente ale sistemelor C4I,* Editura U.N.Ap., Bucureşti, 2004
22. Timofte Gruia, *Stabilitatea sistemelor C4I2 în condiţiile războiului informaţional intens,* Simpozion ştiinţific, Universitatea Naţională de Apărare, Bucureşti, 2004.

INSTRUIREA BAZATĂ PE REȚEA. O NOUĂ PARADIGMĂ A PROCESULUI DE TRANSFORMARE A NATO ÎN AJUTORUL SISTEMULUI DE COMANDĂ ŞI CONTROL

Colonel prof. Ion ROCEANU
Doctorand Cătălin RADU

I. ASPECTE GENERALE PRIVIND E-LEARNING, E-EDUCAȚIA ŞI E-INSTRUIREA

E-learning este un termen general care defineşte noua paradigmă educațională, bazată pe tehnologia comunicațiilor şi informaticii. Limitele conceptului e-learning nu sunt clar stabilite. Cei mai mulți specialişti în domeniu consideră că acest concept acoperă toate aspectele educaționale specifice epocii informaționale. Din această perspectivă, regăsim o largă varietate de soluții e-learning care depind de mai multe variabile şi care toate sunt relaționate cu specificități ale sistemelor educaționale instituționale, cu scopurile şi obiectivele lor concrete. Nici una dintre soluțiile e-learning existente nu este exhaustivă şi nici una nu poate fi exportată fără a fi particularizată către instituții similare. Un lucru este sigur: fiecare dintre aceste soluții se bazează pe o serie de principii comune, după cum urmează:

- folosirea tehnologiei comunicațiilor şi informaticii pentru a distribui cunoştințe şi a îmbunătăți abilitățile celor care învață;
- elementul central al e-learning este reprezentat de conținutul

digital. Dezvoltarea conținutului digital nu este bazat întotdeauna pe standarde generale şi acest aspect are un puternic impact negativ privind interoperabilitatea şi conținutul digital;

- sistemul centrat pe student;
- mai multă flexibilitate în managementul timpului învățării. De aici rezultă două modalități diferite de diseminare a conținutului învățării: sincron şi asincron sau cu alte cuvinte cu sau fără prezența profesorului;
- partajarea cursurilor în diferite tipuri de rețele, în special prin Internet.

Să aruncăm o privire la imaginea următoare (Figura 1) care reprezintă cele mai reprezentative elemente ale unui sistem e-learning.

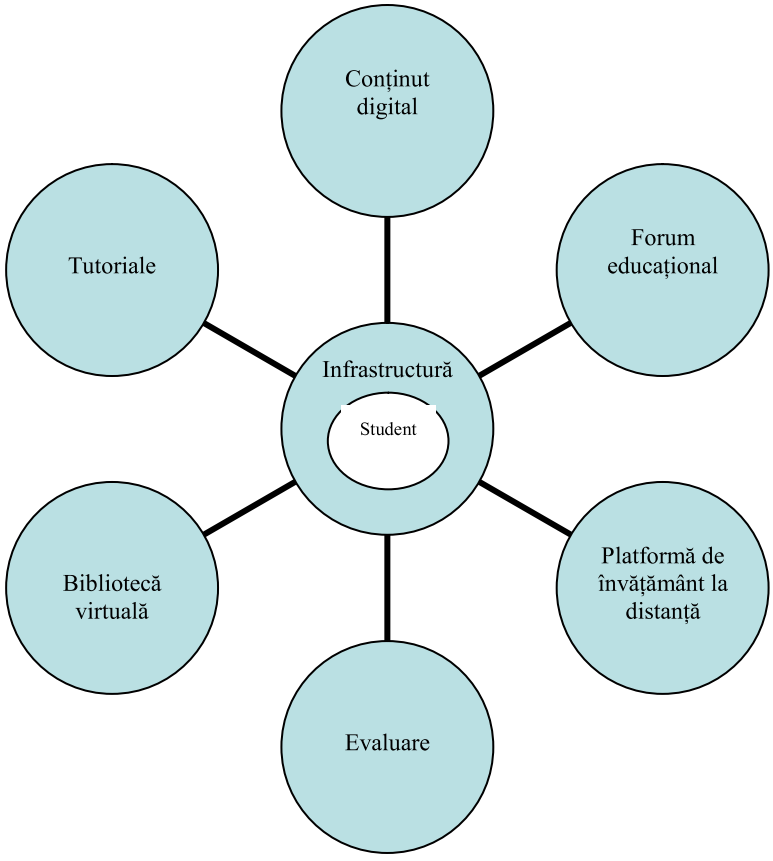


Figura 1. Cadrul general al unui sistem e-learning

Studenţii sunt în centrul sistemului fiind înconjuraţi de infrastructura IT&C, echipament hardware, software şi reţelele de comunicaţii pe care este distribuit conţinutul digital. Acest cadru este destinat conducerii proceselor de învăţământ pentru obţinerea obiectivelor educaţionale. Dar care sunt aceste obiective? Sunt aceste obiective diferite de cele cerute de învăţământul tradiţional? Răspunsul este clar NU. În acest caz diferenţele nu pot fi altele decât instrumentele şi metodele de învăţământ sau de distribuţie a cunoaşterii.

În spiritul acestui articol şi bineînţeles în concordanţă cu părerile specialiştilor în domeniu trebuie să acceptăm că e-learning este un termen general care prinde contur numai în strânsă legătură cu obiectivele educaţionale ale fiecărei instituţii. Instituţiile pot acoperi o arie vastă de aspecte educaţionale, de la educaţia primară la universităţi sau până la corporaţii multinaţionale. Obiectivele educaţionale sunt strâns relaţionate de structura personalului din instituţii, aspiraţiile acestora, aptitudinile lor profesionale, domenii de interes etc. În acest caz, este relevant să amintim că fiecare din aceste instituţii sunt interesate în soluţii e-learning specifice. De aceea, dacă încercăm să îndepărtăm oricare din componentele modelului e-learning general vom observa că modelul descris devine ineficient. În concluzie, adaptarea sau particularizarea sistemului e-learning la cererea instituţiilor trebuie făcută în interiorul elementelor sistemului e-learning .

Companiile care realizează sisteme e-learning nu produc sisteme pentru un singur beneficiar, produsele lor sunt generale în concordanţă cu standardele din domeniu, şi acestea pot fi adaptate conform cerinţelor operaţionale ale instituţiilor rezultând soluţii personalizate.

În figura 2 este reprezentată o schemă simplă prin care încercăm să explicăm implicaţiile pregătirii individuale asupra vieţii. Familia, şcoala şi societatea generează o influenţă egală asupra individului dar fiecare dintre acestea se regăsesc în altă dimensiune a învăţării individuale. La baza acestui triunghi este şcoala şi societatea, acestea având responsabilitatea (dar nu şi exclusivitatea) în formarea abilităţilor cunoaşterii şi aptitudinilor. În consecinţă, dacă dorim să vorbim despre utilizarea tehnologiei comunicaţiilor şi informaticii în activităţile de învăţare trebuie să ne concentrăm asupra întregului ansamblu fără a exclude pe celelalte.

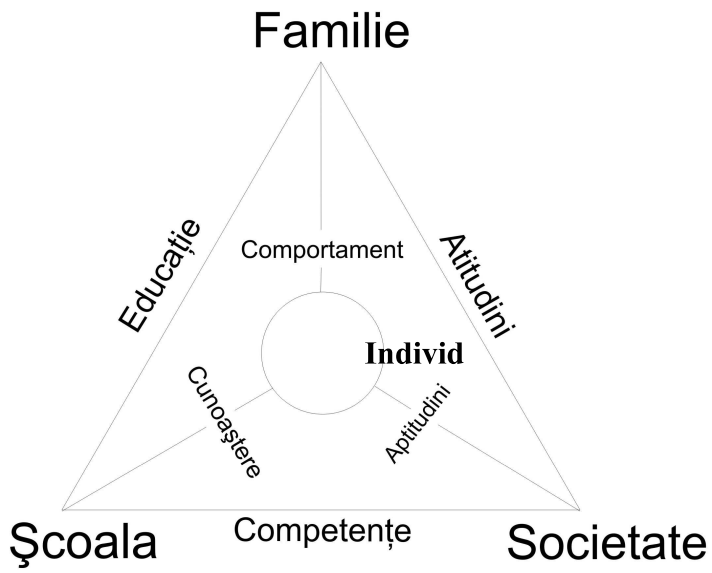


Figura nr. 2. Dimensiunile Învățării pe tot parcursul vieții

Probabil, atunci când specialiştii vorbesc despre împărţirea e-learning în cel puţin două direcţii majore, e-educaţie şi e-instruire, iau în consideraţie pe lângă obiectivele formative şi rolul instituţiilor în schimbarea instrumentelor şi metodelor pentru îndeplinirea obiectivelor.

II. Dezvoltarea sistemului de învăţământ distribuit avansat la distanţă al Universităţii Naţionale de apărare „Carol I”

Universitatea Naţională de Apărare „Carol I” este cea mai importantă instituţie de învăţământ militar din România şi în consecinţă are un rol important în procesul de transformare al forţelor armate, în concordanţă cu cerinţele noului mediu de securitate şi ale statutului de ţară membru NATO.

Misiunile Universităţii Naţionale de Apărare „Carol I” (U.N.Ap.) sunt orientate în două direcţii majore:

1. pregătirea liderilor militari şi civili şi a experţilor selectaţi pentru poziţii de management sau expertiză în domeniul apărării şi securităţii naţionale;
2. elaborarea de studii ştiinţifice la cererea structurilor cu responsabilităţi

în apărarea şi securitatea națională.

U.N.Ap. „Carol I" are, de asemenea, o contribuție majoră la elaborarea Planului director de modelare-simulare (PDMS) pentru forțele armate române. Rolurile îndeplinite de U.N.Ap. „Carol I" sunt următoarele:

- a furniza instrucțiunile PDMS pentru personalul UNAp „Carol I";
- planificarea educațională PDMS pentru personalul forțelor armate române;
- să furnizeze conținutul educațional în cadrul PDMS;
- să funcționeze ca un centru pilot pentru învățământ distribuit avansat la distanță în cadrul forțelor armate române;
- să supervizeze programul de educațional PDMS pentru absolvenți;
- să integreze folosirea tehnologiei pentru îmbunătățirea curriculei naționale prin programul educațional al armatei României;
- să răspundă la cererile armatei romane de analiză şi studiu.

Pe lângă rolul în sistemul educațional militar, U.N.Ap. „Carol I" este interconectată la sistemul național educațional şi avem o acreditare recunoscută la nivel național în sistemul procesului de la Bolonia.

În aceste condiții U.N.Ap. „Carol I" trebuie să se conformeze atât standardelor educaționale militare, cât şi civile, care reglementează învățământul distribuit avansat la distanță. De aceea considerăm că este necesară dezvoltarea unui sistem e-learning compatibil cu ambele tipuri de cerințe.

Suntem convinşi că e-Learning este următoarea tendință în domeniul educațional şi că mai devreme sau mai târziu va fi prezent pe tot globul atât în sistemele educaționale civile, cât şi militare şi dorim să fim pregătiți pentru acest moment. Este un adevăr general acceptat că în acest moment nimeni nu poate fi cu adevărat pregătit să folosească la capacitate maximă instrumentele pe care e-learning le aduce în educație. În consecință prin acest proiect am încercat să punem la dispoziția profesorilor şi studenților cunoştințe, expertiză şi metode educaționale bazate pe tehnologiile informaționale din acest domeniu.

Luând în considerație rolul major şi interesul pentru domeniul e-learning, în toamna lui 2004, U.N.Ap. „Carol I" a creat un nou departament specializat în această problematică numit Departamentul pentru Învățământ Distribuit Avansat la Distanță. Misiunea Departamentului pentru Învățământ Distribuit Avansat la Distanță constă în „asigurarea serviciilor educaționale bazate pe tehnologii didactice informaționale, prin programe de studii oferite prin învățământ la distanță, în conformitate cu legile şi reglementările naționale şi în deplin acord cu principiile şi standardele NATO", moto-ul departamentului este: „de la informație la cunoaştere prin puterea tehnologiei informației aplicată în instruire şi educație,

acolo unde, când, ce şi pentru cine este nevoie".

Efortul departamentului ADL este divizat în două direcţii definite ca e-educaţie şi e-instruire. E-educaţia are în atenţie problematicile care decurg din Procesul de la Bolonia şi are ca principale obiective dezvoltarea capacităţilor descrise în documentele de la Bolonia sub denumirea de suport pentru servicii educaţionale. Aceste cerinţe sunt dezvoltate având în vedere cerinţele sistemului naţional educaţional: licenţă, masterat, doctorat, masterat on-line. E-instruirea este privită mai aproape de standardele NATO în domeniu şi are ca obiectiv pe termen lung, dezvoltarea abilităţilor militare la nivel de individ şi de echipă. E-instruirea se bazează pe conceptele educaţionale ale învăţământului distribuit avansat la distanţă şi în consecinţă este bazată pe standardele SCORM.

Aceste obiective sunt: creşterea abilităţilor şi cunoştinţelor studenţilor, flexibilitate în structura cursurilor şi conţinutului educaţional, folosirea instrumentelor de management al studenţilor, mai multă libertate în gândire, integrarea în sistemul de instruire militar al NATO.

Beneficiarii reţelei e-learning dezvoltate de U.N.Ap. „Carol I" sunt: personalul militar şi civil din cadrul Ministerului Apărării Naţionale, personal din alte ministere cu atribuţii în sistemul naţional de apărare şi securitate, instituţii guvernamentale şi non-guvernamentale, personal din structurile NATO şi din ţările Parteneriatului pentru Pace.

Pornind de la imaginea generală a unui sistem e-learning format din trei elemente esenţiale, infrastructura hardware şi de comunicaţii, platforma e-learning şi conţinut digital educaţional am alcătuit un model prezentat în figura 3. Acest model are trei nivele, fiecare dintre ele acoperind un segment al cadrului general e-learning : *infrastructură, sistem de management al învăţării, conţinutul digital.*

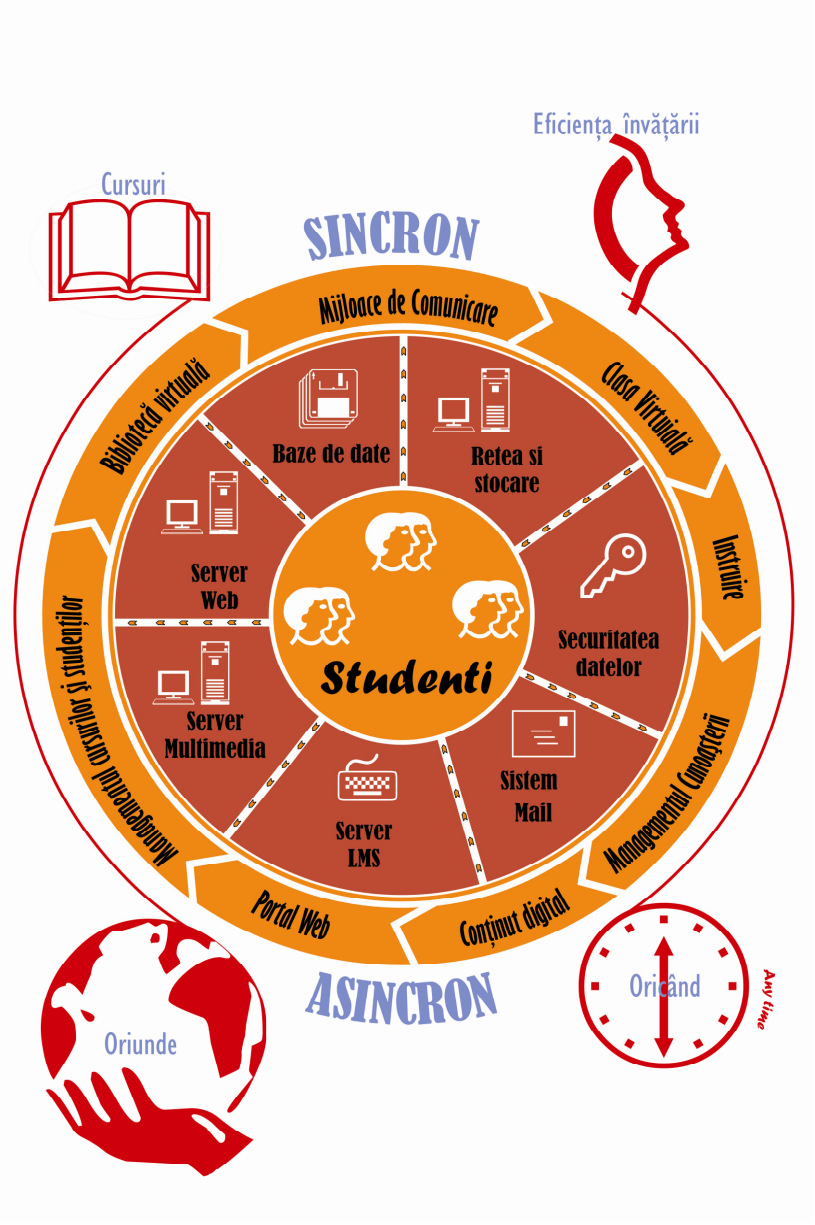


Figura 3. Modelul e-learning al Universităţii Naţionale de Apărare "Carol I"

III. E-educaţie şi e-instruire între comun şi specific

Schimbarea naturii societăţii, a modului în care acesta interacţionează au făcut ca cerinţele referitor la aptitudinile profesionale şi vocaţionale să evolueze. La locul de muncă a crescut complexitatea sarcinilor, de asemenea tipurile de sarcini pe care angajatul trebuie să le soluţioneze s-au diversificat şi s-a introdus un sistem de muncă flexibil şi în echipă ceea ce înseamnă că s-au schimbat şi natura sarcinilor pe care un angajat trebuie să le îndeplinească.

În mod similar, structura societăţii în întregul său a devenit mult mai puţin uniformă decât în trecut şi aptitudinile personale (adaptabilitate, toleranţă a celorlalţi şi a autorităţii, munca în echipă, rezolvarea problemelor, asumarea riscurilor, modul de lucru independent etc) sunt din ce în ce mai cerute dacă oamenii doresc să trăiască împreună în toleranţă şi respect reciproc. Cea mai importantă dintre aceste aptitudini este abilitatea de a învăţa – menţinerea curiozităţii şi interesului în ceea ce priveşte noile dezvoltări tehnologice şi aptitudini fără de care – Învăţarea pe tot parcursul vieţii nu poate exista.

Pentru mulţi profesori, această abilitate este foarte dificil de stimulat, cu toate că această dezvoltare va trebui de acum înainte să fie în centrul atenţiei atât pentru instruirea profesorului, cât şi pentru cercetarea ştiinţifică în domeniul educaţiei în anii care vor urma.

Parte a procesului educaţional este promovarea unei atitudini corecte a cetăţeanului. Scopul acesteia este când şi cum participă cetăţenii în toate sferele vieţii economice şi sociale, care sunt oportunităţile şi riscurile pe care aceştia le întâlnesc prin această atitudine, şi în ce măsură aceştia cred că aparţin şi au un cuvânt de spus în societatea în care trăiesc. Promovarea cetăţeniei active şi oportunităţile de angajare sunt complementare, ambele depind în mare măsură de atitudinea oamenilor, de cunoştinţele şi abilităţile de a aduce o contribuţie la viaţa economică şi socială. În acest context este necesar de a fi redus procentul abandonului şcolar. În acelaşi timp, trebuie menţionat că învăţământul non-formal sporeşte capacitatea tinerilor de a-şi găsi o slujbă şi le dezvoltă competenţele şi abilităţile personale.

Integrarea actuală a tehnologiei informaţiei şi a comunicării în educaţie îşi focalizează atenţia asupra educaţiei formale şi non formale asupra instituţiilor, asupra timpului şi spaţiului, în aceeaşi măsură cu cunoştinţele şi mediul de lucru. Noile servicii-suport sunt cerute pentru a uşura folosirea ITC în educaţie şi pentru a amplifica şansa obţinerii de rezultate pedagogice, de la servicii care facilitează folosirea echipamentului tehnic, la servicii care asigură securitatea pe Internet şi servicii care promovează o mai bună personalizare a procesului educaţional prin ghidare, instrucţie şi tutoriatul fiecărui student.

Plecând de la această idee şi făcând un scurt istoric al educației şi instruirii cu metode clasice rezultă următoarea concluzie logică: dacă educația şi instruirea sunt considerate diferite în abordarea clasică, folosind sistemul digital putem afirma că ele sunt tot diferite.

Această constatare duce la o nouă întrebare: care sunt diferențele între educație şi instruire în modelul educațional tradițional şi cum sunt diminuate diferențele dintre acestea în noua abordare bazată pe e-learning.

Componenta educațională

Sintagma e-education este specifică învățământului formal, sistemului instituțional, de la învățământ primar, la universități. În consecință, grupul țintă pentru e-educație este format din elevi şi studenți. Aceştia trebuie să acumuleze o cantitate mare de cunoştințe, să învețe să gândească, să facă legătura dintre valorile predate în şcoală cu viața reală, să transforme teoria în practică şi aşa mai departe. Din aceste motive, conținutul digital al e-educației pregătit pentru a fi livrat de către infrastructura IT&C destinat pentru autoînvățare sau pentru educația asistată de profesor trebuie să fie în concordanță cu principiile didactice şi pedagogice.

Nu este în intenția mea să aprofundez aici problematicile legate de conținutul didactic şi obiectele e-learning în ce priveşte nivelul de şcolarizare, în acest sens existând foarte multe studii create de experți în domeniu, dar devine evident în conținutul didactic la acest nivel o caracteristică amplu descriptivă în text (abordarea clasică) şi o carateristică mult mai explicită în obiectele multimedia.

2.2. Componenta e-instruire.

Termenul e-instruire este des folosit în asociere cu învățarea pe tot parcursul vieții, în contextul învățământului pentru adulți, dezvoltărilor aptitudinilor profesionale şi a activităților de instruire la nivelul companiilor.

Prin activitatea de instruire, modelele de sarcini de lucru sunt foarte valoroase, deoarece sporesc şansele de angajare şi oferă experiență în ceea ce priveşte piața muncii. Legăturile cu angajatorii sunt importante, de exemplu, aceştia furnizând instructorilor o perspectivă a aptitudinilor ce vor fi cerute în viitor. Zona de interes pentru e-instruire pot fi:

- învățământul vocațional şi de aptitudini;
- continuarea educației după nivel universitar;
- introducere şi instruire în problematica corporației;
- dezvoltare profesională;
- instruirea personalului tehnic;

- instruire conform normelor si standardelor legale.

Datorită domeniului meu de expertiză, educaţia militară, pot declara că în acest sector este relevantă folosirea instrumentelor IT&C pentru îmbunătăţirea abilităţilor, capacităţilor şi aptitudinilor individului etc.

În domeniul educaţiei militare termenii asociaţi e-instruirii au fost definiţi după cum urmează:

Instruire militară generală. Instruire şi/sau pregătire profesională specifică primelor funcţii care vizează etapele de pregătire iniţială, care are o durată de 2-4 ani, care aprofundează pregătirea iniţială şi oferă calificare pentru o anumită sarcină misiune sau carieră.

Dezvoltare profesională. Instruire şi/sau pregătire profesională specifică care apare după instruirea militară generală, în general după parcurgerea a 4 ani de serviciu militar. Dezvoltarea profesională include atât pregătire tehnică, cât şi pregătire în cariera militară.

Instruirea abilităţilor tehnice. Instruire primită oricând după instruirea iniţială care vizează pregătirea indivizilor sau a echipelor pentru sarcini speciale, servicii sau îndatoriri de lucru (exemplu: operarea echipamentelor specifice, instruirea în folosirea limbajului tehnic specific) .

În concordanţă cu opinia experţilor militari americani în probleme de educaţie şi instrucţie, mai mult de un sfert din militarii SUA, din toate armele şi serviciile sunt implicaţi în activităţi de instruire. Costurile pentru pregătirea permanentă sunt mari şi includ atât bugetul educaţiei (profesori, facilităţi, laboratoare, şi exerciţii), cât şi costuri care privesc cazarea, transportul şi alte cheltuieli personale.

Dezvoltarea unui sistem integrat e-learning poate aduce multe avantaje, nu numai din punct de vedere al costurilor, dintre care enumerăm:

- ✓accesibilitate, instruire în orice loc şi oricând pentru indivizi şi echipe;
- ✓agilitate – abilitatea de a personaliza instruirea la nevoile personale;
- ✓creşterea calităţii instruirii iniţiale;
- ✓creşterea calităţii instruirii în limbajul şi/sau cultura militară.

Concluzie

E-educaţia şi instruirea sunt membre ale aceleaşi familii. Diferenţele dintre acestea nu sunt mai importante decât similitudinile şi, în consecinţă, înainte de a vorbi despre una dintre ele, trebuie vorbit despre e-learning.

Bibliografie

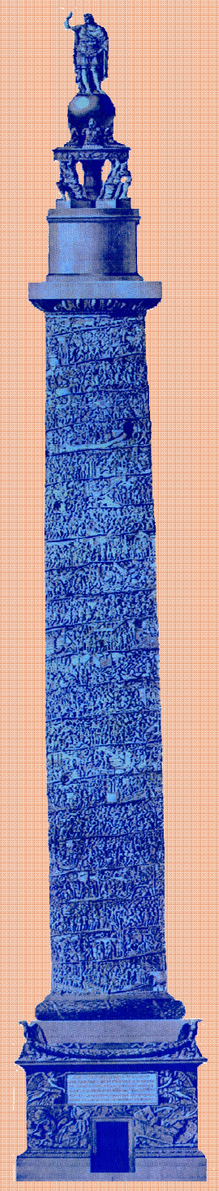
2. *Detailed work programme on the follow-up of the objectives of Education and training systems în Europe,* Official Journal of the European Communities, 14.6.2002
3. *Implementation of "Education & Training 2010" work programme, EUROPEAN COMMISSION Directorate-General for Education and Culture*
4. *US Army's Advanced Distributed Learning Vision,* 2001, Department of Defense Library
5. *The International Relations and Security Network's e-Learning Project, ISN e-Learning Project Description* / Zurich, 10/23/03
6. Ion Roceanu, *ADL master Plan Development*, NATO ADL Forum, Norfolk, SUA 2006
7. Ion Roceanu, *Citizens` security education based on e-learning technology,* Berlin, EDUCA 2007, ISBN 3-9810562-7-2

Revista de Ştiinţe Militare

EDITOR
Secţia de Ştiinţă Militară
a
Academiei Oamenilor de Ştiinţă
din România

Editura Universităţii Naţionale de Apărare "Carol I"
Şoseaua Panduri, nr. 68-72, sector 5, Bucureşti
e-mail: editura@unap.ro
Tel./Fax: 319.59.69; 319.48.80/0215; 0307

Revista de Ştiinţe Militare *apare semestrial*



ÎN ATENŢIA COLABORATORILOR

Pentru o mai bună procesare a articolelor, dorim respectarea următoarelor reguli de tehnoredactare:

1. ***Textul.*** Se introduce în Microsoft Word, folosind fontul Times New Roman şi tastatura standard românească. Nu sunt acceptate fonturile care au mapări neobişnuite (în care caracterele cu diacritice - ş, ţ, ă, î şi Ş, Ţ, Ă, î - înlocuiesc alte caractere - [,], @, ~, \ ş.a.m.d.). Textul în limba română trebuie să aibă în mod obligatoriu diacritice. Articolul trebuie cules, pur şi simplu, fără nicio altă formatare în afara sublinierilor, acolo unde este cazul, folosind bold şi italic. Paragrafele vor fi delimitate de un Enter, părţile articolului fiind separate între ele prin două-trei paragrafe goale.

2. ***Ecuaţiile.*** Indiferent de locul pe care îl ocupă în cadrul articolului, ecuaţiile se introduc numai în Microsoft Equation Editor 0a limită, se acceptă ecuaţii scrise de mână, numerotate şi trimise separat de restul articolului).

3. ***Figurile.*** Sunt acceptate formatele vectoriale standard. în cazul figurilor produse cu o altă aplicaţie decât Microsoft Word (de exemplu, Corel Draw sau în AutoCAD), fişierele respectivelor aplicaţii vor fi trimise împreună cu restul articolului. Figurile trimise în format electronic vor fi desenate la dimensiunile la care pot fi tipărite, iar dimensiunea textului trebuie să fie între 8 şi 12 puncte tipografice. Sunt acceptate şi figuri desenate de mână, pe foi separate de restul articolului, cu condiţia ca desenele să fie clare şi să poată fi uşor identificat locul din cadrul articolului în care trebuie să se regăsească.

4. ***Imaginile.*** Imaginile scanate trebuie incluse atât în documentul Microsoft Word, cât şi trimise separat. Nu se recomandă folosirea imaginilor preluate de pe Internet, deoarece acestea nu satisfac cerinţele necesare pentru tipărirea lor (având o rezoluţie mult inferioară celei necesare pentru un tipar de calitate). Imaginile de calitate au o rezoluţie de minimum 200 dpi. Pentru formatele JPEG şi GIF, aveţi în vedere ca, în urma compresiei, calitatea imaginii să devină rezonabilă.

5. ***Numerotarea.*** Ecuaţiile, figurile, tabelele, titlurile din bibliografie vor fi numerotate cu cifre arabe, astfel:

- între paranteze pătrate pentru bibliografie;
- între paranteze rotunde pentru formule;
- prin exponent, în cazul notelor de subsol;
- precedate de denumire, în cazul observaţiilor, figurilor, tabelelor etc.

Vă mulţumim !

Redacţia

Pentru publicarea de materiale promoţionale în cuprinsul revistei, rugăm agenţii economici şi pe toţi cei interesaţi să se adreseze redacţiei pentru a conveni forma de colaborare.

Coperta I: *Alexandru Ioan Cuza*, primul domn al Principatelor Unite (1859-1862)
(Valentin TĂNASE, ulei pe pânză, 100x70)
Coperta II: *Columna lui Traian*. Sursă: Muzeul Militar Naţional,
prin amabilitatea domnului Neculai Moghior, şeful Secţiei Documentare
Coperta IV: Gravură aquaforte 40x30 *"Universitatea Naţională de Apărare Carol I"*,
Eugen ILINA, Uniunea Artiştilor Plastici, România