IMPLICAŢIILE RĂZBOIULUI BAZAT PE REŢEA ŞI ALE CAPABILITĂŢILOR FACILITATE DE REŢEA ASUPRA REŢELELOR INFORMAŢIONALE DE TIPUL C4ISR LA NIVELUL ARMATEI ROMÂNIEI

IMPLICATIONS OF THE NETWORK WARFARE AND NETWORK ENABLED CAPABILITIES ON THE C4ISR INFORMATION NETWORKS IN THE ROMANIAN ARMY

General locotenent (r) prof. univ. dr. Cristea DUMITRU*

Rezumat: *Ultimele două decenii marchează trecerea omenirii în era informaţională, un nou stadiu de dezvoltare societal, în care societatea modernă este afectată, printre altele, de schimbările tehnologice explozive. În acest context, tehnologia constituie principalul factor al schimbării. Pentru a fi mai precis, mici inovaţii apărute în tehnologia informaţiei şi comunicaţiilor sunt considerate a fi responsabile de transformările la nivel global din structura economiei, politicii şi culturii. Această aserţiune îşi extinde însă valabilitatea şi asupra fenomenului militar, ce reprezintă una din manifestările umane. Folosirea pe scara largă a tehnologiei informaţiei şi comunicaţiilor a dus la cibernetizarea câmpului de luptă şi schimbarea filozofiei de ducere a acţiunilor de luptă, luând naştere noi concepte care descriu mai bine noua realitate: războiul bazat pe reţea şi capabilităţile facilitate de reţea.*

Cuvinte-cheie: *război bazat pe reţea; capabilităţi; reţele informaţionale; tehnologia informaţiei şi comunicaţiilor; noi concepte.*

Abstract: *The last two decades mark out the humankind evolution toward the Information Age, a new stage of societal development where the modern society is affected, among other factors, by the explosive technological changes. Within the context, technology represents the main changing driver. To be more specific, small innovations appeared in the information technology and communications are considered to be responsible global transformations in the economy, politics or culture structure. This assertion also extends its validity over the military phenomenon, which is just another human behavior. The use on large scale of the information technology and communications led to a cybernetic battlefield and the change of the waging war philosophy, with the arising of new*

* Membru corespondent al Academiei Oamenilor de Ştiinţă din România, Secţia Ştiinţe Militare.

concepts that better describe the new reality: Network Centric Warfare, and Network Enabled Capabilities.

Keywords: *the network warfare; capabilities; information networks; the information technology and communications; new concepts.*

1. Introducere

Apreciem că fizionomia conflictelor sfârşitului de secol XX şi începutului de secol XXI s-a schimbat radical, complexul factorilor care o individualizează incluzând: situaţii politico-economice şi strategice de insecuritate aparte, noi scopuri politice şi strategice, noi obiective, forţe şi mijloace de acţiune specifice, o altă concepţie şi intensitate, o altă atitudine faţă de adversar, spaţii diferite de desfăşurare, o paletă foarte vastă de tipuri dominante de acţiuni şi moduri tot mai sofisticate şi neaşteptate de manifestare a violenţei. Lumea acestor conflicte este una a confruntărilor asimetrice.

Dintre principalele caracteristici ale conflictelor militare actuale şi viitoare fac parte din ce în ce mai mult şi următoarele[1]:

- cauzalitatea complexă care rezultă din incompatibilităţile existente dintre sistemele politice dictatoriale sau autocrate şi cele democratice;
- amprenta pusă asupra noilor conflicte militare de decalaje imense dintre lumea bogată şi lumea săracă, dintre civilizaţia înaltei tehnologii şi civilizaţiile tradiţionale, diversificate, cu tradiţii, obiceiuri şi valori ancestrale;
- efectul tehnologic dat de diferenţele tehnologice;
- intensitatea diferită de la violenţa extremă a atentatelor teroriste la cele de îndiguire, de dominare, sau la cele de impunere a unui anumit tip de comportament;
- permanenta ameninţare nucleară, chimică, biologică şi radiologică;
- disimetria şi asimetria;
- omniprezenţa binomului acţiune – reacţie;
- prevenţia şi caracterul primitiv sau represiv;
- implicarea unui nou tip de binom terorism – antiterorism;
- caracterul în mozaic;
- imprevizibilitatea.

Acestor caracteristici li se mai adaugă şi altele, cum ar fi flexibilitatea şi confuzia, caracterul indirect, extremismul politic şi religios. Tipologia războiului este foarte variată, dar când vorbim de dimensiunea conflictualităţii, trebuie să ne referim

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

doar la trei tipuri de războaie, şi anume: război asimetric; război cognitiv; război bazat pe informaţie şi tehnologie de vârf (război bazat pe reţea).

Principiile esenţiale ale războiului erei informaţionale sunt:

- superioritatea informaţională;
- accesul comun la un sistem de informare de înaltă calitate;
- autosincronizarea dinamică – creşte libertatea structurilor operaţionale mici;
- forţe dispersate şi operaţii discontinue;
- forţe flexibile – trecerea cu uşurinţă de la o abordare pe masarea forţelor la una pe realizarea efectelor dorite;
- utilizarea pe scară largă a senzorilor asigură un nivel de informare superior;
- niveluri ale războiului şi operaţii comprimate care conduc la desfăşurarea cu preponderenţă a operaţiilor întrunite;
- viteza crescută a actului de comandă;
- dominaţia în spectrul complet – abilitatea forţelor de a acţiona singure sau împreună cu aliaţii pentru a înfrânge orice adversar sau de a controla sau stăpâni orice situaţie, de-a lungul întregului spectru al operaţiilor militare[2] .

Operaţiile informaţionale reprezintă întrebuinţarea integrată a acţiunilor de război electronic, a operaţiilor psihologice, a inducerii în eroare, a securităţii operaţiilor, a operaţiilor de comandă-control, a operaţiilor „supremaţia informaţiilor", a acţiunilor psihologice, a acţiunilor *hackerilor*, a acţiunilor informaţiilor economice şi a celor din spaţiul virtual[3]:

- operaţii de comandă-control – neutralizează comanda şi sistemele comandă-control ale adversarului; acestea cuprind integrarea operaţiilor psihologice, a inducerii în eroare, a securităţii operaţiilor, a războiului electronic şi a acţiunilor de distrugere fizică;
- operaţii „supremaţia informaţiilor" – proiectarea, protecţia şi anihilarea sistemelor care conţin suficiente cunoştinţe pentru a domina un spaţiu de conflict;
- operaţii electronice – tehnica de cercetare, neutralizare şi distrugere a sistemelor electronice care generează sau transportă informaţii, precum şi tehnici criptografice;

[2] Cf. *Joint Vision 2020,* Department of Defence, Washington D.C., 2000, p. 4.
[3] Cf. Topor, S., *Războiul informaţional,* Editura Universităţii Naţionale de Apărare, Bucureşti, 2005, pp. 25-27.

- operaţii psihologice – informaţia este utilizată pentru a modifica atitudinile şi opţiunile amicilor, neutrilor şi adversarilor;

- acţiuni ale *hackerilor* (pirateria software) – sistemele de calcul fac obiectul atacurilor active şi pasive cu *software* distructiv;

- acţiuni ale informaţiilor economice – blocarea sau canalizarea informaţiilor cu scopul de a obţine supremaţia economică;

- acţiuni în spaţiul de luptă al realităţii virtuale – un punct de acumulare al cercetărilor fundamentale şi tehnologice, al jocurilor de război şi al scenariilor futuriste.

Operaţiile informaţionale ofensive urmăresc neutralizarea personalităţilor sistemelor şi acţiunilor info ale adversarilor, iar cele defensive apărarea elementelor proprii faţă de acţiunile similare ale adversarilor.

Una dintre formele moderne de ducere a acţiunilor de luptă este războiul bazat pe reţea, care este un concept nou, de avangardă conflictuală informaţională şi tehnologică, cu desfăşurări globale, accesibil, deocamdată, numai entităţilor care dispun de sisteme performante de analiză şi cunoaştere, de tehnologii avansate de ultimă generaţie, de tehnologia informaţiei şi comunicaţiilor şi de structurile tehnice de sprijin şi software necesare acestora.

Extras din contextul dimensiunii conflictualităţii, războiul bazat pe reţea poate fi privit din cel puţin trei puncte de vedere:

- război de teatru, reprezentând o confruntare între două sau mai multe entităţi înarmate, într-un teatru de operaţii bine definit ca arie geografică şi ca filozofie şi praxiologie a acţiunilor concrete, ceea ce-l duce în spaţiul asimetric;

- război extins şi în alte domenii decât cele specifice luptei armate, în spaţiul cibernetic, media, economic şi financiar;

- război în teatrul conceptelor, care are ca obiectiv dominanţa în spaţiul cunoaşterii, fundamentarea ştiinţifică a unor sisteme de acţiune şi de reacţie ce permit utilizarea inteligentă şi eficace a forţelor şi mijloacelor existente şi crearea altora noi, mai performante, mai greu de descoperit şi de identificat.

Conceptul şi materializarea războiului bazat pe reţea aparţin ţărilor care dispun de tehnologie de înalt nivel şi tehnologia informaţiei şi comunicaţiilor, îndeosebi SUA, care este de fapt şi singura naţiune care le-a aplicat cu succes, într-o confruntare militară directă, cea din Irak.

Acest concept conţine şase capacităţi esenţiale[4]:

- capacitatea de a realiza şi folosi reţele reale şi virtuale şi de a le echipa cu sisteme C4ISR (similare) dotate cu echipamente şi produse software necesare;
- capacitatea de a construi baze de date şi cunoştinţe corespunzătoare;
- abilitatea de a construi forţe rapide şi flexibile, îndeosebi expediţionare, interoperabile;
- capacitatea de a realiza şi conecta sisteme de arme;
- capacitatea de proiecţie a forţelor şi mijloacelor;
- o capacitate logistică în reţea.

Chiar dacă în Irak războiul bazat pe reţea s-a dovedit extrem de eficient pe timpul ducerii luptei, acesta a avut şi are anumite limite în operaţiile postrăzboi. În aceste condiţii, războiul bazat pe reţea, deşi tinde să domine spaţiul luptei (în general pe cel al confruntărilor armate), nu se află la îndemâna oricui şi, după toate probabilităţile, nu va reuşi, în primele două decenii ale secolului XXI, să-şi execute funcţiile principale pentru care a fost creat decât într-o dinamică prevăzută cu un grad ridicat de certitudine, adică în războiul disproporţionat. Acest război nu este de tip haotic, ci unul care, prin desfăşurarea rapidă şi cu final previzibil, poate produce haos, întrucât disproporţionalitatea creează probleme destul de grave în dinamica imediată politică, economică, socială, informaţională şi militară.

2. Utilizarea sistemelor C4ISR în condiţiile noilor concepte operaţionale de război bazat pe reţea şi capabilităţi NATO facilitate de reţea

Conceptul de război bazat pe reţea descrie combinaţia strategiilor, tacticilor, tehnicilor şi procedurilor organizaţiilor pe care o forţă bazată pe reţea le poate angaja, pentru crearea unui avantaj decisiv în luptă[5]. Dacă acest concept se ancorează strict în realitatea forţelor militare americane, urmaşul său, capabilitatea NATO facilitată de reţea (NNEC), a extins teoria la nivelul întregii Alianţe Nord-Atlantice. Capabilitatea facilitată de reţea este abilitatea cognitivă şi tehnică a Alianţei de a conduce componentele diferite ale mediului operaţional, de la nivelul strategic, inclusiv Comandamentul NATO, până jos la nivelul tactic, printr-o infrastructură informaţională şi de reţea unică, integrată”[6].

---

[4] Cf. Frunzeti, T., Mureşan, M., Văduva, Gh., *Război şi haos*, Editura Centrului Tehnic-Editorial al Armatei, Bucureşti, 2009, pp.35-36.

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

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

Obiectivul aplicării unor noi concepte, precum războiul bazat pe reţea şi capabilităţi NATO facilitate de reţea, în planificarea, organizarea şi ducerea acţiunilor de luptă îl constituie capacitatea de a oferi tuturor liderilor de la toate nivelurile subordonate informaţiile aproape în timp real care le vor permite să înţeleagă situaţia tactică şi să acţioneze în conformitate cu intenţia comandantului. Această capacitate crescută de conducere generează noi provocări operaţionale. În timp ce subordonaţii au acces mai larg la situaţia tactică, comandanţii de la niveluri mai înalte au acces la planuri tactice foarte detaliate. Aceştia din urmă nu trebuie să cedeze tentaţiei de a conduce acţiuni militare minore de la nivelul subordonaţilor, deoarece intenţia lor ar putea reduce beneficiile sistemelor informatice moderne şi înţelegerea situaţiei pe care ei o sprijină. Prin urmare, este necesar să se dezvolte lideri puternici la toate nivelurile şi să se creeze premisa că încrederea şi coeziunea forţelor sunt bazate pe echipamente şi sisteme complexe şi combinate de tipul C4ISR, şi sunt materializate printr-o instruire realistă, exerciţii şi aplicaţii.

O forţă robustă, puternic conectată în reţea îmbunătăţeşte schimbul de informaţii, colaborarea, calitatea informaţiilor şi cunoaşterea situaţiei care generează o creştere însemnată a eficacităţii misiunii. S-a dovedit practic că reţelele informaţionale au un impact benefic asupra puterii combative, sincronizării în spaţiul de luptă, personalului din statele majore şi factorilor de decizie, reducerii pierderilor, creşterii agilităţii forţei şi tempoului operaţional.

Noii senzori, conectivitatea extinsă şi noile sisteme informaţionale contribuie substanţial la eficienţa acţiunilor de luptă ale forţelor. Distribuţia informaţiilor a crescut gradul de cunoaştere a situaţiei, care a îmbunătăţit cunoştinţele despre spaţiul de luptă şi a crescut atât viteza de manevră cât şi precizia focului. Conectarea extinsă permite forţelor să ducă acţiuni de luptă pe spaţii mai largi şi pe distanţe mai mari decât în trecut. Disponibilitatea şi fiabilitatea informaţiilor permit reorganizarea rapidă a sarcinilor şi integrarea completă a unităţilor nou sosite în teatrul de operaţii. Nivelul de dezvoltare a reţelelor fac ca forţele dispersate să fie corelate şi sincronizate în timp şi scop.

Comanda forţelor luptătoare este facilitată de reţea şi este caracterizată de distribuirea şi înţelegerea corectă a informaţiilor şi intenţiei comandantului, de un înalt grad de sincronizare a acţiunilor de luptă şi timp mai scurt de luare a deciziilor care duc la creşterea eficienţei focului şi a vitezei de manevră, tot acest proces reflectând, de fapt, principiile războiului bazat pe reţea[7]. Figura 1 prezintă în detaliu acest proces în contextul organizaţional facilitat de reţea.

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

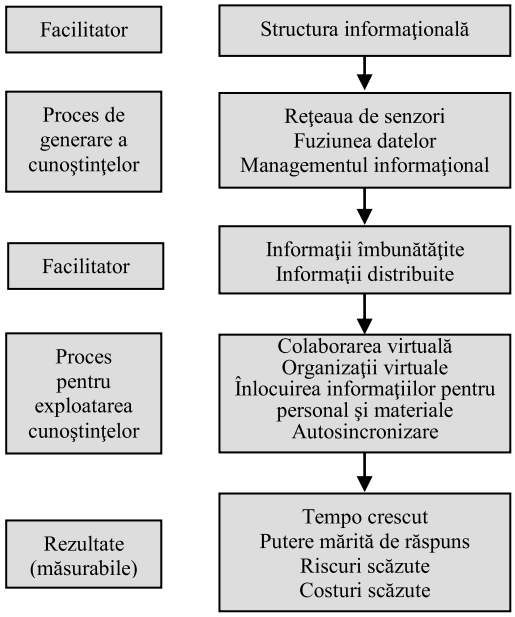

Figura 1. *Comanda forţelor luptătoare facilitată de reţea*

În prezent, există o tendinţă generalizată către o utilizare extinsă a tehnologiei informaţiei şi a comunicaţiilor în sistemele de apărare cu scopul de a dezvolta capabilităţile operaţionale cu costuri minime. În cele mai multe cazuri, intenţia principală este orientarea către lucrul în reţea, semnificând constituirea reţelelor de surse de informaţii, executanţi, comandanţi etc. Această dezvoltare are avantajul utilizării marilor evoluţii din domeniul tehnologiei informaţiei şi comunicaţiilor. Concepte precum războiul bazat pe reţea şi NNEC sunt desemnate să dezvolte şi să extindă capacităţi importante, precum: culegerea, prelucrarea şi diseminarea informaţiilor; calitatea deciziei şi eficienţa comenzii; cooperarea între structuri diferite şi între niveluri diferite ale aceleiaşi structuri; flexibilitatea utilizării unităţilor şi sistemelor de apărare[8]. Aceste noi concepte impun metode perfecţionate sau chiar metode noi de conducere a operaţiilor. Asta înseamnă că introducerea unor noi capabilităţi poate conduce la transformări profunde în organizarea apărării, privind

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

atât utilizarea sistemelor tehnice, cât şi tactica şi instruirea personalului. Dezvoltarea conceptelor coincide, totodată, cu eforturile de adaptare la situaţia strategică politică globală în era de după Războiul Rece, cu ameninţările sale de securitate fragmentate şi uneori neclare. Unul dintre elementele principale impuse de conceptele *război bazat pe reţea* şi *NNEC* este realizarea interoperabilităţii. Interoperabilitatea este un procedeu prin care se întăreşte atât eficienţa şi eficacitatea forţelor multinaţionale sau întrunite, cât şi capabilităţile necesare pentru întreaga gamă de operaţii ale Alianţei. Interoperabilitatea este un facilitator esenţial şi un multiplicator important al forţei[9]. Pentru a înţelege mai bine cerinţele impuse sistemelor C4ISR, pot fi concepute mai multe scenarii operaţionale pentru operaţii sau managementul crizelor, pe baza cărora se pot observa nevoile şi cerinţele informaţionale majore. Cerinţele informaţionale includ date, comunicaţii, capabilităţi şi instrumente de colaborare care facilitează succesul în oricare dintre scenarii. Relaţia dintre scenariile operaţionale şi cerinţele informaţionale impuse sistemelor C4ISR poate fi reprezentată ca în figura 2[10].

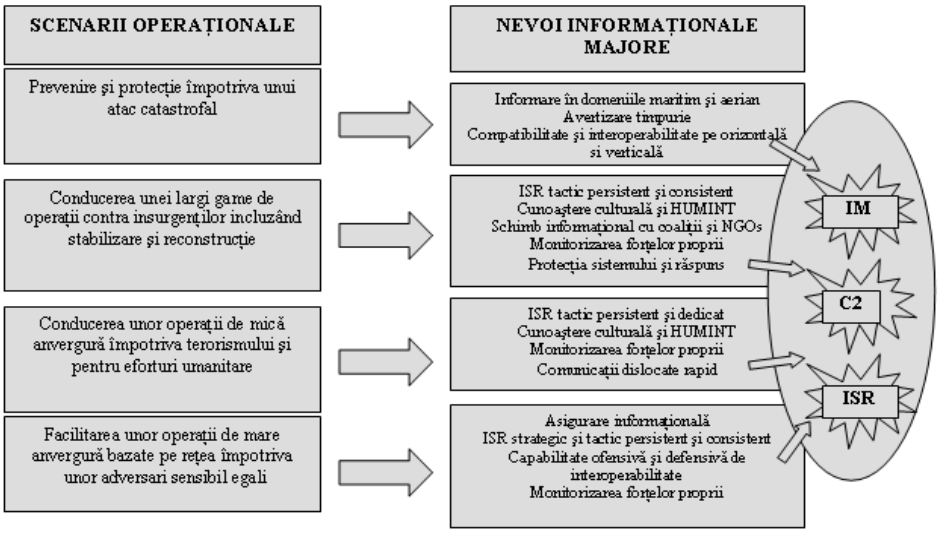

Figura 2. *Relaţia dintre scenariile operaţionale şi cerinţele informaţionale*

[9] *Enhancing Inteoperability,* Executive Working Group, Brussels, 2008, p.1-1.
[10] *Defense Science Board, Summer Study on Information Management for Net-Centric Operations*, *Vol. II*, The Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington, D.C., 2006, p. 10.

Chiar dacă din examinarea scenariilor se observă o anumită linie comună, acestea necesită anumite nevoi informaţionale majore specifice din care, în final, rezultă trei zone sau domenii specifice, astfel: managementul informaţional (IM); capabilitatea informaţională de comandă şi control (C2); informaţii, supraveghere şi recunoaştere (ISR). Luate ca un întreg, cele trei domenii combinate formează o aşa numită capabilitate informaţională pentru luptă/operaţie.

3. Implicaţiile războiului bazat pe reţea şi ale capabilităţilor NATO bazate pe reţea asupra reţelelor informaţionale de tipul C4ISR

Un specific al operaţiunilor militare ale secolului XXI îl reprezintă creşterea continuă a complexităţii, datorită îngemănării nivelurilor strategice, operative şi tactice, a întrepătrunderii obiectivelor militare şi civile, precum şi datorită realizării obiectivelor în comun cu aliaţii. Din ce în ce mai mult, comandanţii militari sunt puşi în faţa problemei privind concilierea modului tradiţional de ducere a operaţiilor militare cu obiectivele misiunii de ansamblu şi ale politicii naţionale.

Fenomenele de globalizare, dezvoltările tehnologice şi ritmul de tranziţie la era informaţională afectează profund mediul social, politic şi de securitate şi, implicit, abilitatea NATO de a răspunde noilor ameninţări, solicitând noi strategii de descurajare, de prevenire şi de preîntâmpinare a atacurilor teroriste, cu reformulări în aplicarea adecvată a puterii civile şi militare, în cadrul operaţiilor a căror abordare este bazată pe efecte.

Acest gen de argumente impun transformarea Alianţei şi a membrilor săi deopotrivă prin perfecţionarea proceselor decizionale bazate pe realizarea superiorităţii informaţionale şi a unor capabilităţi facilitate de reţea. În acest mod se urmăreşte o tot mai profundă integrare a instrumentelor militare şi politice, adoptarea unor noi metode şi construcţii organizaţionale capabile să genereze rezultate rapide, decisive, la nivel tactic, operativ şi strategic în afara zonelor tradiţionale de responsabilitate. Redimensionarea procesului de elaborare a deciziei, pe baza superiorităţii informaţionale şi implementării conceptelor de război bazat pe reţea şi operaţii bazate pe efecte prin capabilităţi facilitate de reţea, reprezintă elemente esenţiale ale transformării armatelor, sistemelor informaţionale revenindu-le un rol decisiv. Cadrul general al transformării Alianţei este prezentat în figura 3.

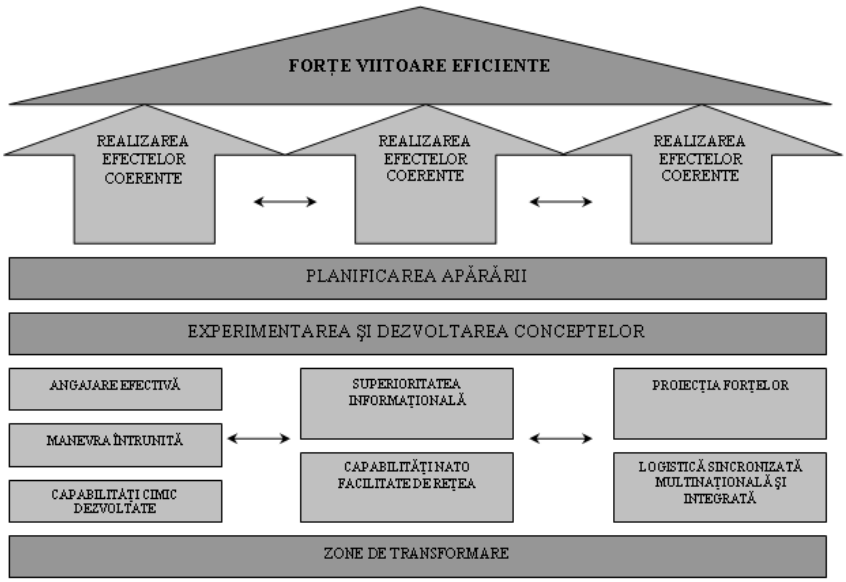

Figura 3. *Operaţii bazate pe efecte*

În plan militar, acest deziderat se asigură prin dezvoltarea potenţialului sistemelor C4ISR ce înglobează coerent elementele implicate în interconectarea senzorilor (surselor de informaţii), executanţilor/sistemelor de arme (elementelor operaţionale) şi a factorilor de decizie, împreună asigurând dezvoltarea unor capabilităţi operaţionale centrate pe reţea[11] şi bazate pe efecte. În acest mod se optimizează desfăşurarea şi susţinerea întrunită a forţelor prin asigurarea informaţiilor care influenţează direct puterea de luptă şi eficacitatea misiunii.

Spaţiul de luptă cibernetizat al viitorului va include elemente ale conceptelor strategice ale războiului bazat pe reţea şi NNEC, care, pe de o parte, vor transforma informaţia în factor de putere şi va mări capacitatea de răspuns şi precizia de angajare a forţelor, iar pe de altă parte, va asimila în viteză toate inovaţiile conceptuale şi tehnologice din domeniul militar. Este necesar de subliniat faptul că, dacă conflictele noului mileniu vor fi purtate preponderent într-un mediu de coaliţie sau alianţă, lucrul cel mai dificil îl va reprezenta înlăturarea decalajului tehnologic dintre statele participante.

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

Cadrul conceptual al războiului bazat pe reţea sau NNEC şi modul în care este concepută integrarea capabilităţilor de colectare a datelor, de elaborare a deciziei şi transmitere a acesteia la elementele operaţionale se prezintă sintetic în figura 4.

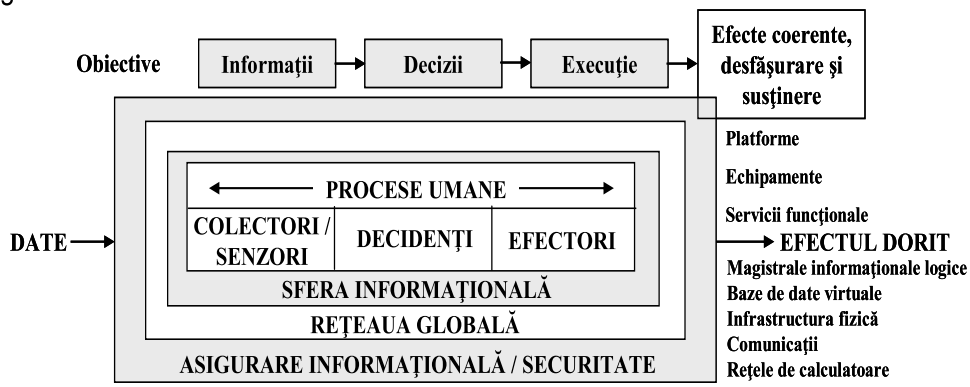

Figura 4. *Cadrul conceptual al războiului bazat pe reţea şi al NNEC*

Integrarea acestor dimensiuni (elemente) permite structurilor NATO şi naţiunilor membre ale NATO să îşi creeze o imagine comună asupra spaţiului de luptă şi, drept consecinţă, să crească nivelul de cunoaştere al acestuia şi eficienţa acţiunilor comune. Principiul de realizare a imaginii operaţionale comune (COP) este prezentat în figura 5.

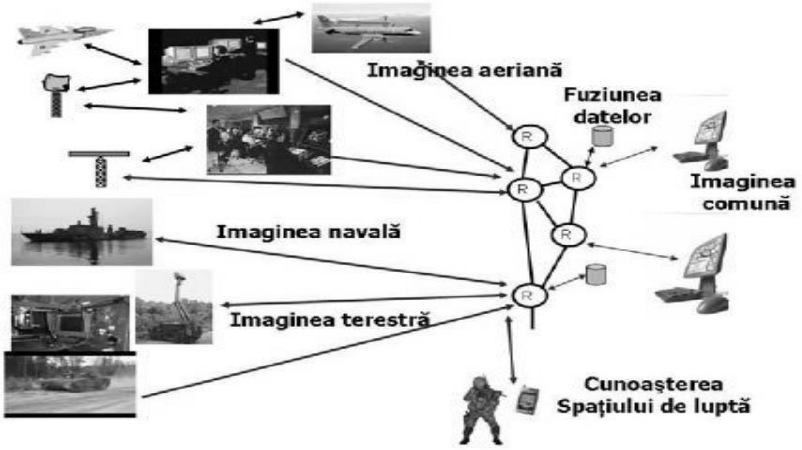

Figura 5. *Principiul de realizare a imaginii operaţionale comune*

Concepte precum războiul bazat pe reţea şi NNEC vor permite trupelor să fie în măsură să acţioneze în cadrul structurilor din care fac parte sau într-o coaliţie de forţe într-un mod care va trebui redefinit în conceptele actuale privind operaţiile militare şi arhitectura sistemelor informaţionale. Realizarea conducerii forţelor impune existenţa unor sisteme C4ISR integrate la toate eşaloanele. Sistemele C4ISR trebuie să asigure, în condiţiile dinamismului deosebit al acţiunilor militare şi al fluidităţii dispozitivelor, acoperirea cu posibilităţi de conducere a întregului spaţiu de responsabilitate, a realizării comenzii şi controlului în timp real al forţelor şi mijloacelor la dispoziţie, precum şi sprijinul logistic eficient. Implementarea conceptelor războiul bazat pe reţea şi NNEC este văzută ca un multiplicator al forţei, ca un generator al superiorităţii informaţionale şi decizionale, permiţând creşterea substanţială a eficacităţii misiunilor.

4. Examinarea dezvoltării capabilităţilor C4ISR din Armata României pentru a fi în concordanţă cu mediul NATO NEC

În acest moment, fenomenul cel mai important în zona militară îl constituie transformarea. Acesta este un cuvânt cheie în NATO şi, deci, în acelaşi timp, şi în Armata României. În esenţă, fenomenul transformării se referă la:

- reconsiderarea naturii operaţiunilor militare, precum şi reconsiderarea doctrinelor, a competenţelor şi a dotării materiale.
- influenţa transformării asupra sistemelor C4ISR, unde pot fi întâlnite următoarele două cadre generale, şi anume capabilităţile facilitate pe reţea şi Infrastructura Naţională Critică (Critical National Infrastructure – CNI)

Scopul principal al celor două cadre îl constituie obţinerea superiorităţii informaţionale, cel din urmă fiind unul dintre pilonii de bază ai conceptului NATO NEC.

Capabilităţile facilitate de reţea permit un sprijin mai rapid şi mai bun al întregului spectru de operaţii. Principalele rezultate aşteptate sunt:

- superioritatea informaţională şi decizională (primul obiectiv al NEC);
- asigurarea coerenţei informaţionale şi interoperabilităţii tuturor utilizatorilor;
- creşterea receptivităţii;
- creşterea flexibilităţii.

Aceste rezultate devin posibile doar în cadrul unei Infrastructuri Informaţionale şi de Reţele (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:

- reţele inteligente;
- aplicaţii de gestiune a informaţiilor incluse în nodurile reţelei;
- distribuirea de servicii de bandă largă;
- garantarea unei anumite calităţi a serviciilor (QoS) punct la punct;
- soluţii de securitate distribuite uniform în întreg sistemul;
- mobilitatea utilizatorilor.

Scopul conceptelor NEC îl constituie crearea de reţele inteligente, capabile să contribuie operativ la gestiunea şi diseminarea informaţiilor. Acest scop implică existenţa aplicaţiilor de gestiune a informaţiilor incluse în nodurile reţelei, implementarea de aplicaţii de comandă-control şi administrative (Intranet), utilizarea pe scară largă de instrumente grafice şi imagistice.

Pentru aceste aplicaţii 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 soluţii de securitate distribuite uniform în sistem pentru a deservi diferite comunităţi de utilizatori (securitatea informaţiilor, autentificarea şi înregistrarea utilizatorilor etc.).

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

Luând în considerare cel de-al doilea cadru menţionat, este necesar să subliniem că acesta a început să aibă consistenţă 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);
- 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 – Reţeaua Militară Naţională de

Comunicaţii (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.

Reţeaua Radio Operativă de Nivel Strategic (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 ale armatei (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 Sistemul de Comandă-Control Aerian Naţional (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, Sistemul Complex de Observare Maritimă (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 Învăţământului Militar (SIMIL);
  - Sistemul Logistic Integrat (AILS).

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

5. Creşterea capabilităţilor de apărare ale Armatei României prin implementarea de tehnologii integratoare, pentru asigurarea de capabilităţi multifuncţionale şi flexibile

Necesităţile de ordin operaţional care pot fi definite pentru o Reţea Comună pentru Armata României sunt: accesul la reţea pentru satisfacerea de criterii cum ar fi flexibilitatea, simplitatea şi securitatea, pe teritoriul naţional sau în afara acestuia, pentru a permite accesul utilizatorilor care exploatează reţeaua:

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

Una dintre cerinţele tehnice esenţiale o constituie realizarea compatibilităţii cu cele mai importante standarde din domeniu, pentru a asigura interoperabilitatea. De asemenea, topologia reţelei va trebui să permită flexibilitate, viabilitate şi servicii corespunzătoare nevoilor utilizatorilor. Totodată, reţeaua trebuie să ofere suport pentru diferite servicii/aplicaţii/funcţiuni şi fluxurile informaţionale specifice, care să permită operaţiuni autonome şi independente, precum şi integrarea şi schimbul de date la cererea serviciilor şi aplicaţiilor specifice.

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

Reţeaua comună pentru Armata României va oferi suport pentru:

- servicii de interconectare între reţele;
- servicii de bază (core services);
- servicii funcţionale (functional areas services), cum ar fi pentru personal, cercetare, operaţii, 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 reţea, într-o perioadă de timp acceptabilă. Având acest scop, trebuie gândite acţiuni de implementare a unei reţele comune prin exploatarea achiziţiilor 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 cerinţe:

- suport pentru servicii de bandă largă (servicii integrate multimedia);
- optimizarea benzii de transmisie avute la dispoziţie;
- dezvoltarea/implementarea de reţele de acces;
- creşterea securităţii reţelei 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 acţiunilor din afara teritoriului naţional prin comunicaţii satelitare şi conectivităţi de mare capacitate către mijloacele mobile;
- mărirea interoperabilităţii între RMNC şi NGCS;
- creşterea funcţiunilor de automatizare şi control pentru înlocuirea forţei de muncă.

Aceste cerinţe conduc la realizarea obiectivelor finale:

- construirea unei reţele sigure şi cu o viabilitate ridicată;
- integrarea totală a componentelor reţelei atât strategice, cât şi tactice;
- gândirea arhitecturii reţelei şi tehnologiilor adoptate pentru a optimiza capabilităţile privind eficienţa şi managementul;
- evoluţia serviciilor.

Pornind de la situaţia actuală, se poate defini un plan secvenţial al acţiunilor care pot conduce la realizarea unei reţele comune pentru Armata României. Serviciile furnizate de reţea sunt împărţite în două categorii principale, având la bază împărţirea Bi-Strategic Command Automated Information System: servicii de bază (core services) şi servicii funcţionale (functional area services). Serviciile de bază

sunt destul de bine dezvoltate în cadrul reţelei, problema principală reprezentând-o, în opinia noastră, diseminarea acestor servicii pentru toţi utilizatorii.

În zona serviciilor funcţionale suntem în faza în care Armata României investeşte efort şi fonduri. Aceste activităţi sunt conduse de necesitatea obţinerii unui schimb de informaţii 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 naţionali, a utilizatorilor NATO, a celor din diverse coaliţii şi a participanţilor la misiuni externe.

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

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

Pentru perioada imediat următoare, ambiţiile sunt mari. Datorită cerinţelor de capacităţi 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 reţele zonale de fibră optică de mare capacitate. Pentru a mări capabilităţile de procesare, vor fi introduse comutatoare multiprotocol şi multiservicii.

Totodată, efortul va fi axat pe:

- integrarea sistemelor existente prin porţi specifice, care nu vor limita performanţele;
- utilizarea de staţii radio definite prin software pentru toate serviciile şi toate tipurile de comunicaţii; staţiile radio cu astfel de capabilităţi au început să fie deja utilizate;
- realizarea unui sistem de management al reţelei de ansamblu;
- în zona INFOSEC, protejarea informaţiilor şi a sistemului, criptoarele IP urmând a fi utilizate ca soluţie standardizată;
- integrarea senzorilor şi utilizarea senzorilor inteligenţi.

6. Concluzii

Ministerul Apărării Naţionale a început diferite programe de modernizare, multe dintre ele la eşaloane inferioare datorită nivelului de angajare din momentul iniţierii 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, apreciem că abordarea arhitecturală recomandată în NATO C3 Systems Architecture Framework este soluţia cea mai bună. Ca tehnologie de bază este adoptată digitizarea spaţiului de luptă, iar ca idee de bază, conceptul C4ISTAR. Nu mai puţin importantă este coordonarea cu toate programele cu care interacţionează.

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.

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, în cadrul Alianţei Nord-Atlantice sau cu structurile militare ale statelor membre ale Uniunii Europene.

BIBLIOGRAFIE

Frunzeti, T., Mureşan, M., Văduva, Gh., *Război şi haos*, Editura Centrului Tehnic - Editorial al Armatei, Bucureşti, 2009.

Joint Vision 2020, Department of Defence, Washington D.C., 2000.

Topor, S., *Războiul informaţional,* Editura Universităţii Naţionale de Apărare, Bucureşti, 2005.

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

NNEC Vision and Concept, MCM-0032-2006, Allied Command Transformation, Norfolk, Virginia, USA, 2006.

Cammomns, D, Tisserand, J.B, Williams, D.E., Seize, A., Linsay, D., *Network Centric Warfare Case Study,* Volume I – Operations, V Corps and the 3rd Infantry Division (Mechanized), 2003.

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

Enhancing Inteoperability, Executive Working Group, Brussels, 2008.

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

NATO Network Enabled Capability Feasibility Study, v 2.0, Executive Summary, NC3A, Brussels, 2005.