UNIVERSITATEA NAȚIONALĂ DE APĂRARE

Centrul de Studii Strategice de Securitate şi Apărare

RĂZBOIUL BAZAT PE REȚEA ŞI VIITORUL ACȚIUNILOR MILITARE

Lucrări prezentate în cadrul seminarului ştiinţific
organizat de Centrul de Studii Strategice de Apărare şi Securitate
26 mai 2005

Editura Universităţii Naţionale de Apărare
Bucureşti, 2005

Coordonator
Dr. CONSTANTIN MOŞTOFLEI

Descrierea CIP a Bibliotecii Naţionale a României
UNIVERSITATEA NAȚIONALĂ DE APĂRARE (Bucureşti).
CENTRUL DE STUDII STRATEGICE DE APĂRARE ŞI SECURITATE
Războiul bazat pe reţea şi viitorul acţiunilor militare/ Universitatea Naţională de Apărare. Centrul de Studii Strategice de Apărare şi Securitate – Bucureşti: Editura Universităţii Naţionale de Apărare, 2005
Bibliogr.
ISBN 973-663-220-2

355.4

Referenţi ştiinţifici:
Dr. NICOLAE DOLGHIN
Dr. GHEORGHE VĂDUVA
VASILE POPA

ISBN 973-663-220-2

CUPRINS

CUVÂNT DE DESCHIDERE

General prof. univ.dr. MIRCEA MUREŞAN,
comandantul (rectorul) Universității Naționale de Apărare

Doamnelor şi domnilor,

Am onoarea să vă salut. Vă rog să-mi permiteți să vă urez Bine ați venit în Universitatea Națională de Apărare, la această manifestare ştiințifică a CSSAS, devenită deja tradițională!

După cum, probabil, ați remarcat, Universitatea Națională de Apărare şi, în acest cadru, Centrul ei de Studii Strategice de Apărare şi Securitate desfăşoară, în fiecare an, seminarii şi sesiuni de comunicări ştiințifice care fac notă distinctă, prin problematica abordată, participare şi mod de abordare, în peisajul ştiințific al Armatei şi al țării. În ultimii ani, s-au editat, în cadrul Universității, zeci de volume, s-au prezentat sute de comunicări valoroase, s-au obținut premii şi, ceea ce este, poate, cel mai important, s-a recreat şi conturat puternic o adevărată şcoală strategică românească, racordată la şcoala strategică de securitate şi apărare a Alianței Nord-Atlantice şi la cea a Uniunii Europene. România se află, deopotrivă, în miezul fierbinte al dezbaterii strategice teoretice şi în cel al punerii în aplicare, în teatrele de operații, acolo unde interesele României, ale Alianței şi ale Uniunii Europene o cer, a noilor principii ale angajării şi acțiunii combat şi non-combat.

Dar cea mai importantă şi cea mai dezbătută temă a ultimilor ani este cea a Războiului bazat pe Rețea. După cum bine ştiți, acum doi ani, Statul Major General, statele majore ale categoriilor de forțe, Universitatea Națională de Apărare, Centrul de Studii Strategice de Apărare şi Securitate, Agenția

de Cercetare pentru Tehnică şi Tehnologii Militare au elaborat, împreună, sub coordonarea CSSAS, primul studiu privind Războiul bazat pe Rețea, care a constituit şi un punct de plecare nu doar în studierea şi aprofundarea acestui nou concept, ci şi în începutul implementării lui în Armata României.

Din acel moment, preocupările teoretice şi practice pentru studierea, implementarea şi aplicarea Războiului bazat pe Rețea s-au intensificat. Numai în cadrul CSSAS, au apărut, în ultimii doi ani, două studii distincte pe această temă, respectiv, „Războiul bazat pe Rețea şi influența lui asupra strategiei militare" şi „Războiul bazat pe Rețea în fizionomia noilor conflicte militare". Au fost elaborate, desigur, şi alte lucrări valoroase pe această temă. Practic, nu există volum pe tema securității şi apărării care să nu trateze, într-o formă sau alta, şi problematica Războiului bazat pe Rețea.

În toată lumea, tema Războiului bazat pe Rețea este de mare actualitate. Cum bine se ştie, acest concept a fost creat, dezvoltat şi aplicat de Statele Unite ale Americii. El este un produs al revoluției în domeniul militar şi revoluționează complet arta militară. Intrăm, deci, într-o altă epocă în ceea ce priveşte tehnologia, fizionomia şi strategia războiului. La Washington, în fiecare ianuarie, se organizează ample activități pe această temă. Activități de acest fel se desfăşoară şi la Londra, la Stockholm, la Paris, la Berlin şi în alte capitale. Înalta tehnologie, tehnologia informației şi noul mediu strategic de securitate impun peste tot astfel de studii, experimente şi dezbateri pe tema Războiului bazat pe Rețea. Teoria are, de-acum, şi un suport practic extrem de bogat, întrucât, atât intervenția promptă în Afghanistan, la sfârşitul anului 2001 şi începutul anului 2002, cât şi acțiunea, îndeosebi a Statelor Unite, împotriva armatei lui Saddam Hussein din martie-aprilie 2003 au aplicat conceptul „Război bazat pe Rețea".

Valenţele şi implicaţiile acestui concept sunt numeroase. Ele continuă să fie studiate şi dezvoltate în întreaga lume, inclusiv în România. Organizarea acestui seminar se înscrie în acest demers. De altfel, nu a existat activitate ştiinţifică organizată în cadrul Universităţii Naţionale de Apărare care să nu trateze distinct şi profund şi problematica Războiului bazat pe Reţea.

Activitatea de astăzi finalizează numeroasele propuneri făcute în acest sens, dar ea rezultă şi dintr-o necesitate ştiinţifică foarte actuală şi se înscrie în acest flux care cuprinde cu rapiditate toate armatele moderne din lume. Pentru Universitatea Naţională de Apărare şi pentru Centrul ei de Studii Strategice de Apărare şi Securitate este o onoare să găzduiască o astfel de dezbatere care, sunt sigur, va deschide noi perspective aprofundării teoretice şi practice a acestui nou concept şi implementării lui în procesul de transformare a Armatei României.

Aşteptăm cu mult interes comunicările dumneavoastră.

Urez succes deplin lucrărilor seminarului!

RĂZBOIUL BAZAT PE REŢEA ŞI ACHIZIŢIILE DE VIITOARE CAPABILITĂŢI MILITARE

General de flotilă aeriană dr.ing. Ion-Eftimie SANDU
Colonel dr.ing. Cristian Mateescu

„Ca şi concept, NCW nu poate avea o definiţie precisă, pentru că definiţiile şi conceptele sunt ca şi materia şi anti-materia. Astfel, dacă un concept este definit, el nu mai poate fi deloc un concept.” (Viceamiral Arthur K. Cebrowski)

Astăzi, mulţi sunt de acord cu aprecierea că lumea este în mijlocul unei revoluţii în domeniul militar. Schimbările constau, în special din punct de vedere tehnologic, în progresele în tehnologia informaţională, care aduc câştiguri în comunicare, precizie şi letalitatea armelor convenţionale. Ca parte a acestei revoluţii, dezvoltarea NCW depinde de schimbările tehnologice, investiţii pentru reducerea decalajelor economice şi tehnologice, dezvoltarea sistemelor şi adaptarea abordărilor operaţionale pentru a profita de această nouă capacitate.

Odată cu intrarea în noul mileniu, domeniul militar a intrat la rândul său într-o nouă eră a războiului – o eră în care războiul este afectat de schimbările strategice ale mediului şi de schimbările rapide ale tehnologiei. Statele lumii experimentează tranziţia de la era industrială la era informaţională. Angajamentul total în războiul global împotriva terorismului, în noua eră a globalizării, precum şi experienţa câştigată în timpul operaţiunilor militare recente sau în desfăşurare au determinat tendinţa de orientare a forţelor armate spre războiul bazat pe reţea (Network Centric Warfare – NCW), ca element central al acestor eforturi.

Conceptul american porneşte de la câteva obiective şi concepte strategice prezentate în documentul american „Joint Vision 2020": superioritatea informaţională, decizia la nivel superior, manevra dominantă, precizia angajării, logistica focalizată şi protecţia la toate dimensiunile. El implică, în general, o nouă abordare privind îndeplinirea misiunilor, o nouă înţelegere asupra organizării şi interrelaţionării, precum şi asupra modului în care se achiziţionează şi se introduc în exploatare sistemele şi capabilităţile pe care le folosim.

Principalele dogme asupra NCW sunt următoarele:

- O forţă robustă interconectată în reţea îmbunătăţeşte distribuţia informaţiei.
- Distribuţia informaţiei întăreşte calitatea informaţiei şi asigură accesul la cunoaşterea situaţiei de luptă.
- Distribuţia situaţiei de luptă cunoscute asigură colaborarea şi autosincronizarea, dar şi măreşte gradul de susţinere şi viteza de comandă.
- Ca urmare, se obţine o creştere substanţială a eficacităţii in misiuni.

Războiul cuprinde, în general, caracteristici ale epocii sale. NCW continuă această tendinţă – este răspunsul atât la provocările, cât şi la oportunităţile create de epoca informaţională.

Ducerea războiului centrat pe reţele presupune, totodată, utilizarea reţelelor integrate de calculatoare şi de comunicaţii pentru comanda şi controlul acţiunilor militare în contextul mai larg al sistemelor de tip C4I (comandă, control, comunicaţii, calculatoare şi informaţii).

Această lucrare oferă o analiză a evoluţiei şi conţinutului conceptului NCW, a beneficiilor şi avantajelor în luptă pe care acesta le poate aduce. Sunt prezentate perspectivele şi impedimentele în implementarea conceptului, precum şi o privire de ansamblu asupra iniţiativelor naţionale

de dezvoltare şi implementare ale capabilităţilor centrate pe reţea.

Cu privire la războiul centrat pe reţea, vom sublinia că există o mulţime de elemente care trebuie integrate pentru a face capabilitatea centrată pe reţea să devină o realitate. Aceasta pentru că, prin natura sa, acest tip de capabilitate:

- Implică noi căi de gândire despre modul în care misiunile pot să fie îndeplinite.
- Schimbă responsabilităţile şi rolul organizaţiilor.
- Cere ca informaţia să fie distribuită în exteriorul comunităţii existente.
- Depinde, în parte, de dezvoltarea de noi tehnologii.
- Reclamă o mai bună înţelegere a modalităţilor de creare, diseminare şi exploatare a cunoştinţelor.
- Creează valoare prin noi modalităţi.

Potrivit autorilor concepţiei, pentru ca NCW să devină realitate, trebuie îndeplinite o serie de condiţii, care includ:

- O infrastructură robust interconectată, care să poată asigura distribuţia informaţiei şi colaborarea.
- O atmosferă sau un climat care să alimenteze creşterea inovaţională.
- O bază tehnologică corespunzătoare şi o înţelegere corectă a problematicii.
- O modalitate de analiză şi de evaluare a capabilităţilor NCW.

1. Conceptul NCW

Se spune că Network Centric Warfare este pentru război ceea ce comerţul electronic reprezintă pentru domeniul afacerilor.

În mod consecvent, termenii "Network Centric Operations" şi "NCW" sunt utilizaţi pentru a descrie tipuri

variate de operaţiuni militare, în aceeaşi manieră în care termenii de „afaceri electronice” şi „comerţ electronic” sunt utilizaţi pentru a descrie o largă clasă de activităţi comerciale, care sunt permise şi suportate de Internet.

Termenul 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[1]. Teoria NCW are aplicabilitate la toate nivelurile războiului – strategic, operaţional şi tactic – şi pe întreaga gamă a operaţiilor militare, de la operaţii combative majore la operaţii de menţinere a păcii.

O forţă bazată pe reţea, care conduce operaţii bazate pe reţea, este un element esenţial ce permite conducerea operaţiilor bazate pe rezultat. Operaţiile bazate pe rezultat (Effects-based Operations – EBO) sunt seturi de acţiuni direcţionate către modelarea comportamentului amicilor, neutrilor şi inamicilor în timp de pace, criză şi război.

Forţele armate ale multor state *se mişcă rapid* spre aria NCW şi dezvoltă capabilităţi proprii pentru a conduce operaţii bazate pe rezultat (EBO). Conducerea operaţiilor militare caută să obţină avantajul maxim derivat din puterea NCW. În acelaşi timp, trebuie subliniat faptul că inamicii şi potenţialii adversari, inclusiv organizaţiile internaţionale teroriste, pot căuta să obţină capabilităţi bazate pe reţea, în scopul utilizării acestora împotriva forţelor opozante, atunci când conduc operaţii de supraveghere sau de planificare, ori când realizează efectiv atacuri, fiind de aşteptat ca organizaţiile adversare/teroriste să analizeze şi să exploateze, la rândul lor, vulnerabilităţile şi slăbiciunile reţelei adversarului.

Cadrul conceptual al războiului bazat pe reţea cuprinde elementele implicate în legarea şi conectarea împreună a

[1] John J. GARSTKA, *Network Centric Warfare Offers Warfighting Advantage,* Signal, May 2003.

colectorilor, efectorilor şi decidenţilor pentru a dezvolta o capabilitate operaţională (figura nr. 1).

Componentele acestui concept sunt individul, informaţia şi reţeaua, entităţi care integrează capabilităţile colectorilor, decidenţilor şi efectorilor (figura nr.2).

Dimensiunea **individuală** cuprinde toate aspectele legate de factorul uman:

- la nivel de **indivizi** - recrutarea, selecţia, trecerea în rezervă, competenţele, conducerea, educaţia şi antrenamentul;
- **organizaţia** include structurile, responsabilităţile şi rolurile;
- **cultura** include barierele culturale, credinţa şi diferenţele care pot afecta percepţia/înţelegerea;
- **procesul de afaceri** include procedurile, acordurile politice, legislaţia şi doctrinele.

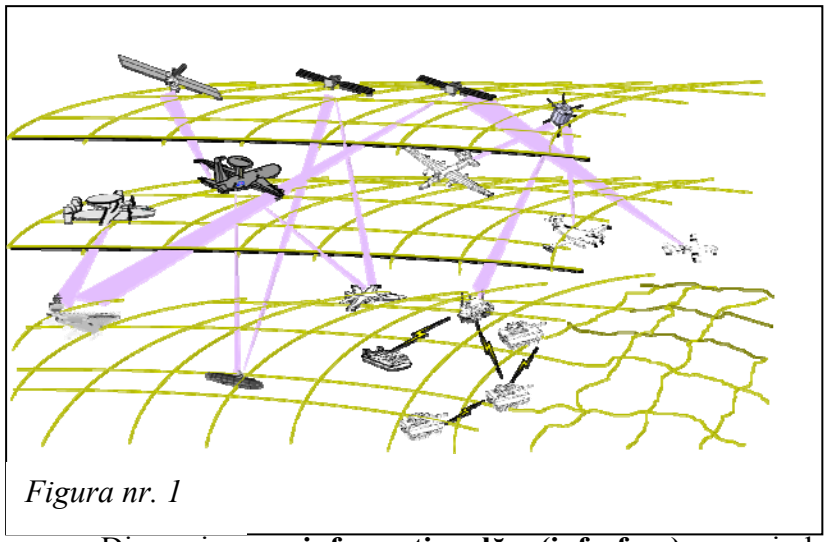


Figura nr. 1

Dimensiunea **informaţională (infosfera)** cuprinde aspectele referitoare la managementul informaţiei. Atributele acestei dimensiuni sunt:

- culegerea informațiilor şi punerea lor la dispoziția celor care au nevoie de ele;
- interpretarea şi translatarea datelor în formate comune;
- calitatea informației;
- prezentarea şi fuziunea informațiilor;
- asigurarea securității informațiilor;
- politici clare de management al informațiilor.

Figura nr. 1. Conceptul de război bazat pe rețea.

Dimensiunea rețea creează mediul pentru partajarea informațiilor şi are următoarele caracteristici:

- o rețea de rețele care se extinde la organizații naționale, internaționale şi nonguvernamentale;
- o lărgime de bandă care să satisfacă toate nevoile operațiilor militare;
- uşurință în desfăşurare şi reconfigurare;
- asigurarea securității datelor transportate.

Colectorii sunt reprezentați de multitudinea şi varietatea surselor de date: senzori tradiționali, servicii de informații, agenții etc.

Decidenții reprezintă colecția tuturor capabilităților de evaluare, predicție, simulare, planificare şi luare a deciziei. NCW asigură interfețele şi serviciile pentru extragerea informațiilor de la colectori, pentru a le fuziona, filtra şi prezenta într-o formă adecvată pentru luarea deciziei şi pentru a transmite **efectorilor** această decizie şi informația necesară pe o cale rapidă şi sigură.

NCW generează creşterea puterii de luptă, datorită următoarelor avantaje:

- prezența în rețea a senzorilor, decidenților şi combatanților;
- exploatarea în comun a situației (Common Operation Picture –COP);
- creşterea vitezei de comandă;
- creşterea ritmului operațiilor;

- creşterea letalității;
- creşterea ratei de supraviețuire şi a gradului de sincronizare a forțelor.

Se translatează, astfel, avantajul informațional în putere de luptă, prin realizarea legăturilor între forțele amice în câmpul de luptă, asigurându-se o partajare a situației şi luarea deciziilor mult mai rapid şi eficient, la toate nivelurile operațiilor militare, permițând astfel creşterea vitezei de execuție. Rețeaua este susținută de elementele de tehnologie a informației, dar este exploatată de operatori infanterişti, aviatori şi marinari, care sunt, în acelaşi timp, componente ale rețelei.

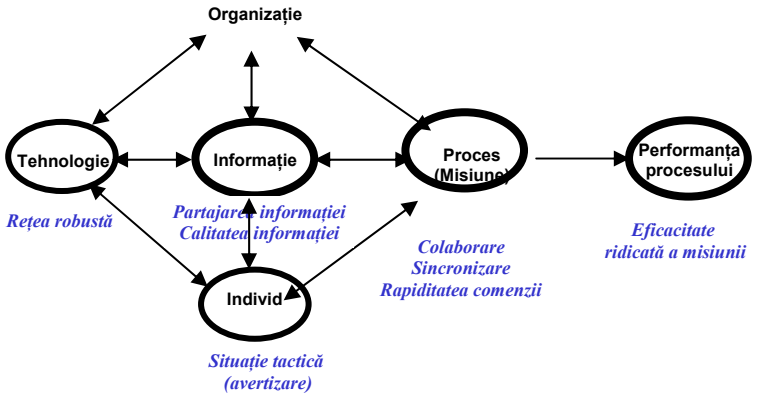


Figura nr. 2. Elementele componente ale conceptului NCW.

2. Particularități şi principiile NCW

Una dintre primele descrieri ale războiului bazat pe rețea a fost publicată în 1998, într-un articol din *US Naval Institute Proceedings*. Autorii compară impactul potențial al

NCW din zilele noastre cu impactul transformațional al conceptului francez "levee en masse" din timpul lui Napoleon. În Statele Unite ale Americii, conceptul NCW şi toate elementele revoluționare asociate în problemele militare se dezvoltă prin schimbările fundamentale ale societății. Acestea au fost dominate de evoluția economiei, tehnologiei informației şi proceselor de afaceri şi sunt corelate prin intermediul următoarelor elemente:

- schimbarea orientării de la platformă la rețea;
- schimbarea modului de privire a actorilor ca elemente independente şi vizualizarea acestora ca parte a unui ecosistem adaptabil continuu;
- importanța alegerilor alternativelor strategice, pentru adaptarea sau supraviețuirea în aceste ecosisteme schimbătoare[2].

Au fost identificate patru teze principale şi un set de principii pentru o forță bazată pe rețea. Împreună, aceste teze şi principii conțin nucleul NCW, ca o teorie a războiului în era informației:

- o forță robustă bazată pe rețea îmbunătățeşte partajarea informației;
- partajarea informației îmbunătățeşte calitatea informației şi a situației partajate;
- situația partajată permite colaborarea şi sincronizarea şi măreşte sprijinul şi viteza comenzii;
- creşterea considerabilă a eficienței misiunii.

Principiile care guvernează o forță bazată pe rețea sunt următoarele (figura nr. 3):

- lupta inițială pentru superioritate informațională;
- partajarea situației;

[2] Viceamiral Arthur K. CEBROWSKI, John J. GARSTKA, *Network Centric Warfare: Its origin and Future*, U.S. Naval Institute Proceedings Annapolis, Maryland, ianuarie 1998.

- rapiditatea elaborării comenzii şi luării deciziei;
- sincronizarea;
- forțe dispersate: operații discontinue;
- cercetare în profunzime, cu senzorii;
- modificarea rapidă a condițiilor inițiale;
- operații comprimate.

Aceste principii, care sunt încă în plină evoluție şi subiect pentru detalieri viitoare, ghidează aplicarea NCW ca teorie emergentă a războiului. În fapt, acestea constituie noile reguli pe baza cărora o forță bazată pe rețea se organizează, se instruieşte şi operează:

Lupta inițială pentru superioritatea informațională generează avantajul informațional, sporind precizia, acuratețea şi relevanța informației, prin:

- creşterea nevoii de informații a inamicului, prin reducerea capacității acestuia de a accesa informația şi creşterea gradului său de incertitudine;
- asigurarea accesului propriu la informație, prin intermediul unei forțe interoperabile, bazate pe rețea, şi protecția sistemelor de informații proprii, inclusiv a sistemelor de senzori;
- reducerea nevoii proprii de informații, în special ca volum, prin creşterea capacității proprii de a exploata toți colectorii.

Partajarea situației asigură translatarea informației şi cunoaşterii la un nivel comun de înțelegere pentru tot spectrul participanților la operații întrunite sau combinate şi ține cont de următoarele elemente:

- construirea unei rețele de rețele colaborative, populate şi actualizate cu date brute sau procesate de calitate, pentru a permite forțelor să construiască o situație partajată, relevantă pentru nevoile lor;

- utilizatorii informației trebuie să devină, de asemenea, distribuitori de informație, responsabili cu transmiterea fără întârziere a acesteia. Accesul la date trebuie să fie permis indiferent de locație;
- situația partajată de înaltă calitate necesită rețele și informații sigure și securizate.

Rapiditatea elaborării comenzii și luării deciziei oferă avantajul unei informații și îl transformă într-un avantaj decisiv prin crearea unor procese și proceduri altfel imposibile (cu menținerea unui risc prudent):

- prin inovație și adaptare la câmpul de luptă se reduce timpul de decizie, pentru a transforma avantajul informației într-o superioritate a deciziei;
- blochează progresiv opțiunile adversarului.

Sincronizarea crește posibilitatea forțelor din eșaloanele de nivel inferior de a opera aproape independent și de a se adapta singure, prin exploatarea situației partajate, și a intențiilor comandantului:

- creșterea valorii inițiativei subordonaților, pentru a produce o sporire semnificativă a vitezei operaționale;
- asistă atingerea „scopului comandatului", exploatează avantajele unei forțe profesioniste, bine antrenate;
- se adaptează rapid la apariția unor modificări importante în spațiul de luptă și elimină activitățile caracteristice operațiilor militare tradiționale.

Forțele dispersate deplasează puterea din spațiul de luptă compact în operații separate, prin:

- creșterea controlului funcțional în spațiul de luptă ocupat fizic și generarea puterii de luptă efective la momentul și locul potrivit;
- obținerea densității de putere necesară la cerere;

- asigurarea unei legături strânse între informații, operații și logistică, pentru a obține efecte precise;
- utilizarea informației pentru obținerea efectelor dorite, limitând necesitatea de a concentra fizic forțele într-o locație geografică specifică;
- creștere tempoului și a vitezei de mișcare pe câmpul de luptă, pentru a face mai dificilă lovirea de către adversar.

Cercetarea în profunzime cu senzorii extinde utilizarea senzorilor distribuiți conectați în rețea, pentru detectarea informațiilor despre elementele de interes la distanțe operaționale relevante, spre a obține efecte decisive:

- mecanism de creștere semnificativă a informațiilor, supravegherii și recunoașterii (ISR);
- utilizarea senzorilor, ca element de manevră, pentru a crește și menține superioritatea informațională;
- exploatarea senzorilor ca un mijloc de intimidare, când sunt utilizați în mod vizibil.

Modificarea rapidă a condițiilor inițiale exploatează principiile pentru partajarea situației, sincronizare, forțe dispersate, cercetarea în profunzime cu senzorii, rapiditatea de elaborare a comenzii, pentru a permite forțelor întrunite să identifice rapid, să se adapteze și să schimbe un context de operare defavorabil în avantajul propriu.

Operațiile comprimate elimină barierele procedurale dintre servicii și procese, astfel că operațiile întrunite sunt conduse la cele mai reduse niveluri organizaționale posibile, pentru a obține efecte rapide și decisive:

- creșterea vitezei de desfășurare, utilizare și de sprijin;
- eliminarea compartimentării proceselor (organizare, desfășurare, utilizare și sprijin) și a

zonelor funcționale (operații, informații şi logistică);
- eliminarea limitelor structurale, pentru a reuni capabilitățile la nivelurile organizatorice cele mai scăzute posibil (operații întrunite la nivel de companie).

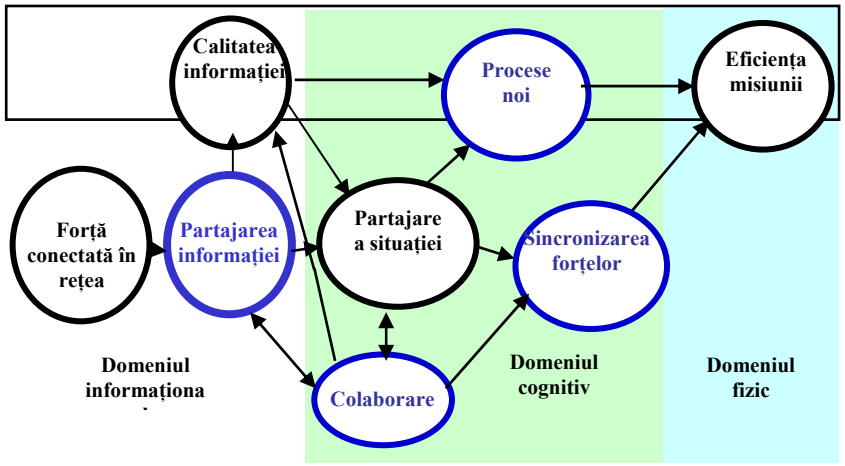


Figura nr. 3. Principiile NCW.

3. Realizări şi perspective la nivel național

Sistemul Informatic pentru Asistarea Deciziei la Brigadă (SIAAB-C2 transportabil) este destinat pentru asistarea activităților în punctele de comandă la eşaloanele brigadă/batalion, instruire şi antrenament de stat major şi interfațarea cu sisteme similare.

În varianta finală, sistemul va fi implementat la nivelul comandamentelor de brigadă şi la unitățile subordonate acestora, de tip batalion şi va fi compus din:

- două rețele locale de calculatoare (pentru punctul de comandă de bază şi de rezervă) interconectate prin mijloace de comunicații multicanal;
- rețele locale la nivel punct de comandă de batalion (divizion);
- abonați îndepărtați;
- pachete de aplicații software pentru asistarea comenzii şi controlului;
- autoritatea de certificare pentru asigurarea infrastructurii de chei publice.

Din punctul de vedere al concepției, sistemul este adaptat conceptului NCW răspunzând în cea mai mare măsură cerințelor specifice. Astfel, într-un mediu specific de securitate (arhitectură de tip infrastructură de chei publice cu autoritate de certificare la nivelul SMFT şi chei hardware pentru identificarea utilizatorilor), sistemul permite schimbul de informații formatate şi neformatate standard NATO, prin intermediul rețelei militare naționale de comunicații (RTP/STAR).

Modernizarea sistemului informatic logistic se înscrie în contextul continuării procesului de transformare a Armatei României. Concomitent cu remodelarea structurilor de logistică, apte să răspundă nevoilor de asigurare a unităților luptătoare cu toate categoriile de tehnică şi materiale (la timpul şi în locul ordonat, cât mai simplu şi cu cheltuieli minime), noile structuri ce se proiectează trebuie să răspundă şi cerințelor de realizare a interoperabilității cu sistemele logistice ale armatelor moderne din țările membre NATO sau partenere. Sistemul informatic logistic trebuie să fie capabil de adaptare modulară rapidă, prin asigurarea unui flux informațional coerent. Acest lucru va permite o abordare unitară, conectarea în rețeaua de informatizare a armatei, o execuție centralizată şi specializată. Logistica focalizată în viziunea americană trebuie să asigure capabilității militare echipamentele şi armele

necesare, sprijin şi personal în cantităţile necesare, la locul necesar şi în timpul necesar susţinerii obiectivelor operaţionale. Acest lucru se poate realiza prin îmbunătăţirea sistemului informaţional, remodelarea prin inovare a structurilor organizatorice, dezvoltarea disciplinată a proceselor, precum şi utilizarea de tehnologii moderne de transport.

Reţeaua militară naţională de comunicaţii (RMNC) asigură în prezent suportul de comunicaţie pentru voce, date şi video pentru componentele Ministerului Apărării Naţionale, forţele dislocate în teatrele de operaţii din Afghanistan şi Irak, şi cu delegaţia permanentă a României la NATO.

Activităţile viitoare de dezvoltare a reţelei vizează integrarea în "NATO General Communication System" (NGCS), pentru a se putea asigura:

- servicii pentru forţele desemnate să acţioneze sub comandă NATO;
- servicii de reţea pentru forţele desfăşurate sub comanda NATO, prin dezvoltarea componentei mobile;
- realizarea reţelelor tactice de comunicaţii şi integrarea acestora în reţeaua militară naţională de comunicaţii.

Participarea României sub egida NATO la programul AGS (Alliance Ground Surveillance), destinat observării – urmăririi (electronice) a terenului prin mijloace aeropurtate, deschide o perspectivă nouă privind accesul la tehnologii moderne, inclusiv printr-o viitoare implicare a industriei româneşti în acest proiect. Această tehnologie a NATO şi-a avut începutul, în primul rând, prin intermediul Statelor Unite, cu ocazia războiului din Golf, cu ajutorul sistemului propriu JSTARS (Joint Surveillance and Target Attack Radar System).

De atunci, importanţa urmăririi electronice a terenului nu a încetat să crească, noul sistem AGS reprezentând unul din proiectele prioritare ale NATO, fiind derulat pe baza contractului încheiat cu consorţiul TIPS (Transatlantic Industrial Proposed Solution). TIPS oferă un sistem AGS bazat

pe o platformă aeriană medie, cel mai probabil de tip Airbus. De asemenea, platforma pilotată va putea fi completată cu sisteme de avioane fără pilot performante, probabil de tipul RQ-4B. Propunerea TIPS a fost acceptată pentru caracteristicile oferite, referitoare la: arhitectura de sistem deschis, interoperabilitatea, utilizarea de tehnologii COTS, maximizarea punctelor comune între elementele aeriene, terestre şi de suport, tehnologia comună radar, legăturile de date tip Link 11, 16, 22, precum şi comunicaţiile UHF prin satelit.

Soldatul viitorului - Sistem integrat de acţiune în contextul interoperabilităţii NATO este un proiect de cercetare-dezvoltare în derulare, finanţat în cadrul Programului Naţional de CDI RELANSIN, destinat să furnizeze capabilităţile necesare ducerii acţiunilor de luptă în comun cu trupele NATO şi asigurarea facilităţilor de comandă şi control pentru asigurarea exercitării comenzii. Sistemul integrat unitar cuprinde: cască integrată, computer, radio, armament, echipa-ment individual de protecţie şi echipamente optoelectronice. Concepţia SMFT şi modelele existente (de ex., cel britanic, Future Integrated Soldier Technology - Viitoarea Tehnologie Integrată pentru Soldat) sunt extrem de utile în dezvoltarea sistemului românesc.

Pentru a valorifica eficient avantajele oferite de era informaţională, NATO a iniţiat un proces amplu de transformare structurală, doctrinară şi conceptuală, pentru a-şi asigura superioritatea informaţională prin crearea capabilităţilor facilitate de reţea (NATO Network Enabled Capability – NNEC).

Scopurile urmărite în implementarea acestui nou concept sunt:

- sensibilizarea şi conştientizarea naţiunilor asupra dobândirii superiorităţii informaţionale prin crearea capabilităţilor facilitate de reţea pentru forţele naţionale şi multinaţionale;

- identificarea posibilităţilor de valorificare a experienţei naţiunilor membre NATO;
- definirea direcţiilor şi modalităţilor concrete de transformare a NATO;
- definirea rolului şi modului în care agenţiile NATO vor contribui la implementarea şi valorificarea conceptului NNEC.

Pe plan naţional, implementarea capabilităţilor NCW nu va implica numai adaptarea elementelor deja existente la acest concept, ci şi stabilirea cadrului legal (adaptarea strategiei naţionale de securitate, definirea doctrinelor etc.) care va permite forţelor întrunite trecerea de la gândirea centrată pe platformă la cea orientată pe reţea.

Acest proces este unul continuu şi fără un punct final previzibil acum. Echipele implicate în transformarea şi implementarea NCW vor trebui să ia în calcul faptul că acest fenomen este strâns legat de coevoluţia a şapte factori funcţionali importanţi din domeniul doctrinei, organizării, antrenamentului, tehnologiei, conducerii şi educaţiei, personalului şi facilităţilor.

Dimensiunile multiple ale contribuţiei cercetării şi tehnologiei la capabilităţile NATO, începând cu domeniul senzorilor, continuând cu cel informaţional (comandă-control) şi ajungând chiar la acţiuni concrete de luptă, au fost definite de adjunctul secretarului general NATO pentru investiţii în domeniul apărării, domnul Marshall Billinsglea: „Senzorii trebuie să detecteze ţintele neconvenţionale, lunetiştii din spatele zidurilor, moleculele explozive clasice sau neclasice, comportamentul uman suspect, obiectele de mici dimensiuni care se deplasează sub apă; urmează fuziunea senzorilor (radar, optic, sateliţi ş.a.), detecţia, identificarea şi urmărirea ţintelor; prin sistemele de comandă-control se asigură superioritatea informaţională, informaţiile fiind transmise până la nivelul luptătorului, care trebuie să acţioneze cu echipamentele din

dotare într-un mediu bazat pe reţea". Astfel că şi preocupările noastre pentru soldatul viitorului sunt similare cu concepţia generală privind „arhitectura" hardware a soldatului viitorului (figura nr.4).

Figura nr. 4. „Arhitectura" hardware a soldatului viitorului.

În cadrul acţiunilor de luptă efective sunt utilizate nemijlocit rezultatele activităţilor de cercetare ştiinţifică:

- Platforme: mici UUVs, mini UAVs, UCAVs, roboţi tereştri;
- Armamente: transportabile pe calea aerului, cu precizie sporită şi daune colaterale mai reduse;
- Echipamente moderne pentru soldatul viitorului;
- Capabilităţi specifice lucrului în reţele şi pentru integrarea sistemelor din cadrul NATO.

Domeniile considerate *critice,* cu resurse şi planuri de lucru specifice, considerate cerinţe privind capabilităţile pe termen lung (LTCR), sunt:

- Interfețele NATO cu sistemele informaționale naționale;
- Susținerea forțelor cu caracter expediționar;
- Nivelul inferior, superior şi faza de susținere a apărării împotriva rachetelor balistice tactice;
- Supravegherea din spațiu a obiectivelor terestre;
- Conectare sincronă senzor-trăgător pentru localizarea, identificarea şi atacarea țintelor de mare însemnătate, critice din punct de vedere temporal.
- Detecția şi identificarea rapidă a țintelor de mare însemnătate, critice din punct de vedere temporal;
- Capacitatea de desfăşurare în dispozitiv a forțelor de luptă;
- Suprimarea rapidă, eficace şi cu riscuri minime a apărării antiaeriene a inamicului;
- Imaginea operațională comună;
- Imagine aeriană comună recunoscută;
- Imagine comună pentru războiul electronic;
- Decontaminarea echipamentului şi personalului fără a utiliza mijloace toxice;
- Identificare şi interoperabilitate în condițiile operațiunilor de luptă comune;
- Identificare şi interoperabilitate în condițiile operațiunilor de luptă comune şi achiziția țintelor;
- Livrarea precisă a echipamentelor şi proviziilor, prin lansarea din mijloace aeriene;
- Operațiuni de căutare şi salvare la mare distanță;

- Surse de alimentare cu greutate redusă, autonome;
- Ochirea în intervale de timp critice, evaluare şi repartizarea/realocarea sarcinilor pentru echipamentele de lovire;
- Dispozitive uşoare, compacte, portabile pentru furnizarea imaginii operaționale comune.

Astfel, progresul în implementarea NCW nu poate fi măsurat numai prin analiza unei singure dimensiuni, cum ar fi tehnologia sau doctrina, ci trebuie evaluat prin capacitatea misiunilor de a integra cele şapte elemente menționate anterior: doctrină, organizare, antrenament, tehnologie, conducere şi educație, personal şi facilități.

O schimbare profundă în oricare din aceste domenii necesită schimbări în toate celelalte elemente.

Nu în ultimul rând, transformarea, în general, şi transformarea militară în special, ca şi implementarea conceptului NCW, se referă la schimbarea valorilor, atitudinilor, încrederii forțelor armate asupra desfăşurării şi dezvoltării operațiunilor militare.

Achiziția oricărei componente NCW va trebui, astfel, să se supună unei strategii de achiziție care să aibă următoarele obiective principale:

- apartenența la un sistem de sisteme;
- orientarea numai către sisteme deschise (arhitecturi şi interfețe);
- prioritatea selectării, pe cât posibil, a sistemelor civile în favoarea sistemelor militare dezvoltate în mod special;
- interconectivitatea şi conceptul „Universal Plug and Play”;
- extinderea cunoaşterii, prin implicarea în fenomenul NCW a industriilor naționale şi internaționale, private

sau de stat, precum şi a centrelor de cercetare ştiinţifică (universităţi) civile şi militare.

4. Politici viitoare cu privire la dezvoltarea conceptului NCW

În domeniul personalului (cea mai importantă valoare):

- Nevoia de fundamentare/documentare a conceptului de selectare, formare şi de educaţie a resursei umane;
- Crearea unor iniţiative stimulative, care să împiedice plecarea personalului în domeniul privat civil, pentru locuri de muncă mai bine plătite;
- Acţiuni pentru atragerea şi păstrarea specializărilor critice;
- Nevoia de pregătire şi specializare permanentă a personalului;
- Asigurarea unei viziuni stabile a carierei în acest domeniu;

În domeniul emiterii şi evaluării cerinţelor (în cadrul Sistemului integrat de management al achiziţiilor pentru apărare-SIMAPA):

- Îmbunătăţirea procesului de dezvoltare a cerinţelor operaţionale în concordanţă cu cerinţele procedurale ale SIMAPA;
- Respectarea politicilor şi procedurilor pentru uniformizarea şi disciplinarea procesului de generare a cerinţelor;
- Menţinerea de opţiuni rezonabile şi deschise privind costurile, performanţele şi graficul de realizare;

- Evitarea de angajamente cu soluţii pentru un anumit sistem, mai ales pentru acel care împiedică inserţia de tehnologii şi articole nedezvoltabile;
- Definirea cerinţelor pentru o capabilitate operaţională în termeni largi;
- Definirea cerinţelor pe faze şi perioade de realizare, cu valori-obiectiv şi valori-prag;
- Evaluarea posibilităţilor de modificare a cerinţelor de performanţe dorite, în mod rezonabil, pentru a uşura utilizarea articolelor şi componentelor comerciale şi nedezvoltabile;
- Evaluarea posibilităţii sistemului de a putea opera şi supravieţui în mediul anticipat de ameninţări;
- Stabilirea de informaţii critice pentru program şi cerinţe de protecţie;
- Stabilirea în Documentul cu Cerinţele Operaţionale (DCO) de valori-obiectiv şi valori-prag privind costurile pe întreaga durată de viaţă;
- Includerea de cerinţe de securitate, garanţii pentru asigurarea accesului la informaţii şi pentru protecţia infrastructurii critice, precum şi de criterii privind transmiterea de informaţii în contextul operaţiilor multinaţionale;
- Stabilirea de criterii de suportabilitate, schimb de informaţii şi cerinţe de interoperabilitate pentru familiile de sisteme aflate în mediul operaţional;
- Stabilirea şi considerarea interoperabilităţii ca un parametru-cheie de performanţă, atât în DCO, cât şi în Baza Programului de Achiziţie;
- Cerinţele de interoperabilitate şi de suportabilitate pentru toate programele de sisteme IT sau C2+, trebuie să aibă în vedere, în primul rând, cerinţele naţionale. Cerinţele din Documentul cu Nevoile Misiunii (DNM) şi din DCO trebuie să fie

actualizate pe parcursul derulării procesului de achiziție, operare şi mentenanță, pe durata de viață operațională a sistemului.

În domeniul achiziționării sistemului (în cadrul SIMAPA), având în vedere achiziția de „sisteme de sisteme" şi achiziția de capabilități tip NCW şi pentru superioritatea informațională:

- Procesul de management şi politicile specifice de dezvoltare a sistemelor de sisteme trebuie să fie orientate către achiziția de capabilități NCW, ținând cont de cerințele de conectivitate, cerințele pentru luptători, strategiile de achiziție şi cerințele de asigurare a resurselor;
- Definirea cerințelor pentru achiziția de capabilități NCW trebuie să aibă în vedere şi trecerea de la sistemele moştenite existente la noile viziuni de capabilități NCW;
- SIMAPA trebuie să asigure transformarea nevoilor utilizatorilor finali, ținând cont de oportunitățile tehnologice existente şi de posibilitățile de susținere financiară a cerințelor operaționale propuse de aceştia: reprezentarea judicioasă a balanțelor de cost, grafic de realizare şi performanțe față de cerințele exprimate; posibilitățile de interoperabilitate cu alte sisteme (naționale, ale aliaților, ale coaliților sau cu altele specificate în DCO); utilizarea de tehnologii probate, proiecte de sisteme deschise, capacități tehnologice şi de producție sau servicii utilizabile, asigurarea unei competiții inteligente; dacă ne putem permite achiziția unui asemenea sistem şi dacă putem să-l operăm şi să-l întreținem în limitele bugetare existente, incluzând cerințele de

scoatere din uz sau de externalizare a unor servicii;
- Revizuirea în cadrul MApN a unor cerințe operaționale mai vechi şi documentarea asupra sistemelor de sisteme existente şi conceptelor viitoare, precum şi asupra viitoarelor capabilități militare avute în vedere la nivelul categoriilor de forțe şi al Statului Major General.

În domeniul ştiinței şi tehnologiei:

- Coordonarea investițiilor şi eforturilor de cercetare şi dezvoltare tehnologică, la nivelul Statului Major General, pentru a asigura complementaritatea şi consistența acestora;
- Dezvoltarea de experimentări şi demonstrații tehnologice, studii şi cercetări de laborator, cercetări operaționale, studii de modelare şi simulare, studii de fezabilitate şi de oportunitate;
- Elaborarea de studii şi cercetări teoretice şi practice privind: stabilirea de rețele care să servească toți utilizatorii; deplasarea informației în cadrul constrângerilor existente în diferite rețele; gestionarea, în calitate de utilizator, a creşterii enorme în cantitate şi varietate a informațiilor disponibile; managementul resurselor din rețea pentru gestionarea priorităților; asigurarea protecției şi nivelului adecvat de acces la informații şi servicii pentru diverşi beneficiari; utilizarea în rețea a altor aplicații necesare utilizatorilor pentru îndeplinirea sarcinilor;
- Sincronizarea dezvoltării strategiei militare şi doctrinei cu progresele înregistrate în domeniul tehnologic şi cu procesul de inserție tehnologică;

- Experimentarea conectării la rețele tip NCW, conectarea la pachetele de capabilități de misiuni, inserția tehnologică sincronizată şi mai rapidă;
- Planificarea efectuării de studii şi cercetări privind accesul la surse de date şi informații, oricând şi oriunde, incluzând utilizarea sistemelor ISR;
- Din perspectiva NCW, eforturile în ştiință şi tehnologie trebuie să conducă şi la îmbunătățirea aplicării tehnologiilor şi practicilor comerciale, la investiții în ştiințele sociale şi fizice pe care sectorul comercial nu le asigură, precum şi la implicarea utilizatorilor finali în inițiativele de experimentare, demonstrare şi accelerare a introducerii acestora în operare;
- Asigurarea co-evoluției conceptelor cu doctrina şi dezvoltarea tehnologică.

În domeniul planurilor de informatizare:

- Înțelegerea saltului de la platformă de lucru către lucrul în rețea;
- Utilizarea unor rețele comune;
- Dezvoltarea de software pentru sisteme de arme de precizie;
- Realizarea de rețele orientate către servicii;
- Adoptarea standardelor COTS şi ale celor industriale;
- Utilizarea tehnologiei pentru realizarea şi difuzarea imaginii operaționale unice, a suportului de intelligence, a sistemului de transfer al mesajelor şi pentru planificarea acțiunilor în colaborare;
- Adoptarea unui mediu de lucru şi a unei arhitecturi care să aibă la bază PC-urile;
- Investiții pentru domeniile comandă şi control, separat, împreună şi combinat; supraveghere şi

recunoaştere; suport pentru culegere de informații, logistică, planificare şi conducere; război informațional, incluzând război electronic etc.

5. Impedimente în calea dezvoltării conceptului NCW

- Dificultăți în aprecierea posibilelor dezvoltări tehnologice;
- Resurse reduse alocate pentru domeniu;
- Deficiențe în existența interoperabilității necesare, care să servească, de exemplu, şi drept mesager pentru interoperabilitate în viitor;
- Insuficient progres cu privire la structura de informații care să asigure nivelurile de interoperabilitate şi de conectivitate necesare sprijinirii operațiilor bazate pe rețea (Network Centric Operations) ;
- Practicile şi procesul de achiziții care nu permit ținerea ritmului cu cel al dezvoltării de tehnologii şi cu exploatarea integrală a capabilităților comerciale;
- Disfuncțiile inerente dintre procesele de elaborare a cerințelor, de achiziție, de contractare şi de experimentare;
- Procese care nu sunt adecvate co-evoluției şi dezvoltării simultane a pachetelor de capabilități;
- Nevoia de înțelegere a bazelor ingineriei sistemelor şi specificului procesului de experimentare, inclusiv a termenilor de proiectare, conducere şi colectare, precum şi de analiză a datelor şi rezultatelor experimentale;
- Nevoia existenței unui plan strategic, care să exprime ipotezele cu privire la evoluția NCW;
- Absența unui punct focal care să gestioneze procesul de atingere graduală a capabilităților NCW;

- În viitor, rețeaua tip NCW va constitui poate singurul şi cel mai important contributor la dobândirea puterii şi supremației în luptă.

6. Concluzii

Aşa cum, în secolul al XV-lea, artileria a revoluționat războiul, aşa cum produsele erei industriale - tancurile şi avioanele - au transformat felul în care s-a luptat în secolul al XX-lea, „zorii erei informaționale - evoluțiile tehnologice care propulsează sectoarele specializate în calculatoare, senzori şi comunicații vor conduce în următorii 20-30 de ani la schimbări mai radicale decât în orice altă perioadă a istoriei umanității".

Capabilitățile NCW trebuie să fie dezvoltate şi această teorie aplicată la scară extinsă pentru întreg sistemul național de apărare. Forțele întrunite trebuie să fie integrate în rețea la nivelurile strategic, operațional şi tactic. În scopul maximizării potențialului pentru creşterea puterii de luptă al NCW, doctrinele de operații trebuie să evolueze similar capabilităților implementate pentru războiul în rețea.

Aliații şi partenerii României au dezvoltat propriile concepte şi capabilități pentru NCW. Operațiunile militare din Bosnia, Kosovo, Afghanistan şi Irak au permis aplicarea cu succes de către aceste state a principiilor războiului bazat pe rețea.

O strategie națională pentru implementarea NCW va avea un impact major asupra dezvoltării forțelor armate şi asupra deciziilor de investiții ale Ministerului Apărării Naționale.

Rolul experimentărilor în procesul de implementare a conceptelor şi capabilităților orientate pe rețea este crucial. Se minimizează, astfel, riscurile dezvoltării unor sisteme care nu

corespund cerințelor operaționale şi, implicit, al respingerii acestora de către utilizatorul final – efectorul.

Pe scurt, calea corectă de urmat este clară. Nu trebuie achiziționate tehnologii de ieri. Trebuie investit, dezvoltat şi/sau cumpărat privind către viitor, dar nu tehnologie pe cale de dispariție. Este necesară concentrarea asupra domeniilor cu cerințe esențiale. NATO îşi doreşte membri care să dispună de capabilități puternice de apărare națională, chiar dacă aceste sisteme nu sunt interoperabile la toate nivelurile. În multe situații, doctrina şi politica de securitate nu vor asigura, în totalitate, interconectivitatea.

Oricare strateg ştie că victoria zâmbeşte celor care anticipează schimbările în caracterul războiului, nu celor care aşteaptă pasivi şi resemnați. Astăzi, nimeni nu-şi poate permite luxul să ducă o politică izolaționistă sau să ignore tehnica modernă. Statele fac eforturi de achiziționare a tehnologiilor de ultimă oră şi nici România nu face excepție. Este important de observat că tehnologia nu reprezintă un scop în sine, ci un mijloc de realizare a unui scop.

În contextul unei abordări globale, „**tehnologia**" depăşeşte granițele domeniului tehnic tradițional şi tinde a fi definită ca **aplicarea practică a unui corp de cunoştințe, concepte operaționale şi mijloace tehnice pentru a participa efectiv şi eficient la viața economică, socială, politică şi militară internațională**.

Există câteva tehnologii-cheie, cu rol catalizator, ce ar trebui luate în considerație de către orice națiune care doreşte să acceadă în structura de comandă-control a NATO. Aceste elemente tehnologice sunt: **tehnologia echipamentelor miniaturizate şi compacte; tehnologiile comunicațiilor digitale,** cu subsisteme **de comunicații personale autentificate şi securizate; tehnologii pentru** rețele destinate consultării politice sau comenzii şi controlului specifice **sistemelor de comunicații strategice** actuale ale NATO;

produsele Microsoft disponibile comercial, utilizate în mod curent ca elemente de bază în cadrul sistemelor informatice, care asigură infrastructura necesară îndeplinirii funcțiilor de consultare militară şi politică; **interfețele grafice cu utilizatorul şi produsele software realizate în tehnologie web, ce permit accesarea de baze de date şi biblioteci dinamice distribuite; video-teleconferințele în regim secretizat**, susținute şi de afişarea pe monitorul calculatorului a situațiilor operaționale curente, au devenit o capabilitate de rutină, dar esențială atât în procesul de consultare politică, cât şi în domeniul comenzii şi controlului; existența unui **sistem informațional geografic digital** de largă cuprindere; **automatizarea tuturor aspectelor specifice desfăşurării acțiunilor aeriene** a evoluat, în sensul scurtării duratei ciclurilor de planificare a acestora şi al controlării stricte a preciziei loviturilor, a interceptărilor şi a acțiunilor de salvare/evacuare; **tehnologii software ce permit desfăşurarea distribuită a exercițiilor asistate de calculator, realizarea facilităților de pregătire şi antrenament, bazate pe medii sintetice şi pe scenarii etc.**

În viitor, aceste capabilități vor fi utilizate pentru planificarea acțiunilor militare, pentru analiza cursului acțiunilor şi pentru **evaluarea alternativelor decizionale**.

Trebuie subliniat şi repetat că schimbările tehnologice şi politice influențează sistemele de apărare. De aceea, este necesar să avem în vedere următoarele aspecte:

- Convergența dintre sistemele de comunicații şi informații, semnificând faptul că foarte puține sisteme IT sunt individuale;
- Utilizarea largă a componentelor COTS în sistemele militare operaționale C2;
- Influența Internetului şi a tehnologiilor Internet;

- Apariția unor rețele informaționale care permit integrarea comunicațiilor strategice, operaționale şi tactice şi o interoperabilitate la nivel înalt;
- Existența unei revoluții a relațiilor militare şi a rețelei centrale de război.

Marea provocare constă în a schimba modul de gândire în legătură cu acțiunile militare, cu misiunile militare, precum şi cu structura şi modul de pregătire a forțelor militare, dar şi cu modul de echipare, protecție şi comunicare al „soldatului viitorului", integrat în şi la niveluri diferite de rețele.

BIBLIOGRAFIE:

1. Department of Defence, *Network Centric Operations Conceptual Framework, version 2.0, iunie 2004.*
2. John J. GARSTKA, *Network Centric Warfare Offers Warfighting Advantage*, Signal, May 2003.
3. Viceamiral Arthur K. CEBROWSKI, John J. GARSTKA, *Network Centric Warfare: Its origin and Future*, U.S. Naval Institute Proceedings Annapolis, Maryland, ianuarie 1998.
4. Proceedings of the fifth international conference, *Network Centric Warfare Europe 2004.*
5. Ion-Eftimie SANDU, *Decizii în condiții de incertitudine şi risc. Managementul riscului aplicat la programele de achiziții pentru apărare*, Colegiul Național de Apărare, București, iunie 2001.

STADIUL ACTUAL ŞI PERSPECTIVELE DEZVOLTĂRII SISTEMULUI DE COMUNICAŢII AL ARMATEI ROMÂNIEI PENTRU A CORESPUNDE CERINŢELOR NNEC (NCW)

General-maior dr. Cristea DUMITRU

GENERALITĂŢI

Sistemul de comunicaţii şi informatică al Armatei României (SCIAR) cuprinde totalitatea mijloacelor de comunicaţii şi informatică, a infrastructurii, a serviciilor, aplicaţiilor informatice existente în dotarea Armatei României, care pot fi interconectate şi care asigură actul conducerii la toate eşaloanele. El are o componentă staţionară, permanentă şi o componentă mobilă.

Elementele de bază ale componentei staţionare de comunicaţii sunt Reţeaua de Transmisiuni Permanentă (RTP/STAR) şi Reţeaua Radio Operativă de Nivel Strategic (RRONS/STAR).

Locul şi rolul RTP/STAR şi RRONS/STAR în cadrul SCIAR este prezentate în anexa nr. 1.

1. Stadiul actual de dezvoltare a RTP/STAR

RTP/STAR reprezintă o reţea geografică mare, acoperind zonele de interes pentru MApN din teritoriul naţional şi oferind servicii de voce securizată şi nesecurizată, de date, fax şi videoteleconferinţă criptată pentru unităţile şi subunităţile tuturor categoriilor de forţe şi ale structurilor centrale dispuse pe teritoriul naţional, precum şi pentru reprezentanţele Statului Major General şi forţele dislocate în afara teritoriului naţional.

De asemenea, asigură comunicaţiile de voce, fax şi date securizate pentru abonaţii sau structurile nominalizate să aibă acces în regim securizat la serviciile NGCS, precum şi comunicaţiile de voce nesecurizate pentru toţi abonaţii reţelei către NGCS. În acelaşi timp, RTP/STAR asigură canalele de date de mare viteză necesare amplificării reţelei NATO geografice de transmiteri de date cu caracter secret (NATO SECRET WAN-NS WAN), atât în dezvoltarea actuală, cât şi în faza a doua şi în fazele ulterioare de extindere a acesteia în România. Această reţea este cunoscută şi sub numele de Reţeaua NATO CRONOS.

RTP/STAR asigură interfaţa STAR cu sistemele de comunicaţii ale celorlalte structuri ale Sistemului Naţional de Apărare, cu sistemele de comunicaţii ale operatorilor publici naţionali, precum şi cu sistemul NATO General de Comunicaţii (NGCS=NATO General Communications System).

Reţeaua RTP/STAR asigură suportul necesar de comunicaţii pentru o serie de programe importante de modernizare şi operaţionalizare a forţelor, precum:

- sistemul informatic integrat al MApN;
- sistemul de asigurare a suveranităţii aeriene, ASOC;
- sistemul de senzori de radiolocaţie tridimensional, de mare altitudine, FPS-117;
- sistemul de schimb al datelor de zbor, FDEx;
- sistemul de difuzare a imaginii aeriene unice recunoscute, STASA;
- sistemul meteorologic integrat, SIMIN;
- sistemul de control al traficului pe mare, SCOMAR;
- sistemul de avertizare şi raportare a situaţiei nucleare, bacteriologice şi chimice, SAR NBC;
- conducerea elementelor de POLIŢIE AERIANĂ;
- sistemul de coordonare şi planificare a mişcării, SIPLANET;
- Sistemul criptat de videoconferinţă al MApN.

Prin canale de acelaşi tip şi capacităţi, aflate în curs de activare, urmează să se asigure suportul de comunicaţii pentru programele aflate în dezvoltare:

- sistemul integrat de coordonare a mişcării ADAMS;
- sistemul logistic integrat AILS;
- sistemul integrat pentru managementul carierei militare;
- sistemul de senzori de radiolocaţie tridimensională de medie şi joasă altitudine, GAP-FILLER;
- sistemul de Comandă Control Aerian Naţional (SCCAN) integrat în sistemul NATO (ACCS).

Dezvoltarea reţelei pe teritoriul naţional s-a făcut utilizând linii digitale magistrale, de acces sau de interconectare realizate pe suport radioreleu militar sau pe fluxuri închiriate de la SNTc Romtelecom SA. Acestea din urmă sunt realizate de SNTc Romtelecom SA utilizând reţeaua magistrală naţională de fibră optică.

Pentru realizarea liniilor radioreleu militare s-au utilizat, cu predilecţie, turnuri autoportante construite de MApN în interiorul unităţilor militare şi, în unele cazuri, poziţii închiriate în locaţiile SN Radiocomunicaţii SA.

Numărul total de centre RTP/STAR magistrale, de acces sau terminale instalate şi integrate în reţea până în prezent este de 143.

Reţeaua astfel realizată asigură accesul direct (prin conectarea abonatului nemijlocit la un centru RTP/STAR) sau indirect (abonatul este conectat la o centrală analogică conectată, la rândul ei, la un centru RTP/STAR distant) pentru abonaţii din 727 unităţi militare.

Numărul total de abonaţi telefonici cu acces direct este de aproximativ 16.500, dintre care 320 sunt dotaţi cu terminale de voce, date şi acces radio secretizate DELTA 01M.

Reţeaua RTP/STAR asigură şi un număr de 228 canale de transmiteri de date punct la punct cu capacităţi de transmitere cuprinse între 32 şi 128 Kbps.

1.1. Extensia RTP/STAR la reprezentanţele României la NATO

Asigurarea serviciilor de comunicaţii şi informatică la reprezentanţele României de la Bruxelles şi Mons a devenit o necesitate în preajma şi, în special, după integrarea formală a ţării noastre în NATO.

Soluţia imediată, care oferea toată gama de servicii activată structurilor echipate cu centre RTP/STAR, a constituit-o chiar instalarea a câte unui centru cu dezvoltare minimală la fiecare din cele două reprezentanţe şi integrarea lui în RTP/STAR printr-un flux de 2 Mbps, închiriat din reţeaua publică de telecomunicaţii internaţională.

S-a obţinut, astfel, extensia RTP/STAR în cele două locaţii. Membrilor reprezentanţelor li s-au asigurat, în acest mod, servicii de voce nesecretizată, servicii de voce secretizată cu terminalul numeric DELTA 01 M, servicii de videoconferinţă criptată în reţeaua MApN, servicii de date în reţeaua INTRANET MILITAR, cu protecţia transportului informaţiei folosind echipamente CRIPTO IP.

În anexa nr. 2 este prezentată aplicaţia descrisă anterior, în care a fost inclusă şi o extensie planificată la reprezentanţa României la Norfolk.

Separat, prin grija NATO, în cele două locaţii se asigură şi accesul prin voce nesecurizată la reţeaua de comunicaţii analogică a NATO (IVSN = Initial Voice Switched Network) - şi, prin aceasta, la NGCS - iar prin date criptate, în reţeaua CRONOS (NS WAN).

În viitor, o soluţie similară urmează să se aplice şi pentru Reprezentanţa de la Norfolk, de la Comandamentul Aliat pentru Transformare (ACT).

1.2.Extensia RTP/STAR în teatrele de operaţii în care România participă cu forţe

Asigurarea serviciilor de comunicaţii şi informatică pentru bazele de dislocare a forţelor româneşti din teatrele de operaţii reprezintă un obiectiv major al structurii în a căror responsabilitate intră aceste forţe - Comandamentul 2 Operaţional Întrunit/S.M.G.

Pentru aceasta, soluţia a fost identificată în crearea unor module de comunicaţii şi informatică dislocabile, uşor de transportat cu orice mijloc şi având capacităţi de conectare la RTP/STAR, oriunde s-ar afla pe glob. Fiecare modul este echipat cu tehnică de comunicaţii robustizată, identică cu cea folosită în RTP/STAR, la care se adaugă echipamente multicanal de satelit (în benzile civile şi militare), precum şi o reţea de calculatoare pentru integrarea în INTRANETUL MILITAR. Segmentele satelitare spaţiale se închiriază de la operatorii publici sau de la organismele militare care controlează activitatea sateliţilor militari de telecomunicaţii. Se asigură, astfel, întreaga gamă de servicii: voce nesecretizată, voce secretizată cu DELTA 01M, servicii de videoconferinţă criptată, servicii de date în reţeaua INTRAMAN, precum şi servicii de date în reţeaua INTERNET (cu terminale separate).

Până în prezent au fost activate trei asemenea module în Irak (în punctele Tallil, White Horse şi Al Hilah) şi unul în Afghanistan (Kandahar), potrivit anexei nr. 3.

1.3. Interconectarea RTP/STAR cu Reţeaua Numerică Interforţe a armatei italiene şi asigurarea de servicii de comunicaţii pentru subunităţile româneşti care execută misiuni alături de forţele italiene

În anexa nr. 4 se prezintă soluţia prin care se beneficiază de suportul armatei italiene pentru asigurarea, acolo unde este posibil, a unui minim de legături de voce pentru forţele româneşti dislocate în puncte comune cu cele italiene.

Reţeaua Numerică Interforţe a Armatei Italiene (RNI) este realizată cu aparatură similară cu cea utilizată în RTP/STAR, furnizată de acelaşi producător – Marconi Selenia Communications. Ca urmare, interconectarea celor două reţele se face cu uşurinţă, cu condiţia asigurării între ele a unui mediu de transport informaţional de mare distanţă.

Cea mai uşoară soluţie o reprezintă utilizarea unei legături prin satelit.

Armata italiană dispune de un sistem de sateliţi - SICRAL - care face parte din constelaţia selectată de NATO pentru a completa sistemul NATO SATCOM; constelaţia este alcătuită, pe lângă sateliţi SICRAL, şi din sateliţi britanici (SKY NET) şi francezi (SYRACUSE).

Pornind de la toate acestea, s-a decis interconectarea RNI cu RTP/STAR prin instalarea într-un centru al RTP/STAR a unui terminal de satelit SICRAL şi asigurarea accesului la satelit de către armata italiană.

Armata italiană dispune, la forţele dislocate în teatrele de operaţii, de terminale satelitare care permit interconectarea forţelor respective cu Reţeaua Numerică Interforţe (RNI) realizată pe teritoriul Italiei.

Acolo unde forţele noastre acţionează alături de cele ale Italiei, s-au asigurat, în comutatoarele italiene conectate la terminalele de satelit, câteva posturi de abonaţi telefonici pentru persoanele cu funcţii din subunităţile româneşti. În acest fel, de

la orice post telefonic abilitat al RTP/STAR se poate intra în legătură cu aceste persoane şi oricare dintre ele poate apela orice post telefonic din RTP/STAR.

Legătura este asigurată numai în regim de telefonie nesecretizată.

1.4. Interconectarea RTP/STAR cu Rețeaua Metropolitană a Ministerului Administrației şi Internelor (anexa nr. 5)

Cooperarea dintre MApN şi MAI în cadrul Sistemului Național de Apărare este o necesitate evidentă. Prin interconectarea sistemelor de comunicații ale celor două ministere se asigură suportul tehnic al cooperării, cu reducerea costurilor care, în lipsa conectării, rezultau din utilizarea serviciilor închiriate de la operatorii publici. Interconectarea s-a realizat între două centre de transmisiuni, unul din rețeaua RTP/STAR şi celălalt din Rețeaua metropolitană a MAI, prin utilizarea unui flux numeric transportat pe o linie radioreleu realizată de MAI. De asemenea, pe teritoriul național, acolo unde a fost tehnic posibil, unitățile şi subunitățile de jandarmi, poliție, poliție de frontieră şi protecție civilă au fost conectate la RTP/STAR, proces care continuă şi în prezent. Prin aceste acțiuni se asigură, pe de o parte, cooperarea menționată şi, pe de altă parte, RTP/STAR oferă servicii de transport informațional între elemente ale MAI aflate la mare distanță, MAI acoperă doar costurile de conectare la RTP/STAR.

1.5. Asigurarea serviciului terminal-la-terminal secretizat între abonații cu funcții importante conectați la RTP/STAR

Serviciul este realizat prin utilizarea terminalului numeric de voce şi date criptat DELTA 01M. Acesta funcționează atât în regim necriptat, mai ales pe perioada luării legăturii, cât şi criptat.

El oferă abonaților serviciul de legătură de voce şi legătură de date prin conectarea la portul său extern a unui calculator; viteza de transport a datelor se poate seta, de la 1.200 la 32.000 bps.

În regim necriptat, legătura poate fi realizată cu orice abonat telefonic al RTP/STAR, indiferent de tipul terminalului telefonic la dispoziție (analogic sau numeric). În regim de transmiteri de date, legătura se asigură numai între abonații dotați cu terminale Delta 01 şi/sau Delta 01M.

Atât în regim de voce, cât şi de date criptat, legătura se asigură numai între abonații echipați cu terminale Delta 01M.

Serviciul poate fi asigurat atât pe teritoriul național, cât şi în afara acestuia, acolo unde s-au activat extensii ale RTP/STAR şi unde există, astfel, condiții tehnice de conectare a terminalului Delta 01M.

Procesul de instalare şi activare a terminalului Delta 01M a fost inițiat în anul 2003 şi va continua până la epuizarea terminalelor Delta 01 şi transformarea lor în terminale Delta 01M, în anul 2006.

Începând cu anul 2006, procesul de dotare cu terminale numerice criptate va continua, prin crearea noului terminal Delta 01S, într-o nouă tehnologie, care va rămâne compatibilă din punct de vedere funcțional cu Delta 01M.

1.6. Asigurarea serviciilor de videoconferință criptată

Pe suportul RTP/STAR este implementat şi serviciul criptat de videoconferință al Ministerului Apărării Naționale. El este conceput a fi realizat în mai multe etape, de la conducerea ministerului până la batalionul de infanterie aflat în misiuni în teatrul de operații. În momentul de față sistemul a fost implementat la nivelul conducerii politico-militare, la şefii categoriilor de forțe şi are extensii la reprezentanțele militare de la Bruxelles şi Mons şi în două teatre de operații (Irak şi Afghanistan). De asemenea, pentru diferite aplicații tactice, a

fost realizat şi prototipul unei autostaţii de videoconferinţă; în funcţie de necesităţile ce vor apărea şi de rezultatele obţinute cu acest prototip, numărul autostaţiilor va creşte la 4-5, putându-se înfiinţa un pluton de videoconferinţă. O prezentare a stării actuale a sistemului criptat de videoconferinţă este făcută în anexa nr. 6.

II. PERSPECTIVA DEZVOLTĂRII ŞI TRANSFORMĂRII SISTEMULUI DE COMUNICAŢII PRIN CREAREA RMNC ŞI IMPLEMENTAREA CONCEPTULUI NCW

1. Integrarea RTP/STAR în Sistemul NATO General de Comunicaţii (NGCS) şi crearea Reţelei Militare Naţionale de Comunicaţii (RMNC)

După cum se cunoaşte, condiţia minimală de iniţiere a implementării conceptului de Război centrat pe reţea şi de creare a Capabilităţilor NATO facilitate de reţea este conectarea şi integrarea reţelelor militare naţionale de comunicaţii în Reţeaua de Comunicaţii Globală (Global Grid). Realitatea din ţările NATO arată că fiecare şi-a creat reţeaua naţională conform unor principii şi procedee organizatorice şi de prelucrare informaţională mai mult sau mai puţin particulare. Rezultatul îl reprezintă caracterul eterogen al acestor reţele şi imposibilitatea interconectării lor imediate şi nemijlocite. Acest lucru ar fi posibil numai dacă s-ar crea un număr deosebit de mare de interfeţe de adaptare a fiecărei reţele cu toate celelalte sau, pentru a simplifica lucrurile, dacă între acestea ar exista un „liant" care să reducă problema de interfaţare doar între fiecare reţea naţională şi acest liant comun. Această ultimă soluţie a fost adoptată de specialiştii NATO, care au iniţiat procesul de creare a Sistemului NATO General de Comunicaţii (NATO General Communication System – NGCS) care să joace rolul de „liant".

În cadrul acestui concept, reţelele militare de comunicaţii ale naţiunilor membre NATO (NDN = National Defence Network) sunt reprezentate de totalitatea elementelor naţionale care asigură comunicaţiile directe, automate pentru abonaţii conectaţi la ele cu toţi abonaţii din NGCS şi din reţelele NDN ale celorlalte naţiuni.

Noţiunea de NDN a fost acceptată şi implementată şi în Armata României, sub denumirea de Reţea Naţională Militară de Comunicaţii (RMNC). Ea este, în prezent, reprezentată doar de RTP/STAR şi de toate extensiile acesteia la reprezentanţele României, la forţele din teatrele de operaţii, la MAE şi la MAI.

Există acţiuni în derulare de integrare în RMNC a reţelei RRONS şi a reţelei PHOENIX (MATRA).

Pas cu pas, tot mai multe elemente ale STAR vor fi integrate în RMNC. Trebuie remarcat că toate aceste elemente şi sisteme coexistă şi vor coexista (RTP/STAR, RRONS, STAR, ca ansamblu, PHOENIX etc). RMNC nu substituie RTP/STAR şi nici sistemul STAR în ansamblu nu este substituit de RMNC.

Tranziţia de la STAR la RMNC este prezentată în anexa nr. 7.

Interconectarea RTP/STAR la NGCS este prezentată în anexa nr. 8, iar structura generală a punctului de prezenţă NATO în România (Point of Presence = PoP) în anexa nr. 9.

În România, PoP a fost instalat în localul M 100 şi este operaţional, oferind servicii NATO UNCLASSIFIED de voce pentru toţi abonaţii RTP/STAR (accesul la NGCS este asigurat indiferent de localizarea lor în reţea, inclusiv în extensiile acesteia din ţară şi din afara ţării, la reprezentanţele României de la Bruxelles şi Mons, precum şi în teatrele de operaţii), servicii până la NATO SECRET de voce şi fax pentru utilizatorii din trei locaţii RTP/STAR (cu echipamente „telefon/fax secure" asigurate de NATO) şi servicii de date

NATO SECRET pentru utilizatorii din două locații RTP/STAR (cu rețele de calculatoare „secure" asigurate de NATO).

Echipamentele din Punctul de prezență au fost achiziționate şi instalate de NATO, sunt exploatate de specialişti militari români şi sunt incluse în sistemul Agenției NATO pentru Suport C3 (NCSA) de management centralizat.

2. Implementarea conceptelor NCW şi dezvoltarea sistemului.

Capabilitățile Facilitate de Rețea se dezvoltă prin implementarea unor principii NCW a căror aplicare în realitatea specifică sistemului militar românesc de comunicații este prezentată - succint - în continuare.

2.2.1 Principiul amplificării conectivității (conectivity)

* Amplificarea rețelei naționale de rețele de comunicații şi informatică (RMNC)

✓ Conectarea la RTP/STAR a RRONS/STAR în regim de voce şi date

✓ Conectarea la RTP/STAR a rețelei radio trunking PHOENIX pentru servicii de voce şi date

✓ Conectarea rețelei INTRAMAN la RRONS/STAR

✓ Pentru asigurarea de canale redundante în paralel cu cele asigurate de RTP/STAR.

✓ Pentru asigurarea de suport de comunicații cu locațiile izolate neintegrate în RTP/STAR.

✓ Pentru transfer de informații între abonați de date din INTRAMAN şi abonați de date din RRONS/STAR.

* Amplificarea rețelei naționale prin dezvoltarea rețelelor componente la nivel magistral în toate zonele de interes pentru organismul militar

✓ Dezvoltarea rețelei de centre magistrale a RTP/STAR în zona de răsărit, centru, nord-vest şi sud-vest, prin instalarea

centrelor deja achiziționate în locații închiriate de la direcțiile de radiocomunicații şi de la alți operatori de telecomunicații; în anexele 10, 11 şi 12 se prezintă extensia teritorială a rețelei în anii următori.

✓ Dezvoltarea rețelei RRONS, cu precădere în locațiile izolate a căror accesibilitate la RTP/STAR este dificilă sau imposibilă, cu eforturi raționale.

✓ Dezvoltarea rețelei INTRAMAN în locațiile în care se implementează servicii RTP/STAR şi RRONS/STAR.

2.2.2. Principiul amplificării benzii

✓ Introducerea în nodurile rețelei RTP/STAR şi în centrele importante de acces ale RTP/STAR a echipamentelor care optimizează utilizarea benzii (MPS) – anexele nr. 13 şi 14.

✓ Dublarea liniilor de transport pe direcțiile supraaglomerate, prin instalarea de radiorelee suplimentare sau prin închiriere de fluxuri de la operatorii publici.

✓ Trecerea de la utilizarea canalelor SUC de 128 kbps în exclusivitate pentru interconectarea elementelor INTRAMAN la utilizarea combinată a canalelor SUC cu cele de mai mare capacitate (1 sau 2 Mbps).

✓ Introducerea radioreleelor magistrale cu capacitatea de 155 Mbps pe traseele supraaglomerate.

✓ Mărirea capacității unora dintre liniile de interconectare de la 2 la 8 Mbps.

2.2.3. Principiul asigurării şi amplificării accesului (richability)

✓ Instalarea de centre RTP/STAR în toate locațiile de dispunere a forțelor, prin utilizarea echipamentelor deja achiziționate pentru forțele nominalizate să acționeze sub comanda NATO şi prin achiziționarea de noi echipamente pentru celelalte forțe.

✓ Instalarea de centre sau terminale RRONS/STAR cu precădere în locațiile care, inițial, sunt dificil de integrat în RTP/STAR.

✓ Instalarea de elemente/rețele locale din INTRAMAN în toate locațiile de dispunere a forțelor prevăzute pentru operaționalizare în 2007, respectiv 2012.

✓ Completarea centrelor de transmisiuni magistrale cu un sistem de antene orientabile care să permită accesul rapid prin radioreleu pentru mijloacele mobile de comunicații.

2.2.4. Principiul asigurării şi amplificării securității

✓ Instalarea de terminale numerice criptate DELTA 01 în toate locațiile de dispunere a forțelor prevăzute pentru operaționalizare în 2007, respectiv 2012 (minim un terminal/locație);

✓ Generalizarea criptării stațiilor radio utilizate în RRONS/STAR.

✓ Implementarea infrastructurii PRI în toate elementele INTRAMAN.

✓ Crearea rețelei INTRAMAN/SECRET la nivelul structurilor centrale.

2.2.5. Principiul managementului centralizat şi integrat al resurselor de comunicații

✓ Înlocuirea sistemului de operare UNIX cu Windows/Linux;

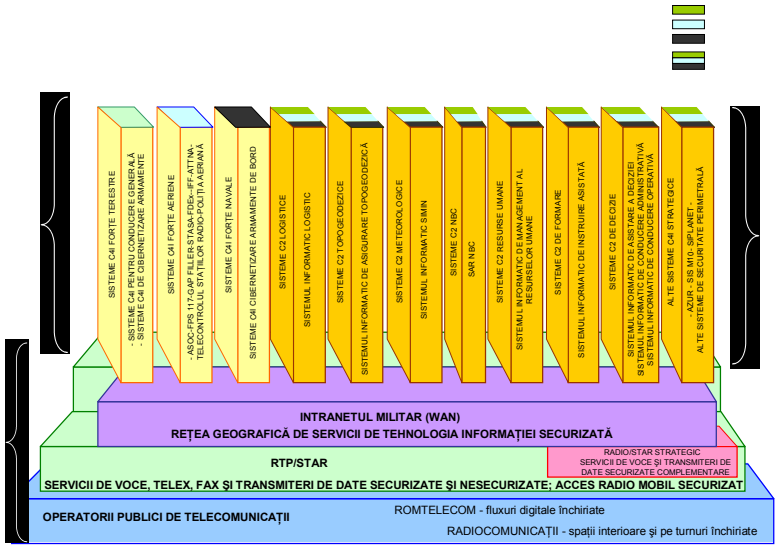
✓ Introducerea managementului de la distanță al locațiilor nedeservite;

✓ Integrarea în sistemul de management a echipamentelor cu funcțiuni noi (echipamente MPS, routere, terminale prin satelit, echipamente radioreleu cu capacitate de 155 Mbps etc.);

✓ Introducerea calculului în timp real al parametrilor liniilor radioreleu, prin utilizarea hărților digitale;

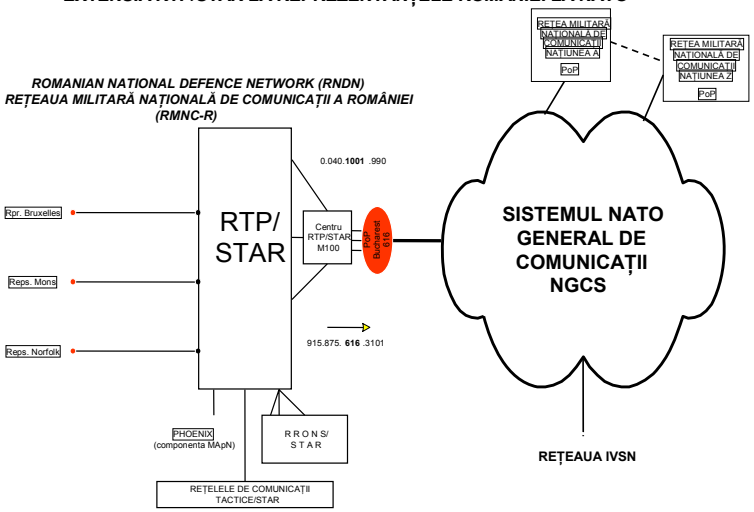
✓ Asigurarea controlului de la distanță al antenelor orientabile pentru accesul mijloacelor mobile.

ANEXE



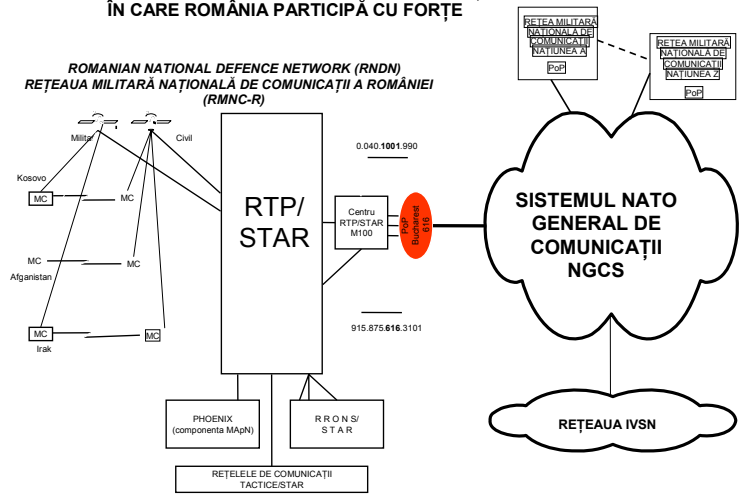
Anexa nr. 1 – Locul şi rolul RTP/STAR şi RRONS/STAR în cadrul SCIAR

EXTENSIA RTP/STAR LA REPREZENTANȚELE ROMÂNIEI LA NATO



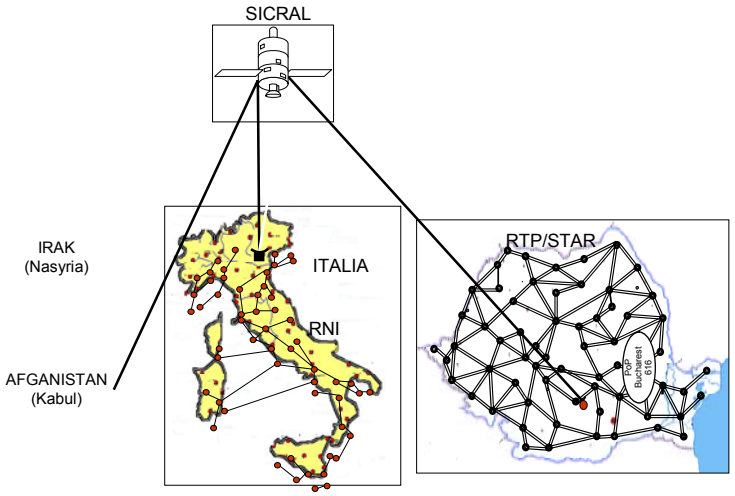
Anexa nr. 2

EXTENSIA RTP/STAR ÎN TEATRELE DE OPERAȚII ÎN CARE ROMÂNIA PARTICIPĂ CU FORȚE



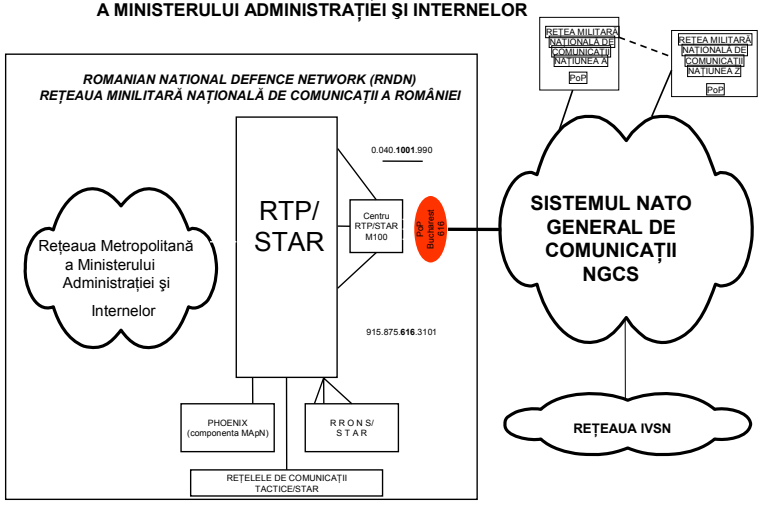
Anexa nr. 3

INTERCONECTAREA RTP/STAR CU REȚEAUA NUMERICĂ INTERFORȚE A ARMATEI ITALIENE

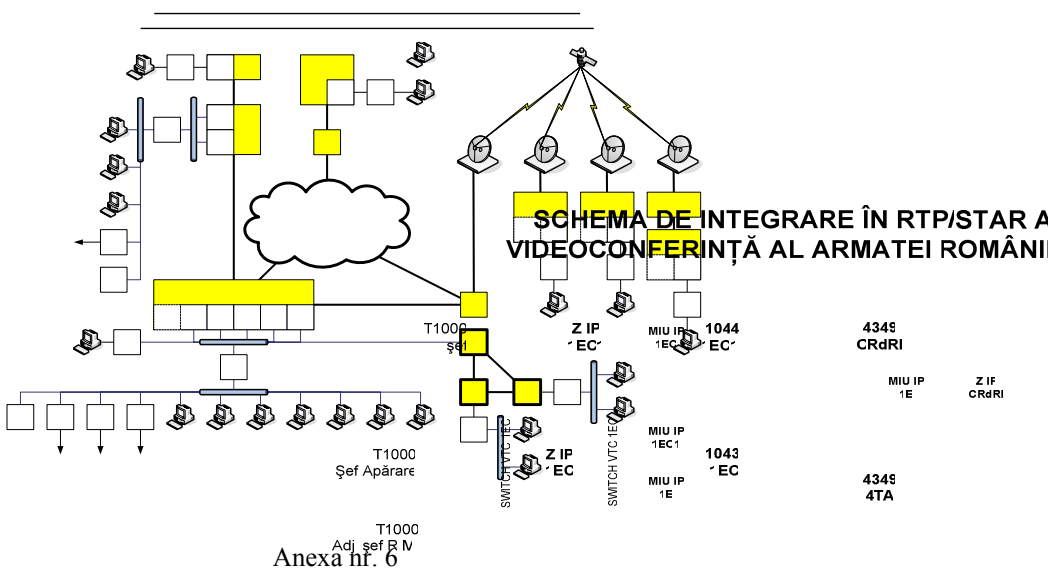


Anexa nr. 4

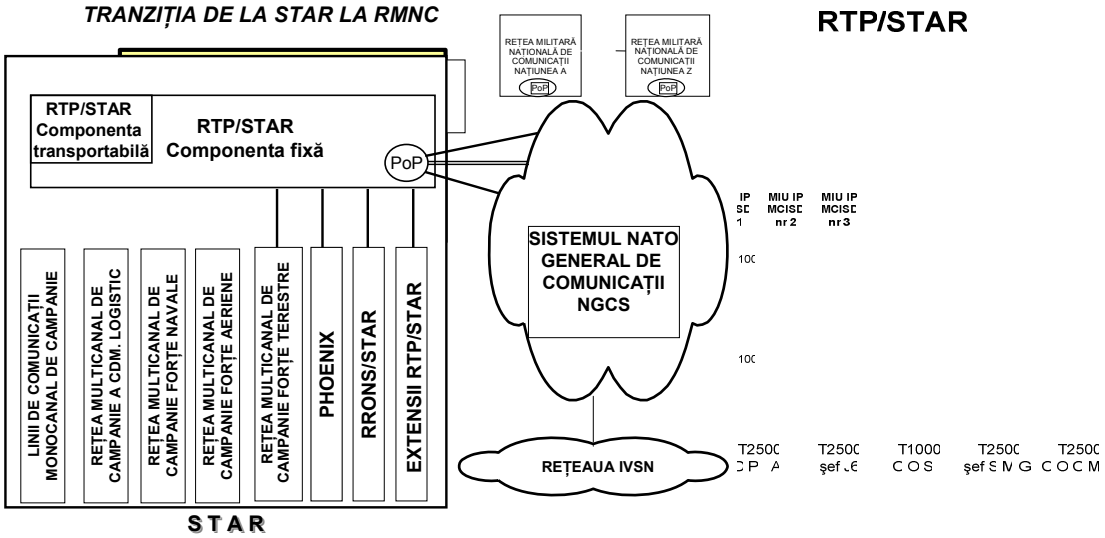
INTERCONECTAREA RTP/STAR CU REȚEAUA METROPOLITANĂ A MINISTERULUI ADMINISTRAȚIEI ŞI INTERNELOR



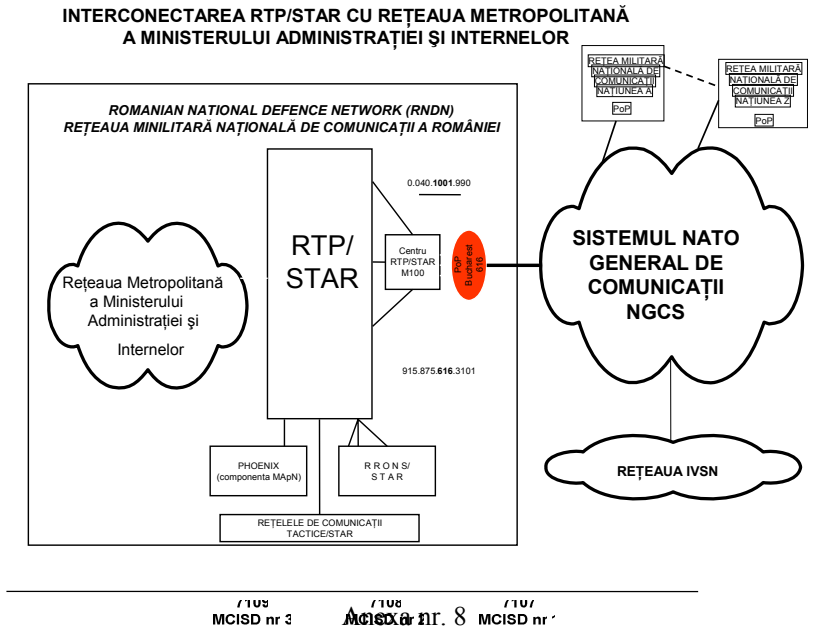
Anexa nr. 5



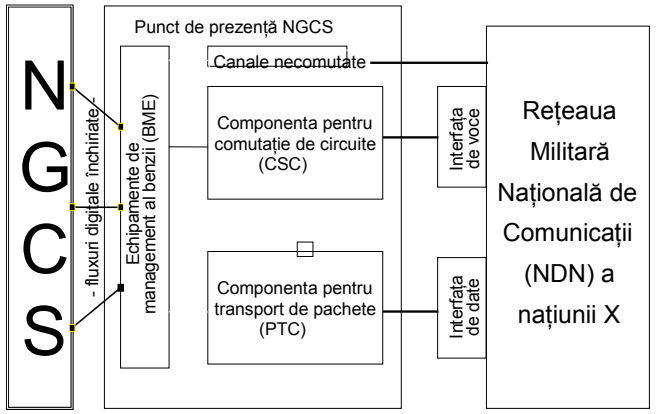
Anexa nr. 6



Anexa nr. 7

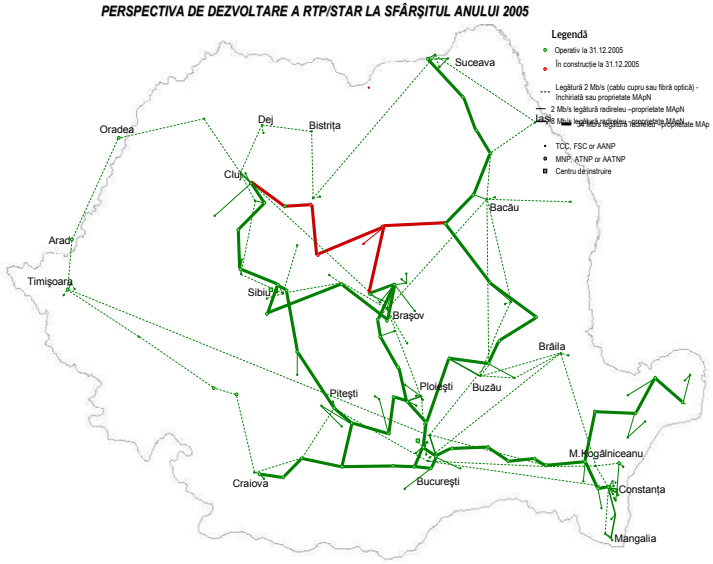


Anexa nr. 8



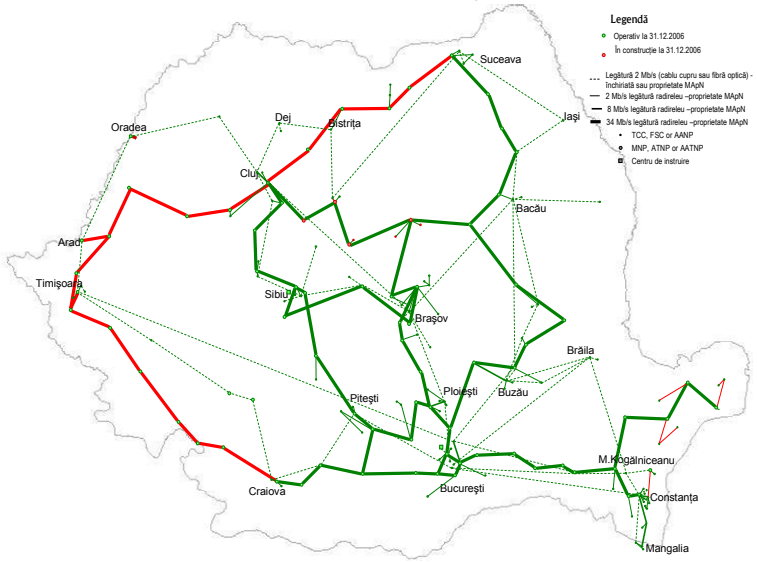
Anexa nr. 9

PERSPECTIVA DE DEZVOLTARE A RTP/STAR LA SFÂRŞITUL ANULUI 2005



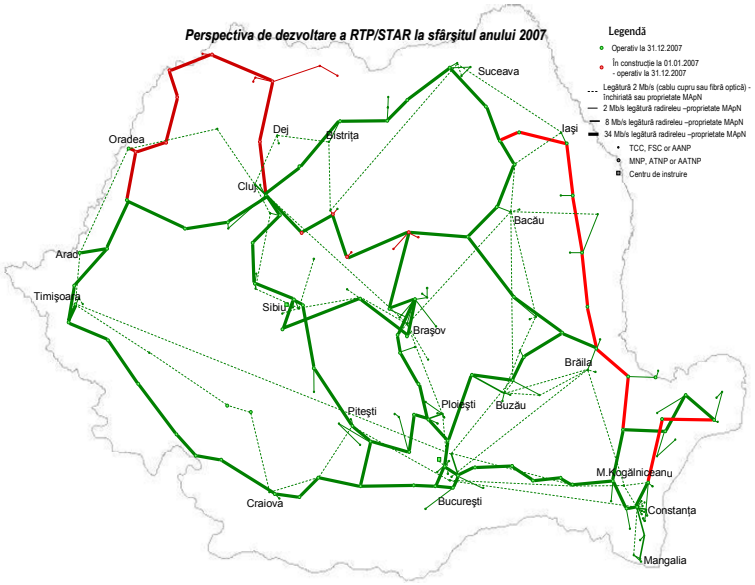
Anexa nr. 10

PERSPECTIVA DE DEZVOLTARE A RTP/STAR LA SFÂRŞITUL ANULUI 2006



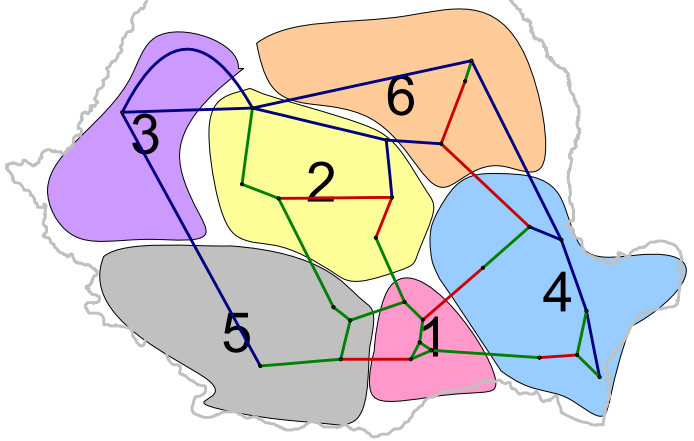
Anexa nr. 11

Perspectiva de dezvoltare a RTP/STAR la sfârşitul anului 2007

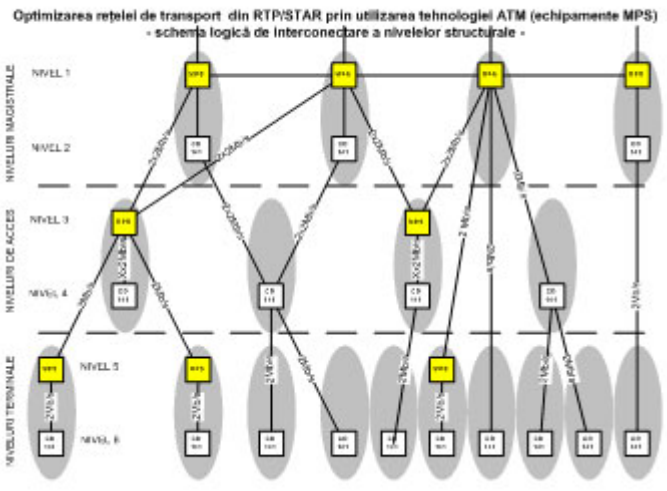


Anexa nr. 12

OPTIMIZAREA REŢELEI MAGISTRALE DE TRANSPORT DIN RTP/STAR PRIN UTILIZAREA TEHNOLOGIEI ATM (ECHIPAMENTE MPS)
- NIVELUL 1 -



Anexa nr. 13



Anexa nr. 14

RĂZBOIUL BAZAT PE REȚEA - DINCOLO DE TEHNOLOGIE

Locotenent-colonel prof. univ. dr. Ion ROCEANU

Din 1998, de când a fost lansat acest concept, de către Cebrovski şi Garstka, a fost o avalanşă de scrieri, evenimente, analize, studii, conferințe, aşa încât am considerat ca fiind inutilă o abordare formală, teoretică a conceptului. Pe de altă parte, am observat că cele mai multe abordări ale specialiştilor militari au vizat fie latura tehnologică exclusivă, fie latura aplicativ-operațională. Considerăm o astfel de abordare normală şi corectă, întrucât se înscrie pe axa fundamentală a conceptului *mobilitate – conectivitate – informație- acțiune eficientă*, unde tehnologia creează plusvaloare acțiunii militare.

Studiind cu atenție, în ultima perioadă, aspectele tehnologice bazate pe teoria rețelisticii şi legătura acestora cu comanda şi controlul acțiunilor militare, am constatat că ceva lipseşte din inelul logic al ciclului OODA (Observation - Orientation - Decision - Action) şi anume conexiunea **informație - cunoaştere.**

Startul acestui articol îl reprezintă sintagma „NCW is more than network is networking”[3]. Atunci se pune întrebarea dacă nu cumva a pune accentul exclusiv pe tehnologie şi ceea ce înseamnă *„rețea”* în tehnologia informației şi comunicațiilor reprezintă o abordare incompletă a conceptului şi, până la urmă, a fenomenului. Avem în vedere aici câteva întrebări la care

[3] David S. ALBERTS, John GARSTKA, Frederick STEIN, *Network Centric Warfare-Developing and Leveraging Information Superiority,* Second Edition, Library of Congress, feb.2000, p.6.

trebuie căutate răspunsuri adecvate, dintre care le enunțăm pe cele la care vom face referire în continuare:

1. Ce înseamnă şi care este configurația rețelei în domeniul informațional? Dar în cel cognitiv?

2. Care este diferența majoră între „sharing of information" şi „sharing of awareness"?

3. Care sunt, din punct de vedere al rețelisticii, parametrii noțiunii de „auto - sincronizare"?

I. Domeniile informațional şi cognitiv - elemente fundamentale ale Războiului Bazat pe Rețea

În lucrarea *Network Centric Warfare-Developing and Leveraging Information Superiority* se subliniază faptul că Războiul Bazat pe Rețea este, de fapt, un nou concept de ducere a acțiunii militare, care are drept scop fundamental obținerea succesului în spațiul de luptă prin realizarea şi exploatarea avantajului informațional, pe toate treptele acestuia: dominație, superioritate şi supremație.

Avantajul informațional este concretizat în superioritatea deciziei, ca rezultat al comenzii şi controlului, iar comanda şi controlul primesc plusvaloare prin sistemele integrate de tipul C4I. Teorie şi practică există suficientă în acest domeniu, acumulate în cei peste 20 de ani, de când a fost lansată, pentru prima dată, ideea de sisteme integrate de comandă şi control.

În acest sens, susținem că Războiul Bazat pe Rețea a venit ca o consecință firească şi ca rezultat al evoluției tehnologiei informațiilor şi comunicațiilor ce a permis perfecționarea sistemelor de comandă şi control, dar şi ca răspuns la noile provocări privind securitatea internațională şi noua fizionomie a conflictelor militare.

Din acest motiv, considerăm că Războiul Bazat pe Rețea trebuie privit mai degrabă din punctul de vedere al transformărilor conceptuale pe care le provoacă artei militare şi

artei conducerii, şi mai puțin din punct de vedere tehnologic. Tehnologia care susține acest concept nu este altceva decât aceeaşi care stă la baza sistemelor de tip C4I, evident, adusă în parametri evolutivi contemporani, dar mai ales gândită cu multă perspectivă. Mai mult decât atât, ultimele realizări în domeniul comunicațiilor şi informaticii, precum şi direcțiile de acțiune de perspectivă din Armata României, realizate sau generate de către Direcția Comunicații şi Informatică, dau consistență acestei afirmații. Din nefericire, tehnologia nu poate înlocui procesele de comandă şi control, astfel încât subliniem că efortul de înțelegere şi adoptare a principiilor Războiului Bazat pe Rețea ar trebui îndreptat către domeniile informațional şi cognitiv.

Primul pas în abordarea conceptelor care definesc şi încadrează comanda-controlul îl constituie acceptarea unui limbaj special, care să conțină ideile de bază de la care se poate porni în înțelegerea acestor concepte.

Înțelegerea mediului de comandă-control presupune înțelegerea mediului global în care au loc acțiunile, mediu privit ca un ansamblu de trei domenii, potrivit figurii nr. 1, care formează o partiție primară.

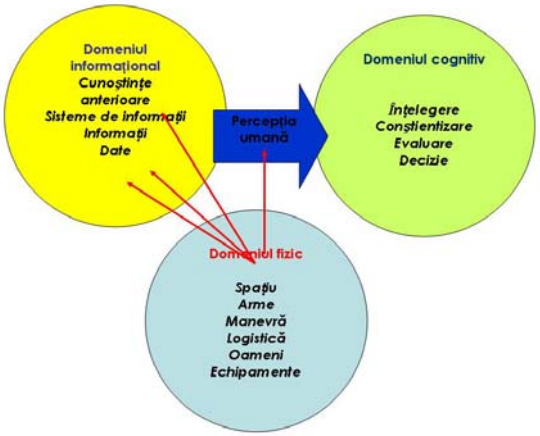


Figura nr. 1 - Domeniile mediului global al acțiunii militare

Conceptul RBR propune abordarea pe domenii a spațiului de luptă, fiecare cu conținut şi elemente proprii, interconectate între ele, care să conducă în final la o înțelegere unitară a situației, decizie în condiții de risc minim şi acțiune convergentă.

Domeniul fizic este domeniul tradițional al războiului. În cuprinsul său lovirea, protecția şi manevra au loc în mediile terestru, maritim, aerian şi spațial. Comparativ, elementele acestui domeniu sunt cel mai uşor de măsurat şi, în consecință, puterea combativă a fost măsurată primar în acest domeniu. Două importante matrice pentru măsurarea puterii combative în acest domeniu, letalitatea şi supraviețuirea, au fost şi continuă să fie pietrele de temelie ale cercetării operațiilor militare.

Domeniul cognitiv este domeniul minții luptătorului şi al populației care-l sprijină, domeniul unde luptele şi războaiele sunt câştigate şi pierdute. Este domeniul intangibilităților: conducerea, moralul, coeziunea unității, nivelul de instruire şi experiența, înțelegerea situației şi opinia publică. Acesta este, de asemenea, domeniul unde tacticile, tehnicile şi procedurile se reelaborează. Caracteristicile acestui domeniu sunt extrem de dificil de măsurat, luând în considerare că fiecare subdomeniu (fiecare minte individuală) este unic.

Domeniul informațional este domeniul unde există informația. Este domeniul unde informația e creată, manipulată şi distribuită, domeniul care facilitează comunicarea informației între luptători. Aici se exercită comanda şi controlul forțelor militare moderne şi este reelaborată intenția comandantului. Prin urmare, creşte domeniul informațional care trebuie protejat şi apărat, pentru a permite unei forțe să genereze putere combativă împotriva acțiunilor ofensive ale unui adversar. Se poate afirma că în toate luptele importante, pentru obținerea

superiorității informaționale, domeniul informațional este „punctul zero”[4].

Altfel spus, există o singură realitate sau un singur domeniu fizic, care este convertit în informații (date, informații, intelligence) de către sistemele informaționale şi, ulterior, în cunoştințe, de către factorul uman (sau sistemele-expert).

Prin antrenament şi acumulare de experiență, se încearcă elaborarea unui „şablon” al activităților cognitive ale decidenților, care, însă, în mod cert, prezintă diferențe semnificative printre decidenții din structuri, generații, țări diferite etc.

La o privire mai atentă şi trecând dincolo de repulsia pe care o provoacă şablonismul, în general, trebuie să recunoaştem că în domeniul militar acesta are un rol bine definit, chiar benefic, în măsura în care face parte din compatibilitate şi interoperabilitate. Pe de altă parte, vom observa în continuare că esența conceptului „auto - sincronizare” este reprezentată tocmai de nivelul de uniformitate obținut în domeniul instruirii, comenzii şi controlului.

Dar ce este avantajul informațional? Avantajul informațional este o condiție a domeniului informațional, creată atunci când un competitor este capabil să stabilească o poziție informațională superioară vizavi de adversar. Corespunde la o balansare în favoarea unui actor, în domeniul informațional, către un avantaj relativ al informației. Conceptul avantajului informației nu este nou. Comandanții au gândit întotdeauna şi câteodată au obținut un avantaj informațional decisiv asupra adversarilor. Într-adevăr, surpriza, unul dintre principiile fundamentale ale războiului, poate fi văzută ca un tip de avantaj informațional, pe care o forță este capabilă să o stabilească împotriva alteia.

[4] David S. ALBERTS, John GARSTKA, Richard HAYES, David SIGNORI, *Understanding Information Age Warfare*, CCR Publications, aug.2001.

Un avantaj relativ al informației poate:

• fi persistent sau tranzitoriu;

• exista în unele arii ale spațiului de luptă, dar nu în altele;

• fi măsurat, în contextul unei misiuni sau set de misiuni;

• fi creat prin luarea acțiunilor de reducere a nevoilor proprii de informații şi/sau creşterea nevoilor de informații ale adversarului;

• fi obținut prin conducerea sinergică a operațiilor informaționale, asigurarea informațiilor, obținerea şi exploatarea acestora.

Indiferent de cine a dezvoltat, particularizat sau interpretat conceptul, pot fi extrase câteva dintre elementele comune, care, de fapt, reprezintă esența demersului de a pune în centru rețeaua, care, la rândul său, este constituită din trei grile sau planuri ierarhice: grila senzorilor, grila informațională şi grila acțională. Această rețea este distribuită sau, mai bine spus, are conexiuni în cele trei domenii enunțate anterior.

Modelul de principiu al confruntării în spațiul de luptă propus de Războiul Bazat pe Rețea este prezentat în figura nr.2[5].

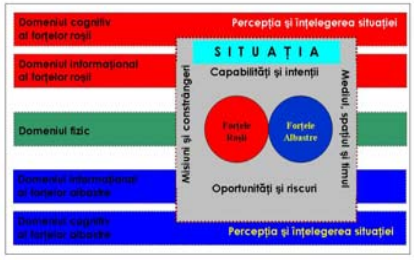


Figura nr.2 - Modelul confruntării în spațiul de luptă

[5] Ion ROCEANU, **Fundamentele Sistemelor C4I**, Bucureşti, Ed. UNAp, 2004.

II. Elemente-cheie din domeniile fizic, informațional şi cognitiv care intervin în comanda şi controlul acțiunii militare

Următorul set de 12 concepte (elemente), considerate de bază, este necesar pentru modelarea procesului de comandă-control. Aceste concepte au fost definite în relație cu cele trei domenii anterior menționate: percepția; informația; transmiterea informației; cunoaşterea; transmiterea cunoştințelor; înțelegerea; conştientizarea; comuniunea convingerilor; decizia; acțiunea; colaborarea; sincronizarea.

2.1. Percepția

Există două tipuri de percepție: directă şi indirectă.

Percepția directă are loc când se descoperă un obiect, eveniment sau fenomen în domeniul fizic printr-unul din simțuri (cum ar fi: văzul, auzul sau mirosul) şi percepția este înregistrată direct în domeniul cognitiv.

Percepția indirectă are loc când un senzor, indiferent de tipul acestuia, este implicat de către om pentru a-i uşura observarea unui aspect din domeniul fizic.

Observația indirectă se formează în domeniul informației, unde aceasta este filtrată de percepția umană şi ajunge în domeniul cognitiv.

Observația directă e formată prin trecerea directă din domeniul fizic în cel cognitiv. De mii de ani, observația directă a fost modul de bază folosit pentru obținerea informațiilor despre câmpul de luptă.

Începând cu secolul al XVII-lea, observarea directă a fost înlesnită de tehnologie (telescopul sau binoclul). În cel de-al doilea război mondial au fost folosiți noi senzori pentru radiodetecție – radarul - şi pentru detecția acustică - sonorul.

Aceştia au mărit considerabil posibilitățile de a observa câmpul de luptă, reducând incertitudinile cu privire la poziția avioanelor şi submarinelor care fuseseră nedetectabile până atunci.

Astăzi se foloseşte o gamă bogată de senzori (ochelari de vedere pe timp de noapte, senzori termici, sateliți etc.) pentru a ajuta la observarea câmpului de luptă.

Când tehnologia este folosită pentru a obține date, ea devine parte a domeniului informațional. Acestea sunt observate numai după ce trec prin filtrul uman şi ajung în domeniul cognitiv.

2.2. Informația

Cuvântul *informație*, în întrebuințarea obişnuită, se referă la diferitele puncte din spectrul informațional, de la date la cunoştințe. Totuşi, ca termen de bază, informația este rezultatul aşezării observațiilor individuale (oferite de senzor) într-un context cu înțeles.

Data/informația este reprezentarea faptelor în mod individual, a concepțiilor sau instrucțiunilor într-un mod corespunzător pentru comunicație, interpretare sau procesare de către om sau mijloacele automatizate. Exemple de date ar fi sesizările radar, observațiile senzorilor şi datele înregistrate.

Termenul „prelucrarea datelor" (procesare) este des folosit, deşi, de fapt, toate datele sunt procesate. Când se foloseşte acest termen, se intenționează sugerarea procesării suplimentare. Se creează informație, chiar dacă se foloseşte observarea indirectă. Multe din observații pot fi pierdute, lăsate în domeniul informației sau filtrate de către „lentilele" de percepție ale indivizilor.

2.3. Transmiterea informației

Punerea în comun a informației este o interacțiune care poate avea loc între două sau mai multe entități în domeniul informațional (acestea pot fi oameni, baze de date sau programe). Abilitatea de a împărți informația este esențială pentru a putea dezvolta un stadiu al cunoaşterii comune, după cum este esențială pentru colaborare şi/sau sincronizare.

Pot fi implicate multe entități, iar forma de transmitere a informației poate varia semnificativ. Când două sau mai multe persoane sunt situate la mică distanță, informația poate fi schimbată între acestea prin voce, conversând una cu cealaltă, sau prin alte tehnici, care implică mişcări ale corpului, ca semnele făcute cu mâinile, gesticulările. „Limbajul corpului" poate fi folosit în comunicare, dar poate fi uşor înțeles greşit. În unele situații, expresia privirii poate fi întrebuințată pentru a spori sensul ideilor sau conceptelor comunicării.

Când două sau mai multe persoane sunt geografic situate la distanță, pentru transmiterea informațiilor trebuie folosite câteva tipuri de tehnologie (telefonul, poşta electronică, teleconferința). În timp, diferite tipuri de tehnologie au fost dezvoltate pentru a capta, înmagazina şi transmite informațiile. După cum se va dezbate mai târziu, tehnologia informațiilor defineşte granițele şi capabilitățile domeniului informațional.

2.4. Cunoaşterea

Cunoaşterea presupune concluzii trase din modelul sugerat de o informație disponibilă. Cunoaşterea unei situații rezultă din concluziile care pot fi trase dintr-o informație ce se referă la acea situație, de exemplu tipul şi locul de luptă.

Cunoaşterea există atât în domeniul informației, cât şi în cel cognitiv. De exemplu, doctrina este adesea un mijloc de a pune în comun informațiile despre o situație şi un mod de a se reacționa la aceasta corespunzător entităților spațiilor.

Cunoştinţele sunt acumulate în domeniul cognitiv, ca rezultat al învăţării, înmagazinate în domeniul informaţiei. Încărcarea în domeniul cognitiv individual se poate face prin câteva căi, incluzând:

- instruirea anterioară, antrenamentul sau experienţa;
- experienţa directă în domeniul fizic;
- interacţiunea cu alţi indivizi;
- interacţiunea cu domeniul informaţiei.

Cunoaşterea poate, de asemenea, să fie mutată din domeniul cognitiv în domeniul informaţiei, atunci când este transmisă altor indivizi, sub forma instrucţiunilor sau regulilor de manevrare, ori pentru stocare în computere.

2.5. Transmiterea cunoştinţelor

Într-o oarecare măsură, transmiterea cunoştinţelor există în toate eforturile depuse de oameni, pentru a colabora. Instrucţia şi doctrina au fost angajate de-a lungul istoriei să dezvolte un înalt grad al transmiterii cunoştinţelor, avertizărilor, în rândul trupelor, astfel încât acestea să înţeleagă şi să reacţioneze la situaţii în modul indicat. Transmiterea cunoştinţelor este esenţială pentru ca elementele independente ale unei forţe să-şi poată coordona acţiunile şi pentru ca aceasta să devină vitală, mai ales când forţele încearcă să-şi coordoneze acţiunile fără comunicaţii sau să se autosincronizeze. Gradul în care transmiterea cunoştinţelor poate fi dezvoltată are o influenţă semnificativă asupra naturii comenzii şi controlului, naturii şi cantităţii comunicărilor necesare dezvoltării şi întreţinerii transmiterii de avertizări, uşurinţei şi gradului în care forţele pot fi sincronizate.

Există, nu de puţine ori, tendinţa de a pune semnul egalităţii între transmiterea informaţiilor şi transmiterea cunoştinţelor, ceea ce este eronat, nu numai din punct de vedere al comunicării propriu-zise, dar şi al suportului tehnic, sau, mai degrabă, al conţinutului digital. O informaţie poate fi transmisă

ca fiind o succesiune de date sau, pur şi simplu, ca un mesaj, ştire, enunţ limitat la a defini un eveniment (obiect). Transmiţătorul şi receptorul unei informaţii nu trebuie neapărat să fie compatibili din punct de vedere al nivelului de educaţie şi instruire, cultural sau de altă natură şi, mai mult decât atât, aceştia nu personalizează conţinutul.

Transmiterea de cunoştinţe înseamnă, în primul rând, compatibilitate între comunicatori, înseamnă logica prelucrării superioare a informaţiei, înseamnă personalitate şi experienţă adăugate, înseamnă intervenţia cognitivului asupra evenimentelor. Din acest motiv, conţinutul comunicării este total diferit între informaţie şi cunoştinţe, iar structura suportului tehnologic este diferenţiată, mai ales în domeniul bazelor de date care se transformă în „knowledge center”. Mai mult decât atât, pentru a face schimb de cunoştinţe, este necesar a avea aceeaşi bază educaţională, ceea ce presupune într-o mare măsură compatibilizarea sistemelor educaţionale şi conţinutul acestora. Acest deziderat a făcut posibil sau, mai degrabă, a generat apariţia sistemelor educaţionale cu conţinut distribuit, tip e-Learning. Este cunoscut proiectul american ADL (Advanced Distributed Learning), lansat în anul 1999 şi care îşi propune difuzarea de conţinut educaţional şi instruire acolo unde este nevoie şi când este nevoie.

Schimbul de cunoştinţe, alături de schimbul de convingeri (conştientizări - awareness) stă la baza conceptului autosincronizare, aşa cum schimbul de informaţii asigură imaginea operaţională comună a spaţiului de luptă, conform figurii nr. 3.

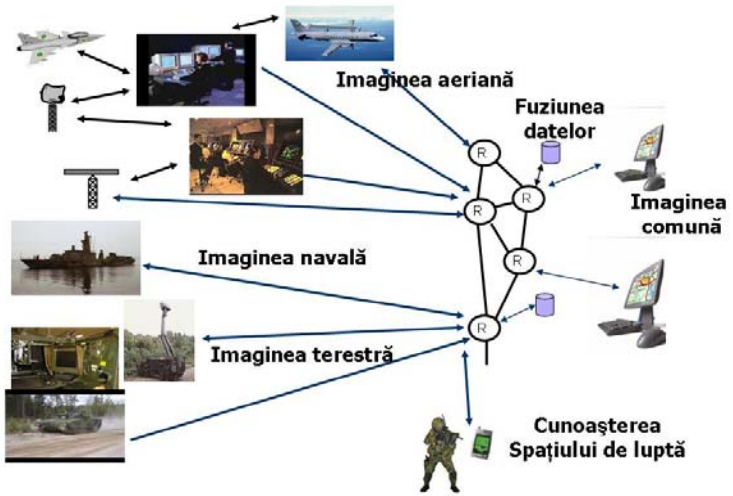


Figura 3 - Imaginea operațională comună

2.6. Înțelegerea

Înțelegerea implică deținerea unui nivel suficient de cunoştințe care să permită obținerea unor concluzii despre posibilele consecințe ale situației, cât şi o suficientă cunoaştere a situației pentru a prezice viitoare modele. Situația conştientizată este focalizată pe ceea ce este cunoscut din situațiile trecute şi prezente, în timp ce înțelegerea unei situații militare este focalizată pe ceea ce poate deveni situația şi cum vor avea impact asupra situației rezultate acțiuni diferite.

2.7. Conştientizarea

Conştientizarea se referă la o situație şi la rezultatul interacțiunilor complexe dintre cunoştințele (şi convingerile) anterioare şi actuala percepție a realității.

Fiecare individ are un mod unic de a conştientiza, indiferent de situație. Educația profesională şi instruirea sunt folosite pentru a le furniza militarilor aceleaşi date, informații şi cunoştințe actualizate, care să conducă la obținerea unui mod similar de avertizare.

2.8. Comuniunea convingerilor

Comuniunea convingerilor reprezintă o stare existentă în domeniul cognitiv, când două sau mai multe entități sunt în măsură să dezvolte cunoştințele similare despre o situație anume. Gradul de asemănare cerut (sau de diferențe tolerabile) va depinde de tipul şi gradul de colaborare şi sincronizare necesar.

O multitudine de factori influențează gradul în care un stadiu al comuniunii de cunoştințe poate fi dezvoltat între două sau mai multe entități (similitudinile şi deosebirile punctelor de vedere, cultura, limbajul şi urmărirea intereselor). Convingerile comune reprezintă o cerință esențială pentru abilitatea de a sincroniza acțiunile în domeniul fizic, în absența unui plan detaliat. Evaluarea stadiului de comuniune a cunoaşterii este mult mai complexă decât măsurarea gradului de comuniune a informațiilor; practic, nu se poate măsura direct, trebuie măsurat şi apreciat indirect, având la bază evaluarea comportamentului şi chestionarea directă a subiecților.

2.9. Decizia

Deciziile, de asemenea, sunt situate în domeniul cognitiv. Ele reprezintă alegeri, opțiuni asupra a ceea ce este de făcut. Lărgirea viziunii asupra deciziei presupune includerea tuturor deciziilor într-un model conceptual al spațiului misiunii, indiferent de nivelul de la care emană, dacă afectează semnificativ rezultatele pe câmpul de luptă. De exemplu, ordinele pot transmite unei forțe - ce, unde şi când are ceva de

făcut. Pentru a stabili o nouă misiune forțelor subordonate, organizația trebuie să pornească un nou proces de decizie. Pe de altă parte, subordonații pot pune în aplicare intenția comandantului, luând la rândul lor o serie de decizii.

Deşi deciziile sunt descrise ca rezultat al înțelegerii, ele pot fi luate, în mod evident, şi în lipsa oricărei înțelegeri. Asemenea decizii pot să fie întâmplătoare şi, în acest caz, este puțin probabil să fie eficiente într-un context militar, dar se presupune că forțele şi comandanții acestora vor avea întotdeauna un oarecare nivel de cunoştințe şi de conştientizare asupra situației. De aceea, implicit, ei au un nivel ridicat de înțelegere şi deciziile lor sunt direcționate spre un scop.

2.10. Acțiunea

Acțiunile se desfăşoară în domeniul fizic şi sunt determinate de deciziile în domeniul cognitiv, care, fie sunt direct transformate în acțiune, fie sunt transportate dintr-un domeniu al informației către altul. Nivelul individual al cunoaşterii influențează nivelul de conştientizare, gradul de înțelegere şi procesul de luare a deciziilor. Deciziile simple sunt acelea care implică o selecție dintr-un set de opțiuni în care cea mai simplă spune dacă să se acționeze sau nu (a trage).

Deciziile complexe implică dezvoltarea unui set de opțiuni, a criteriilor de alegere şi combinarea regulilor prin care aceste criterii sunt integrate. Dezvoltarea, aprecierea (evaluarea) şi selectarea cursurilor de acțiune de la nivel batalion în sus este, în general, un tip de decizie complexă.

2.11. Colaborarea

Colaborarea este un proces care are loc între două sau mai multe entități în domeniul cognitiv şi implică întotdeauna lucrul în comun pentru atingerea unui scop. Această

particularitate îi dă distincție în fața simplelor comuniuni ale datelor şi informației, cunoştințelor sau a convingerilor.

În cadrul colaborării, prin extensie, se pot aborda şi problematicile cooperării şi coordonării.

Cooperarea implică o punere în comun a datelor, informațiilor, cunoştințelor şi percepțiilor referitoare la anumite fapte şi situații, presupunând lucrul împreună al tuturor actorilor ce urmăresc îndeplinirea unui scop comun.

Scopul cooperării este acela de a permite o înțelegere şi o perspectivă similară asupra situației, concomitent cu sincronizarea, în vederea organizării optime a activităților, astfel încât să fie evitate redundanțele ori impedimentele reciproce şi să se obțină un efect maxim raportat la scopul propus.

Cooperarea este folosită pentru sporirea eficienței în îndeplinirea unei misiuni, lucru cuantificabil prin intermediul unor măsurători corespunzătoare, numite măsuri ale performanței (MOP). Aceste standarde au la bază analiza capacităților după îndeplinirea misiunii, dar şi rata cheltuielilor în timpul îndeplinirii misiunii. La aceste standarde se pot adăuga cele de măsurare a eficienței forței (MOFE) sau de măsurare a eficienței politicii (MOPE).

Cooperarea se bazează pe câțiva factori definitorii: timpul necesar, continuitatea, amploarea, densitatea informațiilor, domeniul, structura, rolul participanților şi modul de interrelaționare al acestora.

Reuşita unei activități de cooperare constă, în primul rând, în posibilitatea participanților de a beneficia de aceleaşi informații în timp util şi de a le interpreta sau utiliza după aceleaşi reguli. În acest demers un rol deosebit îl joacă sistemele tehnice, în mod deosebit cele bazate pe tehnologia informațiilor şi comunicațiilor, care sunt capabile să asigure aceste cerințe. Utilizarea în acelaşi timp a informațiilor necesare poate fi realizată, în mai multe moduri, astfel:

- modelul clasic al schimbului de informații, caracteristic sistemelor de tip platformă, în care întâlnim un transmițător de informații şi unul sau mai mulți receptori. Acest model are o seamă de dezavantaje, printre care timpul mare de distribuire a informațiilor, necorelarea cantității de informație cu necesarul specific al participanților (toți primesc aceleaşi informații în acelaşi timp). Modelul solicită canale de comunicații între toți participanții la cooperarea respectivă, iar aceste canale pot fi cele clasice, end-to-end, prin mijloace de comunicații sau pot fi din cele distribuite de genul poştă electronică, mesagerie vocală sau workflow (lucru colaborativ);

- modelul oferit de conceptul Război Bazat pe Rețea, care preia principiile sistemelor C4I - se sprijină pe o bază de date centrală la care pot avea acces controlat toți cei implicați într-o activitate de colaborare asociată îndeplinirii unei misiuni. În acest fel, este suficient ca cei implicați să primească strict datele referitoare la cooperare. Celelalte informații necesare în cantitatea dorită, la momentul optim, sunt decise de fiecare în parte sau, în anumite situații, coordonat, de un responsabil de misiune.

Timpul necesar cooperării pentru îndeplinirea unei misiuni variază de la caz la caz. Orice activitate pe care o implică procesul de cooperare – schimbul de informații, stabilirea punctelor şi momentelor de coordonare, stabilirea regulilor de operare comune – presupune un anumit consum de timp. Şi cooperarea poate diferi din punct de vedere al continuității sau al gradului de sincronizare între comandamente şi între acestea şi forțele care operează în spații geografice distincte şi la distanțe mari sau foarte mari.

Coordonarea este definită ca fiind un aranjament al forțelor, mijloacelor şi acțiunilor în timp şi spațiu în jurul unei misiuni (scop). Ea implică toate cele trei domenii – cognitiv, informațional şi fizic, este generată de cerințele din domeniul fizic, concepută şi fundamentată în domeniul cognitiv şi se

realizează bazându-se pe elementele din domeniul informațional.

Coordonarea este influențată de trei factori:

Complexitatea acțiunii este generată, pe de o parte, de existența unui număr mare de entități cu grade diferite de libertate a acțiunii şi, pe de altă parte, de dorința de a modela efortul participanților pentru atingerea scopului comun.

Eterogenitatea este generată de nevoia de coordonare a entităților provenite din medii cu culturi diferite, nivel de instruire diferit, dotare şi doctrine diferite etc.

Ritmul rapid este caracteristic acțiunilor militare moderne, influențat în mare măsură de explozia informațională şi extinderea capacităților de mobilitate ale participanților în acțiuni militare.

2.12. Sincronizarea

Sincronizarea se desfăşoară în domeniul fizic, este cel mai important aranjament al lucrurilor şi efectelor în timp şi spațiu, rezultatul planificării detaliate şi al conştientei coordonări sau colaborări.

Totuşi, poate să fie şi rezultatul comuniunii de convingere cu privire la o situație care asigură o adecvată ghidare pentru acțiune.

III. Autosincronizarea

Autosincronizarea (self-synchronization) constituie modalitatea de interacțiune a două sau mai multe entități. Ea poate căpăta forme multiple în spațiul luptei, dar RBR îi scoate în evidență potențialul deosebit pentru rezolvarea unor situații din domeniul logisticii, în sprijinul cu foc, sprijinul aerian nemijlocit, în general în misiuni unde se cer soluții imediate. Sunt misiuni complexe, cu riscuri pentru trupele proprii, executate de regulă într-un mediu dinamic. Oportunitățile RBR

pentru atingerea omniscienței forțelor oferă soluții noi pentru executarea unor asemenea misiuni, ajungându-se până la acțiuni autonome ori auto-asumarea unor misiuni.

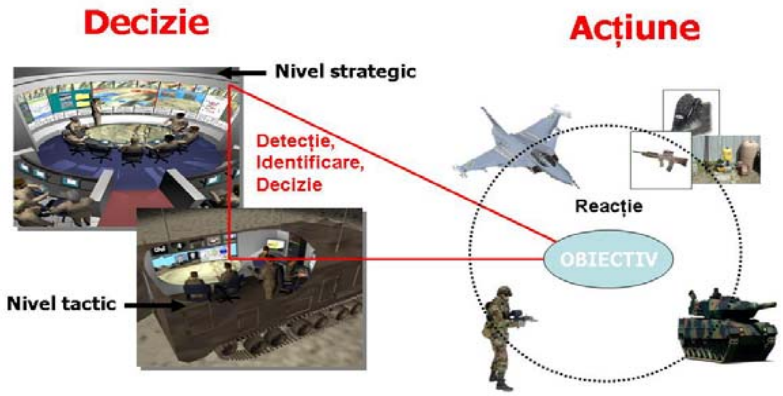


Figura 4 - Autosincronizarea

Autosincronizarea este abilitatea unei forțe bine informate de a organiza şi sincroniza activități complexe ale războiului de jos în sus. Principiile organizatorice sunt unitatea de efort, intenții clare şi articulate ale comandantului, precum şi reguli de angajare atent alcătuite.

Autosincronizarea este permisă de un înalt nivel de cunoştințe privind forțele proprii, forțele adversarului şi toate elementele corespunzătoare mediului de operații, depăşeşte pierderea capacității de luptă inerentă în sincronizarea directă a comenzii de sus în jos, caracteristică multor doctrine convenționale şi converteşte lupta de la o funcție treptată la o funcție continuă de mare viteză.

Un exemplu al acestui tip de C2 descentralizat necesită ca decidenții de la nivelurile inferioare să fie ghidați doar de instruirea lor, înțelegerea intenției comandantului şi grija față

de situație, în părțile relevante ale câmpului de luptă. În unele variante ale acestui concept există o dispoziție pentru managementul prin excepție (comandantul poate nega deciziile luate la nivelurile inferioare pe baza unei excepții). Submarinele operează adesea în acest fel, pentru a evita comunicările ce ar putea dezvălui locațiile sau misiunile.

În acelaşi timp în care sincronizarea devine mult mai importantă în operațiile militare, obținerea sincronizării devine mult mai provocatoare dintr-un număr de motive. Acestea includ complexitatea crescută, creşterea neomogenității şi derularea rapidă a evenimentelor.

Creşterea complexității

Au fost întotdeauna un mare număr de entități cu grade diferite de libertate în operațiile militare. Totuşi, astăzi, se poate observa o dorință pentru mai multă precizie şi nevoia crescândă ca entitățile de pe câmpul de luptă să lucreze împreună. Mai mult, din cauza letalității crescute de pe câmpul de luptă, datorită îmbunătățirii atât în domeniul senzorilor, cât şi al armamentelor, există şi o tendință spre operațiile distribuite cu forțe dispersate, care trebuie să opereze concertat pentru a controla câmpul de luptă. Rezultanta, necesară pentru legătura strânsă şi efectele precise, este complexitatea crescută a operațiilor.

Creşterea neomogenității

Coordonarea multiplelor eşaloane şi entități organizaționale cu diferite culturi, procese, percepții şi cicluri de răspuns, a fost o considerație în mai multe conflicte anterioare. Totuşi, rolul central al operațiilor de război de coaliție în strategia de securitate necesită a fi interoperabil militar cu o mulțime de potențiali aliați, la un nivel nemaiîntâlnit. Apariția operațiilor altele decât războiul impune capacitatea de a fi interoperabil cu multe organizații neguvernamentale. Datorită

incertitudinii referitoare la amenințare şi la tipul operației, vor fi dificil de raționalizat multele diferențe care trebuie depăşite pentru a obține nivelul de interoperabilitate necesar obținerii unui grad ridicat de sincronizare în operațiile coaliției.

Autosincronizarea poate fi înțeleasă şi ca o extensie mai largă a libertății de acțiune prin completarea acesteia cu libertatea de decizie şi asumarea riscului, bazate pe înțelegerea unitară a faptelor şi un nivel comun de instruire şi educare.

Considerăm că autosincronizarea va trebui privită prin prisma a cel puțin trei situații distincte, astfel:

1. În acțiunile militare exclusiv naționale, auto-sincronizarea este posibilă deoarece toți cei implicați în decizie şi acțiune aparțin aceleiaşi culturi, au fost educați şi instruiți în acelaşi sistem, au aceleaşi valori morale etc. Dacă instruirea acestora s-a efectuat pe bază de standarde, dacă standardele au fost îndeplinite, dacă au experiență de lucru în comun, aplică aceleaşi seturi de criterii şi analiză, atunci se poate ajunge la asumarea deciziei, deoarece se presupune că toți ceilalți implicați au ajuns la aceeaşi concluzie.

2. În operațiile militare multinaționale de tip alianță, auto-sincronizarea este posibilă dacă cei implicați acționează exclusiv pe bază de proceduri de operare standard, validate în timp, în practică, prin exerciții şi eventual prin situații reale. Pentru acest lucru este totuşi nevoie de crearea unui sistem de instruire comun, de exerciții şi antrenamente, de interoperabilitate deplină în domeniul tehnologiei, cadru juridic unitar etc.

3. În cazul acțiunilor militare cu o structură de forțe şi comandă multinațională de tip coaliție, problema devine foarte grea, dacă nu imposibilă. Aceleaşi considerente, enunțate mai sus ca fiind puncte de sprijin pentru atingerea autosincronizării, devin în acest caz puncte de divergență. Este greu de imaginat că nivelurile de instruire din SUA şi din Croația, spre exemplu,

o țară cu o armată destul de modernă, sunt compatibile şi că decidenții cu acelaşi rang pot fi complementari.

Concluzii

Tehnologia informației şi comunicațiilor a evoluat foarte mult şi oferă acum soluții pentru multe dintre preocupările omenirii, şi, implicit, pentru domeniul militar. Este de asemenea evident, evidențiere mult vizibilă în business, că nu tehnologia reprezintă punctul nevralgic al unui sistem, ci cultura organizațională şi structura operațională. Din acest motiv, subliniem încă o dată că, în ceea ce priveşte Războiul Bazat pe Rețea, tehnologia oferă soluții la toate provocările teoretice enunțate de către inițiatorii conceptului sau de către responsabilii militari, dar nu poate înlocui aspectele referitoare la resursa umană. Considerăm că este momentul să fie luată o decizie în ceea ce priveşte acest concept în Armata României, definirea sa, crearea unor responsabilități de studiu şi cercetare, precum şi de aplicare şi de generare a unui document-cadru care să pună bazele teoretice ale abordării unitare. Dacă acest aspect va fi rezolvat şi va fi stabilit un „punct 0”, vor fi posibile dezvoltări ulterioare care vor putea fi aplicabile în practică.

BIBLIOGRAFIE:

[1] David S. ALBERTS, John GARSTKA, Frederick STEIN, **Network Centric Warfare-Developing and Leveraging Information Superiority**, Second Edition, Library of Congress, feb.2000

[2] David S. ALBERTS, John GARSTKA, Richard HAYES, David SIGNORI, *Understanding Information Age Warfare*, CCR Publications, aug.2001

[3] Ion ROCEANU, **Fundamentele Sistemelor C4I**, Bucureşti, Ed. UNAp, 2004

[4] *UK Journal of Defence Science*, Volume 8, Number 3, September 2003
[5] *NETWORKED ENABLED CAPABILITY - An Introduction*, Ministry of Defence (United Kingdom), Version 1.0, Aprilie 2004
[6] *Aspecte teoretico-metodologice şi modalităţi de aplicare a conceptului Război Bazat pe Reţea în Armata României, corespunzător „Structurii de forţe 2007”*, Centrul de Studii Strategice de Securitate, Universitatea Naţională de Apărare, 2003.

ROLUL INFORMAŢIILOR MILITARE ÎN RĂZBOIUL BAZAT PE REŢEA

General-locotenent conf.dr.ing. Sergiu MEDAR

Prin excelenţă, serviciile de informaţii au avut întotdeauna o bună capacitate de adaptare, derivată din specificul activităţii, fiind primele organizaţii care au întrezărit schimbările şi tendinţele. Războiul bazat pe reţea este un concept de avangardă, care urmăreşte aplicarea tehnologiei informaţiilor în domeniul militar, asigurând şi cuprinderea noilor dimensiuni ale provocărilor militare şi de securitate. Abordarea acestora implică, în principal, informaţia, al cărei rol, ca un paradox, a rămas în continuare important şi cu aceeaşi putere de determinare.

Asistăm în prezent la o transformare majoră şi firească a civilizaţiei umane. Era industrială este la apus, asigurând premisele tehnologice de apariţie a unei noi ere: cea informaţională, în care capacitatea de culegere şi utilizare a informaţiei devine esenţială, având ca urmare imediată superioritatea în diferite confruntări. Se trece, astfel, de la o etapă de dezvoltare, ale cărei caracteristici au fost îndeosebi statice, reactive, la o etapă proactivă, avidă de comunicare şi informaţie. Faţă de era industrială, măsura succesului va fi dată acum de eficienţa cu care sunt obţinute şi utilizate informaţiile.

Din punctul de vedere al utilizării informaţiei se definesc astfel noi parametri şi dimensiuni. Astfel, era informaţională impune noi ameninţări şi actori, dar şi concepte şi tipuri de relaţionare care determină implicit fizionomia operaţiilor şi acţiunilor militare. În ceea ce priveşte misiunile şi capabilităţile, noile operaţii militare sunt diferite de cele din perioada Războiului Rece sau chiar de cele din anii ‘90. Forţele militare

nu mai sunt structuri statice, defensive, ci forţe moderne cu noi vocaţii: menţinerea păcii şi stabilizarea.

Lucrarea de faţă nu îşi propune analizarea în profunzime a caracteristicilor erei informaţionale. Cele prezentate anterior au urmărit sublinierea importanţei informaţiilor şi a influenţei acestora asupra operaţiilor militare.

Pentru o abordare a conceptului Network Centric Warfare din perspectiva informaţiilor sunt importante câteva caracteristici ale operaţiilor militare cu implicaţii asupra activităţii de informaţii.

Teatrul de operaţii militare nu mai este limitat geografic la zona de desfăşurare a acţiunilor de luptă. Acesta cuprinde şi zonele adiacente, dar şi domeniile de interes nonmilitare care pot afecta operaţiile, cum ar fi terorismul, crima organizată sau alte ameninţări transnaţionale. Informaţiile despre aceste zone sau domenii nu pot fi, de regulă, culese şi analizate folosind capacităţile de informaţii aflate la dispoziţia comandanţilor din teatrul de operaţii, ci sunt asigurate de la nivelul strategic, prin serviciile de informaţii militare.

În condiţiile suprapunerii actorilor şi ameninţărilor neconvenţionale peste cele clasice, militare, protecţia forţelor a devenit o misiune importantă a activităţii de informaţii militare. În aceste condiţii, contrainformaţiile constituie una din sursele de informaţii esenţiale pentru protecţia forţelor.

Ameninţările sunt caracterizate, în principal, de asimetrie şi impredictibilitate. Pentru combaterea acestora, forţele dislocate au nevoie, la nivelul oricărui eşalon, de informaţii de avertizare.

Desfăşurate, de regulă, într-un cadru de coaliţie, operaţiile şi acţiunile militare colocalizează în acelaşi teatru de operaţii un ansamblu de forţe eterogene pentru care cunoaşterea câmpului de luptă devine esenţială, atât pentru îndeplinirea misiunilor, cât şi pentru evitarea acţiunilor fratricide.

În condiţiile prezente de desfăşurare a operaţiilor militare, spectrul obiectivelor de lovit este lărgit, stabilirea ţintelor implicând o mai mare acurateţe şi o capacitate ridicată de decelare a importanţei acestora.

Unul din elementele-cheie ale operaţiilor militare este desfăşurarea operaţiilor informaţionale. Urmărind susţinerea pe termen lung a rezultatelor acţiunilor militare, prin impunerea în mentalul colectiv a unor mesaje şi atitudini, operaţiile informaţionale se bazează aproape în exclusivitate pe informaţii.

Se poate constata că, pentru îndeplinirea cu succes a operaţiilor militare, în prezent, dar şi în viitor, acestea trebuie conduse prin informaţii (“intelligence driven operations”). Suprapunând această concluzie peste impactul şi schimbările determinate de era informaţională, este evident că succesul operaţiilor militare va depinde, în mod covârşitor, de asigurarea superiorităţii de informaţii, respectiv a superiorităţii decizionale.

Superioritatea de informaţii se poate defini drept capacitatea de a culege, procesa şi disemina informaţii în mod continuu, concomitent cu exploatarea sau diminuarea (distrugerea) capacităţii de sprijin cu informaţii a forţelor oponente. Procesele de culegere, procesare şi diseminare trebuie să asigure relevanţa, oportunitatea şi acurateţea informaţiilor necesare forţelor dislocate, în funcţie de cerinţele specifice eşalonului din care acestea fac parte.

Conceptul “Network Centric Warfare” poate fi asimilat astfel unui „nou mod de gândire” aplicat operaţiilor militare. În esenţă, acesta constă în integrarea entităţilor participante la operaţii într-o reţea virtuală, prin care se transportă informaţii. Scopul final este acela de a pune la dispoziţia combatanţilor o imagine unitară a câmpului de luptă.

Elementele-cheie ale sprijinului eficient cu informaţii în cadrul NCW sunt conectarea capacităţilor de culegere de informaţii în reţea, fuzionarea informaţiilor, procesarea acestora

în formate care să poată fi accesate direct şi care să permită efectuarea unui schimb de informaţii continuu. Schimbul de informaţii este asigurat în ambele sensuri, de la structurile de informaţii către subunităţile luptătoare, dar şi invers, în sensul în care combatanţii pot „alimenta" sistemul cu informaţii reale, culese pe timpul desfăşurării misiunilor. Astfel, din această perspectivă, conceptul NCW poate fi aplicat operaţiilor şi acţiunilor de luptă conduse sau desfăşurate pe baza schimbului de informaţii, utilizând în acest scop suportul tehnic oferit de reţelele virtuale.

Astăzi, informaţiile militare au mult mai multe obiective (ţinte) şi beneficiari (consumatori) decât în trecut. Ca un paradox, reorientarea informaţiilor către nivelul operaţional-tactic este cerută de comandanţii din teatrele de operaţii care se confruntă cu oponenţi non-clasici. Ca o consecinţă, informaţiile de nivel operaţional-tactic au o importanţă strategică, iar informaţiile de nivel strategic devin din ce în ce mai relevante şi necesare pentru misiunile de nivel operaţional-tactic.

În măsura în care sistemele de armament şi combatanţii formează o reţea de forţe şi mijloace de luptă, generatorul de informaţie este constituit de către reţeaua de culegere şi analiză a informaţiilor. La baza schimbului de informaţii sunt arhitecturi şi concepte, relaţii şi sisteme tehnice care trebuie să asigure accesul la informaţii, în funcţie de necesităţi şi niveluri de acces, reprezentând, de fapt, imaginea comună asupra câmpului de luptă (Joint Operational Picture).

În principiu, imaginea comună asupra câmpului de luptă (Joint Operational Picture), generată în cadrul sistemelor de tip NCW, se compune din diferite substraturi (geografic, infrastructură, forţe proprii, forţe oponente, de informaţii etc.), care creează imaginea de ansamblu şi este structurată ţinând cont de specificul beneficiarilor (un domeniu pentru structurile de informaţii – pentru protecţia surselor mai ales – şi un domeniu al beneficiarilor informaţiilor).

Din perspectiva informaţiilor militare, aplicarea conceptului NCW la operaţiile militare, dincolo de suportul tehnic necesar constituirii reţelelor virtuale, care asigură cooperarea şi vizualizarea informaţiilor, are ca implicaţii:

- posibilitatea asigurării sprijinului de informaţii de nivel strategic pentru eşaloanele de nivel operativ-tactic (prin asigurarea legăturii structurilor de informaţii dislocate în teatrele de operaţii cu capacităţile de culegere şi analiză de nivel strategic naţionale);
- îmbunătăţirea schimbului de informaţii în cadrul coaliţiei;
- accesul structurilor de informaţii dislocate în teatrele de operaţii la bazele de date de nivel strategic;
- diseminarea în timp real a informaţiilor, determinând extinderea timpului avut la dispoziţie pentru luarea deciziilor;
- posibilitatea redefinirii în timp real a misiunilor capacităţilor de culegere;
- utilizarea eficientă a sistemelor şi arhitecturilor ISTAR (Intelligence Surveillance Target Aquisition and Reconnaissance), inclusiv posibilitatea conectării sistemelor ISTAR naţionale la cele ale coaliţiei;
- posibilitatea de verificare/confirmare a informaţiilor culese din diferite surse specifice activităţii de informaţii militare, de către subunităţile din teren şi transmiterea feed-back-ului acestora către structurile de informaţii;
- culegerea şi analiza multisursă (fuzionarea informaţiilor);
- asigurarea unui substrat de informaţii la imaginea comună asupra câmpului de luptă, care să conţină informaţii relevante pentru subunităţile luptătoare privind localizarea, capacitatea şi intenţiile forţelor oponente;
- asigurarea unui management îmbunătăţit al cererilor de informaţii;

- posibilitatea de automatizare într-un anumit grad a ciclului informațional (culegere, procesare, diseminare);

- sprijinul eficient în desemnarea obiectivelor de lovit, analiza rezultatelor acțiunilor de luptă şi executarea operațiilor informaționale, având în vedere asigurarea legăturii între rețeaua de culegere şi analiză şi cea a forțelor şi mijloacelor de luptă;

- conducerea unitară a activității de informații militare şi eliminarea redundanțelor;

- posibilitatea căutării şi extragerii rapide a informațiilor din bazele de date.

În concluzie, în cazul aplicării conceptului NCW, rolul informațiilor militare este caracterizat de următoarele elemente:

- subrețeaua capacităților de culegere şi analiză constituie generatorul de informații;

- sistemele ISTAR sunt un element-cheie în asigurarea superiorității de informații;

- suportul tehnic/comunicațiile sunt esențiale pentru vizualizarea/ exploatarea informațiilor;

- arhitectura NCW trebuie să includă sprijinul de informații de nivel strategic.

OPERAȚII BAZATE PE REȚEA. STUDIU DE CAZ - BRIGADA STRYKER

General maior Mircea SAVU

Această prezentare se referă la operații bazate pe rețea şi la organizarea noii brigăzi mecanizate digitizate din armata Statelor Unite, denumită STRYKER BRIGADE COMBAT TEAM. În compunerea acestui proiect se regăsesc rețelele de comunicații digitizate şi sistemul de comandă şi control, o nouă forță proiectată pe un vehicul de luptă mediu, de viteză mare şi invizibil pentru mijloacele de detecție obişnuite. În plus față de noutatea concepției operaționale şi structurale, brigada utilizează conceptul de operații de informații bazate pe rețea. Două asemenea mari unități sunt deja operaționalizate şi alte patru sunt în curs de operaționalizare.

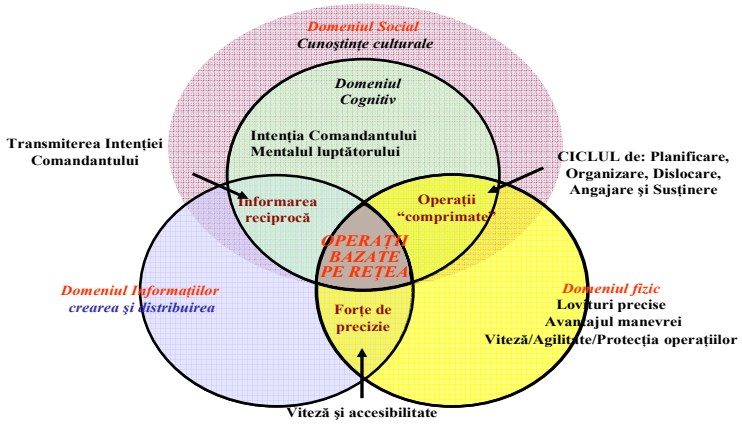
Studiul compară brigada STRYKER cu o brigadă de infanterie uşoară la un exercițiu în cadrul unui **Centru de evaluare a capacității de luptă,** concentrându-se asupra utilizării informațiilor pentru a câştiga avantaj în fata inamicului. Studiul a fost desfăşurat de către Rand National Security Research Institute.

Viitoarele forțe întrunite trebuie să fie: *complet integrate* - toate capabilitățile componentelor ministerului apărării trebuie să aibă caracteristicile unei forțe întrunite, integrate, capabile să îşi coordoneze şi concentreze efortul pentru atingerea unui obiectiv strategic; *legate în rețea* - conectate şi sincronizate în timp şi efort, cu capacitatea de a permite forțelor dispersate să comunice, să manevreze şi să utilizeze o imagine operațională comună a câmpului de luptă; *adaptabile* - forțe cu un grad sporit de flexibilitate structurală şi funcțională, adaptabile modulare, pregătite să răspundă rapid oricărei variante de acțiune; *expediționare* - capacitate de

dislocare rapidă, angajare şi susţinere-indiferent de acţiunile anti-acces sau condiţii de mediu; *să aibă superioritatea deciziei* - câştigarea şi obţinerea superiorităţii informaţiilor, în vederea controlului situaţiei şi păstrarea capacităţii de a reacţiona la schimbări; *descentralizate* - utilizează planuri de colaborare şi informaţii distribuite pentru a permite subordonaţilor să comprime ciclurile deciziei; *letale* - capabile să distrugă un adversar sau/şi sistemele acestuia în orice condiţii şi în orice mediu.

Secolul XXI a marcat saltul de la era industrială la era informaţiei. Câteva elemente legate de domeniile de conflict în era informaţiei sunt relevate în mod succint.

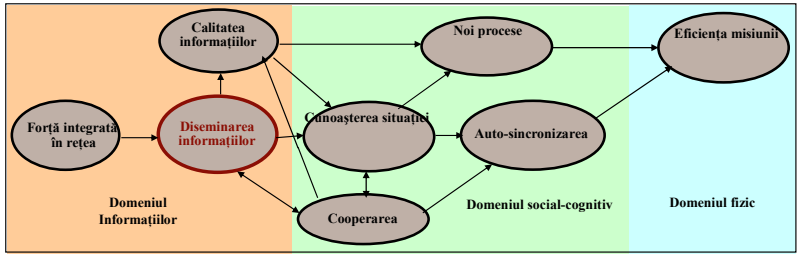
Competiţia în era informaţiei
...resursa de putere a operaţiilor bazate pe reţea...



Intersectarea acestor domenii generează dinamica vitală pentru ariile de conflict, sintetizată în diagrama în **operaţii bazate pe reţea**.

Operaţii pe bază de reţea
...Noul lanţ de valori

- **O forţă robustă integrată în reţea optimizează schimbul de informaţii**
- **Schimbul de informaţii de calitate, în timp oportun, îmbunătăţeşte cooperarea şi menţine cunoaşterea situaţiei la parametrii optimi**
- **Cunoaşterea situaţiei de către toţi participanţii la operaţii, permite cooperarea, auto-sincronizarea, creşterea vitezei de reacţie a comenzii, susţinerea operaţiei şi supravieţuirea**
- **Toate acestea, cumulate, măresc eficienţa în îndeplinirea misiunii**



În domeniul fizic, forţele se deplasează în spaţiu şi timp, în toate mediile - spaţiul cosmic, aerian, maritim şi terestru. În aceste spaţii, forţele desfăşoară operaţii şi se regăsesc platformele care realizează reţelele de comunicaţii, sistemele C2. În domeniul cognitiv se iau deciziile, se desfăşoară acţiuni pentru cunoaşterea şi înţelegerea situaţiei, se desfăşoară activităţile legate de leadership. În domeniul social interacţionează indivizii şi organizaţiile.

Avantajul informaţional ne permite să constituim şi să utilizăm o forţă de precizie, cu mare viteză, agilitate şi acces în toate mediile.

Esenţă

„FORŢELE ORGANIZATE ÎN REŢEA ÎNVING FORŢELE CLASICE”

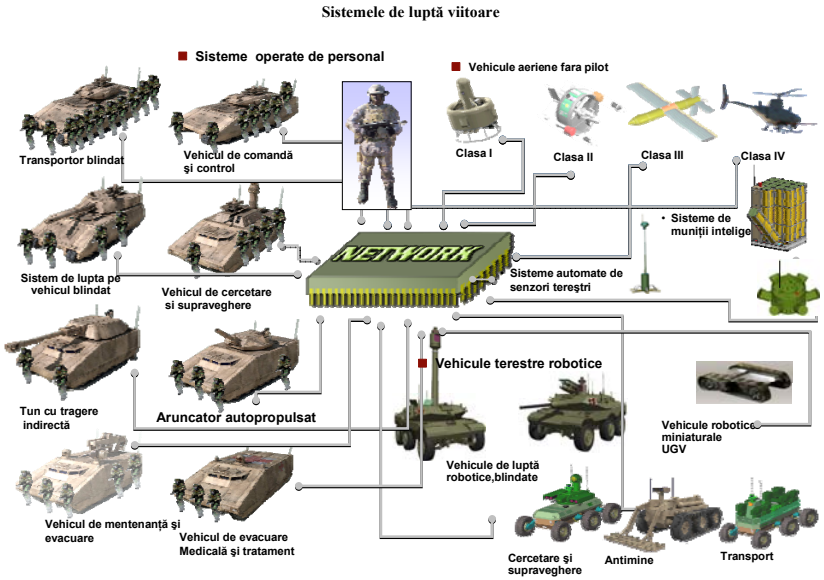
„... noul sistem bazat pe reţea ne permite să luăm decizii şi să acţionăm mai rapid decât oricare dintre oponenţi”.

Gen.-Lt. David D. McKiernan (Combined Forces Land Component Commander, OIF)

Raportul preliminar al studiului de caz, referitor la Brigada Stryker, sponsorizat de Departamentul pentru Transformare al SUA, subliniază importanța „rețelei”, constituită din sisteme şi subsisteme, în centrul căruia elementul principal este luptătorul.

Cele 18 sisteme integrate în rețea denumite „Sisteme de luptă viitoare (Future Combat Systems Program) sunt următoarele:

- 8 Vehicule de luptă terestre operate de personal
- 4 clase diferite de UAV de la subunități mici, la brigada
- 3 categorii de bază de vehicule robotice fără personal la bord; vehicul robotic de luptă, vehicul robotic de transport, vehicul antimine



Fiecare din aceste sisteme este dotat cu un software integrat capabil să conecteze permanent sistemul, la un centru

de control şi să primească/transmită informații (common integrating software).

Capabilitățile de acțiune/luptă „în rețea” ale Brigăzii Stryker sunt evidențiate de noua structură organizatorică şi noile mijloace de luptă, noua rețea de informații şi noile concepte operaționale care amplifică superioritatea informațională. Formațiunea de cavalerie şi accesul la senzorii tehnici permit brigăzii Stryker să „vadă” prima. Sistemele de vizualizare automată în rețea îi permit să înțeleagă concomitent situația forțelor proprii şi pe cea a inamicului, înaintea acestuia. Noile concepte operaționale subliniază agilitatea şi ritmul de acțiune al brigăzii de a acționa prima, prin exploatarea sinergiei dintre mobilitatea forțelor şi agilitatea comenzii.

Brigada Stryker – prezentare generală

Componentele structurale ale brigăzii îi permit să îşi constituie capabilitățile necesare îndeplinirii misiunilor.

Structură:

- Mai mulți “ochi” în teren
  - 3 plutoane de cercetare
  - UAV
  - HUMINT Team in fiecare vehicul de cercetare
- Lunetişti în toate companiile de infanterie
- Companie de Transmisiuni, Antitanc şi Geniu
- Companie de Informații Militare
- Divizion de Artilerie

Batalion Logistic

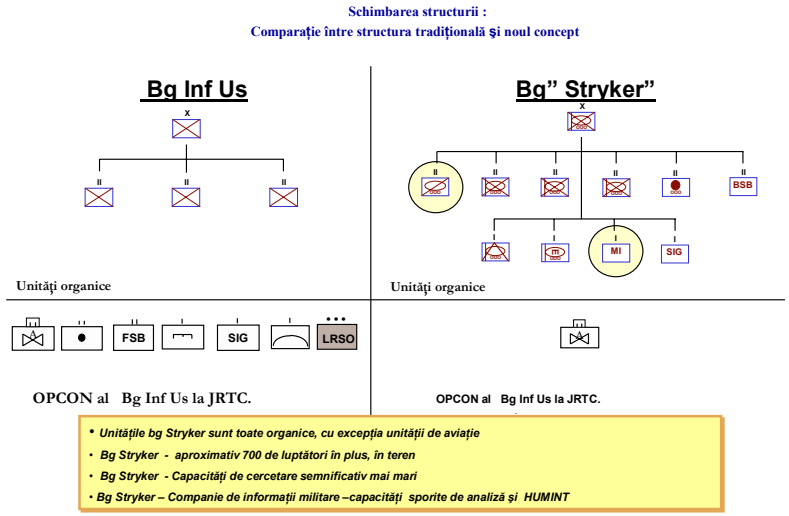
Capacități de C2, automate şi în rețea

- Diseminarea şi vizualizarea rapidă a informațiilor
- Planuri de operații/acțiune, multieşalon
  - Interacțiuni Brigadă-Batalion-Companie

Concepte operaționale

- Operații distribuite integrate
- Înțelegerea completa a situațiilor înainte de contact

- „Vezi primul, înțelegi primul, acționezi primul, finalizezi decisiv”
- Manevra precisă
  - Concentrare şi dispersare rapidă
- Selectarea timpului şi locului luptei
- Evitarea surprinderii/exploatarea avantajelor



În total, brigada Stryker are 793 de militari în plus față de brigada de infanterie uşoară, cu 360 de trăgători cu diferite calibre mai mult, şi de patru ori mai multe capabilități de cercetare.

Cel mai important element, care constituie şi noutatea structurală a brigăzii Stryker, o reprezintă formațiunea de Cavalerie (Recce SysTact Assault), care amplifică potențialul de cercetare al brigăzii. Deficiența cea mai critică a unei brigăzi de infanterie uşoară constă tocmai în lipsa acestei capacități sporite de cercetare (3 plutoane de cercetare. şi o Companie de

cercetare, pentru a sprijini sarcinile de luptă a trei batalioane de manevră şi nevoia de informații a întregii Brigăzi de Infanterie Uşoară, pentru acțiune, analiză şi decizie). Este important să menționăm faptul că principala sursă de informații, cercetare şi supraveghere (Intell Surv Recce), în brigada Stryker, este dată de „ochii umani”. Experiența, atât în centrele de instruire pentru luptă, cât şi în Operația Iraqi Freedom, a relevat limitările senzorilor tehnici de a furniza informații complete, exacte şi în timp oportun, pentru a putea sprijini acțiunile de luptă tactice şi lupta apropiată, directă. Refrenul familiar in OIF este: „noi, încă descoperim inamicul, lovindu-ne de el”.

Diferența dintre Brigada Stryker si forțele tradiționale o constituie existența batalionului de cavalerie, care angajează primul inamicul, conservând capacitatea brigăzii de a-şi păstra libertatea de manevră şi de a alege cursul de acțiune avantajos, în afara contactului, în timp ce Brigada de Infanterie Uşoară ia contact cu inamicul, cu forțele principale, devenind automat şi imediat angajată decisiv.

În sfârşit, Compania de Informații Militare furnizează o semnificativă capacitate de analiză, regăsită în trecut numai la nivelul diviziilor, prin militarii antrenați în operații/acțiuni HUMINT, amplasați în fiecare vehicul de cercetare prin luptă. Această capabilitate HUMINT este absolut critică pentru sprijinul operațiilor de stabilitate, în domeniul cooperării cu autoritățile civile locale.

În total, brigada Stryker are 793 de militari în plus față de brigada de infanterie uşoară, cu 360 de trăgători cu diferite calibre mai mult, şi de patru ori mai multe capabilități de cercetare.

În cadrul brigăzii uşoare de infanterie există o interacțiune limitată, prin intermediul sistemului de comunicații FM, în timp ce sistemul automat interactiv al brigăzii Stryker permite o amplă şi eficientă interacțiune între toate entitățile brigăzii. Fiecare lider din brigada Stryker este permanent în

rețea, fapt ce permite extinderea exponențială a abilității de a schimba informații, de a-i contacta pe ceilalți lideri, de a înțelege situația şi de a colabora pentru rezolvarea tuturor problemelor.

Un alt punct critic îl constituie locul comandantului brigăzii de Infanterie, brigăzii de infanterie uşoară. Comandantul este ori în față, cu subordonații din forțele de angajare inițială, înainte de începerea luptei, pentru a se convinge că aceştia îi înțeleg intenția şi sunt pregătiți pentru luptă sau se află în centrul tactic de operații, coordonând procesul de luare a deciziei. Aceasta este o opțiune „ori/ori".

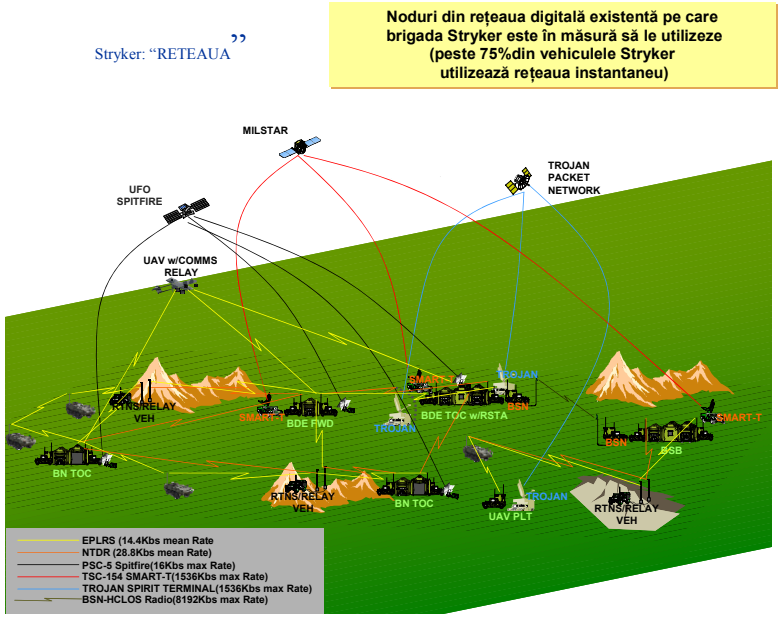
În brigada Stryker, comandantul poate utiliza posibilitățile oferite de comunicațiile în rețea pentru a îndeplini concomitent ambele sarcini majore. El se poate afla împreună cu subordonații şi, în acelaşi timp, poate coordona activitățile statului major, prin sistemul VTC instalat în punctul de comandă mobil. Acest fapt permite creşterea semnificativă a interacțiunilor dintre comandant şi statul major, în timpul procesului de planificare, conferind procesului de luare a deciziei un specific caracterizat prin concentrarea în jurul comandantului si bine ancorat in realitate.

Context

- Mediul Operațional
  - Operații tactice de război
  - Operații de dislocare/intrare rapidă în teatru
- Analiză concentrată pe Certificarea Exercițiului (CERTEX) pentru US Stryker Brigade Combat Team (SBCT)
  - Loc -Joint Readiness Training Center
  - Scenariul: Stryker Bg Cmt Team= Atac asupra obiectivului Shughart-Gordon
- Comparația cu:

  - Brigada de infanterie uşoară nedigitizată
- Rezultate măsurabile şi diferențe:
  - Dimensiuni cuantificabile ale eficienței misiunii:
    - Eficiența forței, supraviețuirea
  - Măsurarea eficienței C2: calitatea cunoaşterii situației, viteza de reacție a comenzii, calitatea deciziilor, sincronizarea forțelor

Brigada Stryker este echipată cu ultima generație de sisteme de comunicații digitale şi cu sistemul de comandă şi control care se află, în acest moment, în dezvoltare.



Cele două capabilități-cheie ale brigăzii Stryker constau în: (1) abilitatea sa de a comunica permanent cu eşaloanele superioare şi alte entități din afara brigăzii şi (2) de a asigura că propriile elemente structurale sunt conectate permanent şi au posibilitatea să schimbe informații continuu.

Deşi nu este perfect, sistemul furnizează o cantitate semnificativ mai mare de informaţii şi cu o calitate superioară celor obţinute de sistemele care dotează unităţile nedigitizate.

Unele unităţi blindate, medii şi grele au sisteme de comunicaţii şi informaţii digitizate. Diferenţa şi superioritatea acţională şi informaţională a brigăzii Stryker este dată de structura organizatorică.

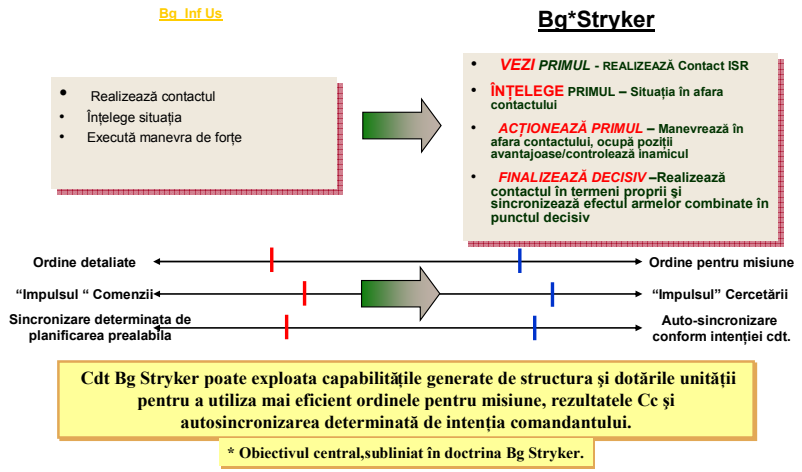
Aceste capabilităţi sunt puse în valoare de sistemul de legături în reţea, care, la rândul său, este structurat în două subsisteme şi cinci subreţele: WAN wide area network, TOC-to-TOC network (TOC = tactical operations center), tactic internet (TI), reţea radio de comandă, Command Net Radio network (CNR) şi sistemul de comunicaţii global - Global Broadcast System (GBS).

În plus faţă de aceste subreţele, numeroase componente ale sistemului de comunicaţii ale brigăzii digitizate STRYKER posedă o varietate de componente specializate, pentru a intra în legătură cu sistemele de informaţii naţionale şi cu sistemele de transmitere a imaginilor din avioanele fără pilot – UAV Imagery System.

Fiecare subreţea joacă un rol important în conectarea elementelor componente ale brigăzii, între ele şi cu entităţi din afara brigăzii.

Concepte operaţionale

Noile concepte operaţionale vor schimba modul de ducere a luptei în conflictele viitoare.



Un concept important este: "See first, understand first, act first, and finish decisively" - să vezi primul, să înţelegi primul, să acţionezi primul şi să învingi într-o manieră categorică.

Acest mod de abordare modifică maniera de executare a unui atac, conform vechiului principiu: „să iei contact cu adversarul, să stabilizezi situaţia şi să angajezi rezervele sau forţele de angajare ulterioară" la o nouă modalitate, concretizată în „realizează contact prin informaţii, supraveghere şi cercetare, stabilizează situaţia în afara contactului, execută manevra de forţe spre o poziţie avantajoasă şi acceptă angajarea decisivă în termeni favorabili forţelor proprii".

Ordinele pentru misiune furnizează o descriere clară a intenţiei comandantului şi a obiectivelor şi mai puţine detalii despre mijloacele/modul de realizare a obiectivelor.

„Impulsul cercetării" se realizează prin capacitatea comandantului de a temporiza alegerea unei direcţii de

înaintare spre contact, până la momentul în care forţele de Cercetare şi informaţii cunosc şi furnizează informaţii detaliate.

Auto-sincronizarea permite comandanţilor subordonaţi să facă ajustările necesare, fără intervenţia eşalonului superior.

Capacităţile brigăzii Stryker permit acestei unităţi să utilizeze mai eficient aceste tactici, tehnici şi proceduri care, în final, optimizează agilitatea forţelor combatante.

Concluzii

Brigada de Infanterie Uşoară:

- Forţele proprii pierd bătălia pentru avantajul informaţional
  - Cercetaşii sunt angajaţi şi nimiciţi de forţele inamice
- Cunoaşterea poziţiei forţelor proprii este limitată:
  - 10% -procent de realizare a informaţiilor despre inamic
  - 20% -procent care reflectă cunoaşterea situaţiei
- Impact operaţional:
  - Forţele proprii atacă poziţii puternice ale forţelor adversarului
  - Suferă pierderi puternice
  - La atingerea obiectivului nu au capacitatea de a îndeplini misiunea
  - Pierd bătălia - raportul forţe proprii/inamic, la pierderi, este 10:1.

Brigada Stryker

- Câştigă lupta pentru avantajul informaţiilor
  - Manevrele amplifică efectele acţiunilor cercetaşilor proprii

  - Forţele de cercetare proprii învinge cercetaşii inamici
- Reuşesc să obţină informaţii semnificative despre poziţionarea forţelor:
  - 80% despre inamic
  - 90% despre forţele proprii
- Impact operaţional:
  - Execută cu succes înşelarea adversarului
  - Surprinderea adversarului
  - Comandantul poziţionează avantajos forţele proprii şi câştigă timp
  - Ajunge la obiectiv cu forţele eficiente
  - Îşi îndeplineşte misiunea – securizează obiectivul, cucereşte clădirile, nimiceşte contraatacul
  - Forţele adversarului sunt învinse în mod decisiv - raportul pierderilor - 1: 1.

Îndeplinirea misiunii şi supravieţuirea

  - Cea mai impresionantă capabilitate demonstrată de noua structură a brigăzii Stryker a fost abilitatea de a afecta în mod decisiv ciclul de decizie a inamicului prin:
    - superioritatea informaţională;
    - viteza de reacţie;
    - mobilitate;
    - capacitate de distrugere;
    - menţinerea îndelungată a capacităţii de luptă ridicate.

Brigada Stryker este în mod semnificativ mai agilă şi mai capabilă decât structurile care au precedat-o - brigăzile de infanterie uşoară/mecanizate nedigitizate.

Numeroşi factori ai capabilităţilor generate de structurile organizate în reţea contribuie la creşterea magnitudinii eficienţei:

- Sistem de comandă organizat în reţea
- Conexiuni în bandă largă în afara vizibilităţii directe (B-LOS) SATCOM
- Creşteri spectaculoase ale capacităţii de a colecta/schimba informaţii între indivizi
- Interacţiuni şi Colaborări/Cooperări de amploare.

Rezultate semnificative rezultate în urma examenului de certificare la centrul de instruire pentru luptă:

- Îndeplinirea misiunii, învingerea adversarului, eliberarea fiecărei clădiri
- Rata pierderilor trupe proprii/inamic a scăzut de la 10:1 la 1:1
- Viteza de reacţie a comenzii în ciclul decizional a crescut semnificativ - de la 24 la 3 ore, combinată şi cu agilitatea tactică

RĂZBOIUL BAZAT PE REŢEA, CONCEPTUL CARE ÎNGLOBEAZĂ TRĂSĂTURILE CONFLICTULUI ÎN ERA INFORMAŢIEI

Colonel Ionel HORNEA

Fiecare trebuie să aibă în minte că nimic nu este mai dificil de executat, nimic mai periculos de administrat decât introducerea unui nou sistem de gândire. Cel care-l introduce are pe toţi cei care profitau de cel vechi un duşman şi ca prieteni apropiaţi pe cei care vor să profite de cel nou.

Machiavelli

Războiul secolului XXI nu va mai avea nimic în comun cu războaiele mondiale pe care istoria le-a traversat. Odată cu terminarea Războiului Rece nu mai sunt necesare forţele masive ce trebuiau să fie menţinute, locul lor urmând să fie luat de structuri suple, agile, dislocabile, capabile să intervină în timp scurt în orice zonă de pe glob.

Această situaţie este un element în plus, care susţine ideea că, în prezent, conceptul de bazare pe reţea a securităţii cunoaşte un amplu caracter de cuprindere, datorită paşilor concreţi făcuţi în sensul realizării acesteia, în cadrul unor sisteme zonale, regionale sau, în viitor, globale.

Caracteristica este puternic impulsionată, de asemenea, de faptul că **informaţia devine o forţă în toate domeniile**, ca urmare a dezvoltării tehnologice pe care o impune era informaţiei.

În acest sens, John Garstka[6] spunea: „Faceţi din forţa transformării un element pivotant al strategiei naţionale de

[6] Asst. Director for Concepts and Operations, Office of Force Transformation, Office of the Secretary of Defense.

securitate sau al strategiei Ministerului Apărării, care să sprijine efectiv cei patru piloni ai strategiei militare naționale”[7].

Generalul de brigadă Thomas J. Verbeck, directorul C3 şi pentru Integrarea acțiunilor de luptă[8] al USEUCOM, sublinia necesitatea concentrării tuturor acțiunilor mai degrabă pe *„prevenirea războiului”,* decât pe *„ducerea războiului”,* ocazie cu care a arătat că „SUA văd Europa ca pe un partener global pentru realizarea păcii şi securității, o Africă autosuficientă şi stabilă şi un întreg Orient Mijlociu în pace, pe baza unui USEUCOM transformat, expediționar”.

Elementul central al viitorului tip de război ce va corespunde cerințelor acestei epoci este conceptul **„de război bazat pe rețea”,** care constituie baza „ca teorie a războiului erei informației, cât şi principiul pentru planificarea militară şi elaborarea conceptelor operaționale întrunite de capabilități şi sisteme”[9]**.** Aceasta va schimba, de jos în sus, structura forțelor militare şi cultura acestora, prin folosirea experimentelor, mijloacelor de transformare şi prin crearea şi distribuirea de noi cunoştințe şi experiențe. Toate elementele se vor concentra pentru **transformarea informației în putere** şi vor asigura, pentru prima dată, preluarea în sistem militar a conceptului **e-business,** specific mediului de afaceri civil.

Introducerea conceptului de Operație Bazată pe Rețea, ca orice element de noutate, formulează răspunsuri la o serie de întrebări fundamentale, precum cea referitoare la posibilitatea ca **operația bazată pe rețea să poată crea o forță mai mobilă şi mai rapidă** şi, totodată, vine cu noi întrebări referitoare la:

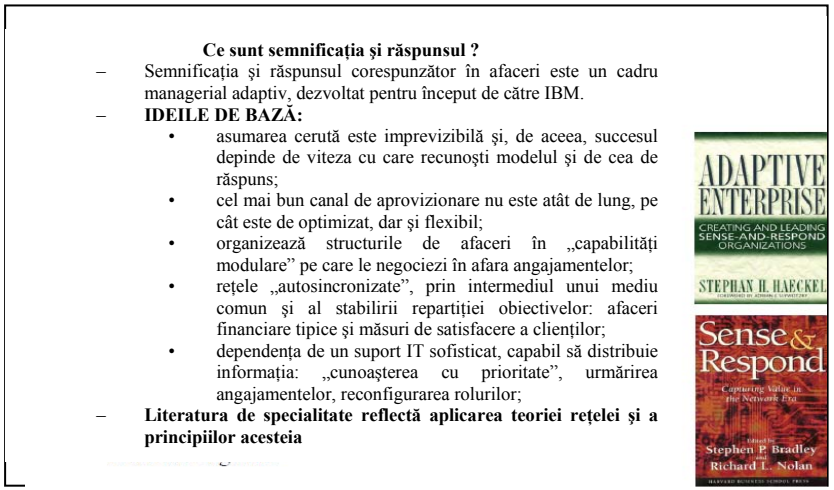
- *care este cea mai bună metodă de comandă şi control a unei forțe bazate pe rețea?*
- *cum creăm o forță bazată pe rețea?*

[7] Expunerea prezentată în Conferința de la Bruxelles, din noiembrie 2003, cu tema „Transformarea - o provocare”.
[8] Director Command, Control and Warfighting Integration.
[9] John J. Garstka.

- *cum putem măsura progresele făcute în direcția realizării unei forțe bazate pe rețea?,*

la care s-au dat răspunsuri de genul:

- este necesară o nouă teorie şi un volum de noi cunoştințe (ar trebui făcute noi experiențe şi sunt necesare noi cercetări);
- este necesar un mecanism pentru dezvoltarea şi aplicarea teoriei de către ministerele apărării şi, în primul rând, un *nou cadru conceptual* şi noi mijloace şi metodologii de evaluare.



În cadrul acestor identificări conceptuale se va urmări punerea în evidență a elementelor-cheie în dezvoltarea unei forțe specifice erei informaționale, precum:

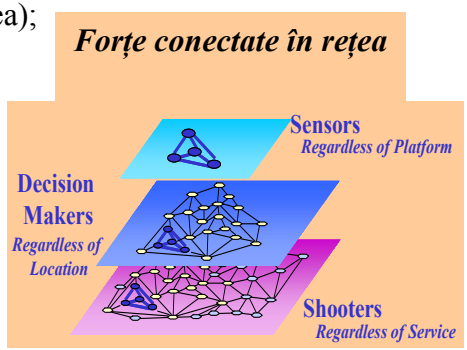
– accelerarea legării în rețea a forței întrunite;
– creşterea mobilității sistemelor bazate pe rețea, a conceptelor şi capabilităților;
– adresarea provocărilor conceptului operației bazate pe rețea, precum şi pe cele ale operațiilor de coaliție sau de alianță;

– experimentarea capabilităților şi conceptelor bazate pe rețea, precum şi a provocărilor-cheie (aplicarea Teoriei Inițiativei Largi[10]);

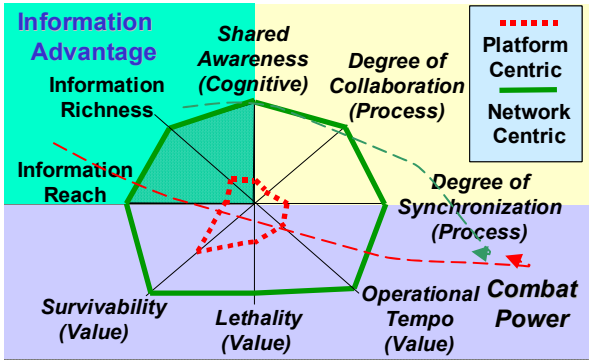
– dezvoltarea *„forței erei informaționale”,* în care rolul principal îl vor avea *:*

– senzorii;
– rețeaua;
– executanții (sistemele de arme);
– comanda şi controlul;
– forța umană;

– realizarea structurilor de forțe alternative (platforme legate în rețea);



– asigurarea eficacității misiunii;



[10] **Applying the Theory Enterprise Wide.**

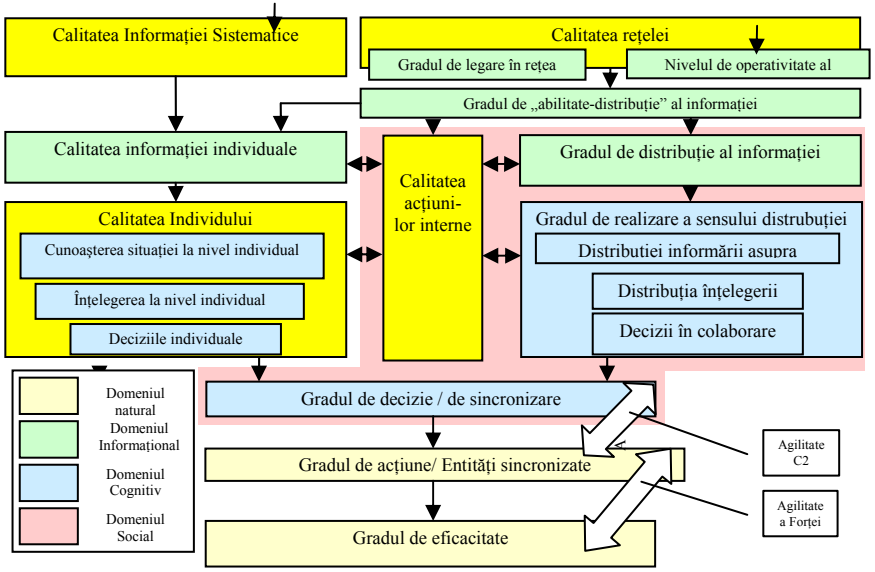
– realizarea comenzii şi controlului *forței în rețea* (**oferind teoriei exactitate**[11]), prin:

– *„Imaginea Operațională Unică“*
– reduce „ceața războiului”;
– *partajarea cunoaşterii situației* (SA[12]);
– *creşterea importantă a cunoaşterii situației* (SA) de către:
– comandant
– comandanții subordonați
– luptătorii individuali;
– scăderea încărcăturii cognitive în dezvoltarea *cunoaşterii situației;*
– cunoaşterea intențiilor comandantului;
– creşterea *gradului de înțelegere* a situației distribuite;
– creşterea posibilităților prin capabilități şi colaborare în timp real;
– creşterea vitezei de elaborare a deciziei;
– agilitate tactică sporită (deplasare rapidă şi uşoară);
– reducerea riscului.

Un alt-aspect cheie va fi Cadrul Conceptual al Operației Centrate pe Rețea[13], care cuprinde:

[11] **Idem.**
[12] Shared Situational Awareness.
[13] The NCO Conceptual Framework.

Acesta se desfăşoară potrivit modelului de mai jos, asigurând interconectarea din punct de vedere al calității şi eficienței celor cinci mari componente, cu evidențierea domeniilor pe care sunt definite:



Cadrul conceptual abordează două teme de importanță hotărâtoare pentru implementarea conceptului. **Prima - înțelegerea clară a conceptului C4IS**. Sarcina de bază este cea a „comenzii şi controlului" în rețea, adică a componentei C2, structurilor specializate din Armata României revenindu-le rolul de a asigura cealaltă componentă, C2IS (computere, comunicații, informații şi sisteme), care reprezintă suportul tehnic al comenzii şi controlului. **A doua -** modul în care se poate realiza standardizarea în implementarea **conceptului de operație bazată pe rețea** de către toate armatele statelor membre. Aici problema a rămas în discuție, deoarece, la acest moment, standardele Alianței nu au fost adaptate pe deplin cerințelor transformării, urmând ca Agenția pentru Standar-

dizare, în cooperare cu ACT, să soluționeze problema în perioada următoare.

În urma participării la campania din Irak, sub comanda SUA, experții Marii Britanii în aplicabilitatea conceptului de *operație bazată pe rețea* au ajuns la următoarele concluzii:

- organizarea (fig. 3) a permis:
  - înaltă flexibilitate – organizare conform cerințelor misiunii misiune (Highly flexible – task organised);
  - desfăşurarea de operații integrate, aeriene şi terestre (Integrated Air / Ground operations – MAGTAF – fig. 4);
  - mobilitate strategică (Strategic mobility), prin:
    - dispunerea în adâncime / prepoziționare la debarcare;
    - realizarea efectelor prin intermediul puterii aeriene;
    - operații de-a lungul litoralului (750km);
    - folosirea masivă a rezervei.

Forța combativă

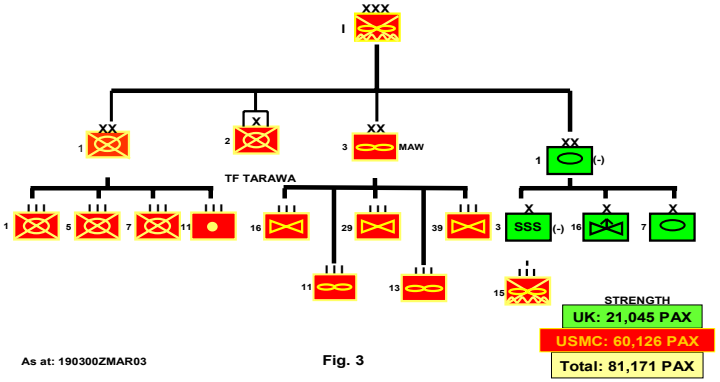


Fig. 3

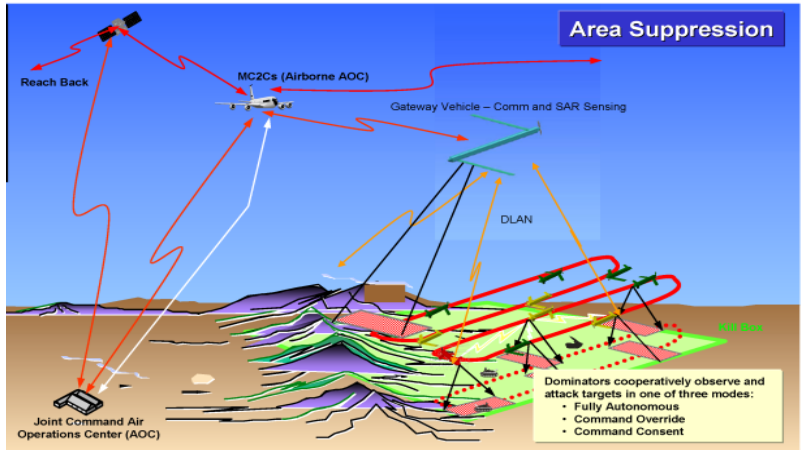


Fig. 4

Conceptul de operaţii bazate pe reţea a fost implementat în **OPERAŢIILE BAZATE PE EFECTE.** Ce sunt operaţiile bazate pe efecte? Sunt, pur şi simplu, o altă denumire pentru o variantă mai sofisticată a determinării efectelor probabile ale mijloacelor de lovire sau poate un alt mod de exprimare referitor la legătura dintre uzură şi „voinţă", cu care analiştii în probleme de operaţii şi-au bătut capul timp de mai multe decenii? Sau sunt ceva mai mult, *o abordare mai largă şi mai integrată a operaţiilor militare în ansamblu,* care, atunci când sunt combinate cu tehnologii noi şi cu gândirea bazată pe reţea, ne oferă posibilitatea de a trata diferit provocările la adresa securităţii, cu care suntem confruntaţi în prezent şi ne-ar putea ajuta, totodată, să exploatăm puterea forţei noastre militare, **excluzând lupta**.

Sub o formă sau alta, operaţiile bazate pe efecte **au existat dintotdeauna.** Ele sunt ceea ce generalii, amiralii şi oamenii de stat au încercat să facă: *să se concentreze asupra formării gândirii şi comportamentului adversarului mai mult decât pe simpla înfrângere a forţelor lui*. Acestea sunt, în spiritul scrierilor lui Sun Tzu şi ale lui Clausewitz privind operaţiile militare, nu o simplă modalitate de acţiune la nivel

tactic şi nici specific militare, ci întreaga gamă de acţiuni politice, economice şi militare pe care o naţiune ar putea să le întreprindă, pentru a determina comportamentul inamicului sau al oricărui oponent sau chiar pe cel al aliaţilor sau neutrilor.

Conceptul operaţiilor bazate pe efecte reprezintă un cadru larg care include idei de genul celor ale „determinării efectelor probabile ale mijloacelor de lovire"[14] şi ale „operaţiilor bazate pe uzură", care, însă, oferă domeniul şi flexibilitatea de a face mai mult: de a *înţelege operaţiile militare în timp de pace, criză sau război, în contextul unui efort politic, economic şi militar naţional general, coerent.*

Acest postulat conduce la un set de întrebări importante: *Cum putem defini conceptul de lucru al operaţiilor bazate pe reţea? Cum ar putea un asemenea concept să schimbe modul în care utilizăm forţele noastre armate sau forţa noastră militară? Cum am putea să operaţionalizăm acest concept în cadrul luptei şi în acţiunile militare de zi cu zi? Şi, în sfârşit, cum poate el modela capacitatea noastră de înţelegere a Războiului Bazat pe Reţea?*

Analiza eficacităţii în luptă, a uzurii mijloacelor şi voinţei adversarului, precum şi a simetriei în conflicte arată că **operaţiile bazate pe efecte** cresc eficacitatea luptei prin (1) concentrarea efortului asupra **voinţei adversarului**, astfel încât lupta să se scurteze şi (2) **utilizarea** operaţiilor bazate pe reţea nu numai la luptă, dar şi **în întreg spectrul conflictului**.

Analiza **războiului de uzură** conduce la concluzia că, oricât de eficient ar putea fi (de exemplu, prin determinarea efectelor probabile ale mijloacelor de lovire), rămâne, în cel mai bun caz, un atac indirect asupra adevăratului determinant al rezultatului conflictului: *voinţa inamicului de a continua să lupte.*

[14] Cap. III**, What Are Effects-Based Operations?** din Effects Based Operations, editată de CCRP în noiembrie 2002.

Problema voinței este fundamentală, atât pentru modelul simetric, cât şi pentru cel asimetric de conflict, dar în moduri foarte diferite. În cel simetric, conflictele bazate pe uzură, distrugerea capacității de a duce războiul lipseşte treptat adversarul de mijloacele fizice de continuare a luptei, pe care este hotărât să o continue. În conflictele asimetrice, distrugerea urmăreşte crearea unui efect psihologic sau cognitiv.

Astfel, **în competiția asimetrică**, bazată esențialmente pe efecte, **obiectivul este înfrângerea voinței adversarului sau remodelarea comportamentului**, în aşa fel încât el să nu mai dorească să continue lupta sau să-l dezorienteze, să nu mai reacționeze coerent. Dacă distrugerea fizică rămâne un factor în operațiile bazate pe efecte, aceasta este creația ori a unui efect psihologic, ori a unuia cognitiv, care reprezintă adevărata esență a abordării bazate pe efecte. Ea reprezintă, de asemenea, contextul real de evaluare a eficienței luptei în operațiile bazate pe rețea şi în cele bazate pe efecte.

De exemplu, **precizia, viteza şi agilitatea sporite** promise de legarea în rețea a senzorilor, forțelor şi comandanților prevesteşte, cu siguranță, **o capacitate de a executa acțiuni foarte rapide şi precise pe câmpul de luptă.** Disponibilitatea potențială a unei mai bune cunoaşteri şi înțelegeri a inamicului cu ajutorul rețelei arată o nouă abilitate a comandanților de a-şi configura acțiunile din câmpul de luptă, astfel încât să se realizeze un „efect" specific, caracterizat în termeni referitori la comportarea inamicului.

Discuțiile despre acțiunile de luptă bazate pe uzură indică un fapt evident: deşi eforturile noastre de a îmbunătăți eficiența în luptă a forțelor şi de a aplica conceptul *de război bazat pe rețea* sunt concentrate asupra luptei, marea majoritate a operațiilor militare nu implică nici lupta, nici distrugerea. Ca să fim şi mai concreți, „o forță militară care nu poate purta războaiele țării sale nu valorează prea mult, dar este la fel de adevărat şi că una capabilă numai să lupte nu va fi de prea mare

ajutor în prevenirea războaielor, limitarea conflictelor sau constituirea unei descurajări stabile, care sunt misiuni-cheie față de provocările determinate de mediul de securitate după 11 septembrie 2001"[15]. Ducând această logică mai departe, trebuie să recunoaştem că atitudinea pe care vrem să o modelăm nu este doar cea a inamicilor noştri**. În esență,** îmbinarea *capabilităților bazate pe rețea* cu o *abordare bazată pe efecte* se pare că ne aduce în față un nou potențial, deoarece atacarea elementelor de voință ale inamicului va diminua direct sau, cel puțin, va zădărnici încrederea noastră în distrugerea fizică. Nici o operație de succes a unei alianțe sau coaliții nu a fost executată fără să se țină seama de impactul acțiunilor asupra fiecăruia dintre parteneri.

De asemenea, nici o operație de răspuns la criză sau de menținere a păcii nu poate rămâne concentrată numai pe agresor, fără a lua în considerare cum vor reacționa alte state din regiune. Realitatea politică este că, deşi ne concentrăm asupra învingerii inamicului, operațiile militare, aproape întotdeauna, trebuie să vizeze sprijinirea aliaților şi liniştirea neutrilor, precum şi descurajarea simultană a unor potențiali viitori adversari, care, probabil, gândesc a se alătura inamicului pentru a ni se opune. Acest aspect al **concepției bazate pe efecte** se află în centrul operațiilor de coaliție, la toate nivelurile şi sub toate aspectele. De fapt, gândind în termenii operaților bazate pe efecte, putem oferi o bază pentru modul în care operațiile militare pot fi orchestrate în scopul formării comportamentului prietenilor şi al duşmanilor pentru a preveni războiul şi menține pacea. **Modalitatea de abordare bazată pe *efecte*** ne poate oferi, de asemenea, un cadru nu numai de aplicare corectă a operațiilor bazate pe rețea în luptă, dar şi de utilizare a acestora într-o varietate de roluri, de-a lungul întregului spectru al conflictului, de la pace, la criză şi apoi la război.

[15] **Effects-Based Operations**, Chapter 3, p. 107, Library of Congress Cataloging-in-Publication Data, Ed. 2002.

Schimbarea ponderii de la „armamente pe ținte” la „acțiuni concentrate” pentru a forma comportamentul adversarului şi al aliaților sugerează o definire largă a operațiilor bazate pe efecte. Operațiile bazate pe efecte sunt seturi de acțiuni coordonate, stabilite pentru a modela comportamentul prietenilor, neutrilor şi adversarilor în timp de pace, în situații de criză şi la război. Reținem aceasta ca pe o definiție a *operațiilor* bazate pe efecte. *Războiul bazat pe efecte* poate reprezenta un subset al acestor operații[16], în timp ce *ochirea bazată pe efecte* (cel puțin varietatea cinetică [17]) poate fi, la rându-i, un subset al războiului bazat pe efecte. Prin aceasta, noi am definit-o ca pe un „proces” în sine. Logic, dacă nu definim inițial ceea ce sunt operațiile bazate pe efecte, nu putem să începem să abordăm un proces referitor la modul cum să le plănuim şi să le executăm. De aceea, vom porni cu definirea termenilor-cheie în conceptul operațiilor bazate pe efecte şi a unui set de reguli derivate din utilizarea anterioară, încercând să identificăm procesul care va susține finalizarea conceptului. Definiția de mai sus a operațiilor bazate pe rețea prezintă, pe deasupra, o largă înțelegere a acțiunilor sau a setului de acțiuni şi a legăturilor acestora cu comportamentul. Termenul **acțiune** este în mod deliberat larg, pentru a subsuma nu numai acțiuni militare, dar şi politice, economice sau alte acțiuni ale guvernului şi, la fel de bine, ale agențiilor internaționale sau nonguvernamentale, precum şi ale actorilor nonstatali.

[16] *Alberts et al.* face o distincție clară între operația bazată pe rețea, aplicarea tehnologiilor bazate pe rețea, gândirea tuturor operațiilor militare şi războiul bazat pe rețea, precum şi în aplicarea lor, ca subset, în operații. ***Alberts et al.*** , ***Understanding Information Age Warfare***. p.58.

[17] Termenul de ochire utilizat aici este, în mod frecvent, contextual utilizat pentru atacarea şi producerea de pierderi în domeniul entităților psihice ale inamicului. Oricum, trebuie reținut că termenul poate fi utilizat şi în sensul *operațiilor informaționale*, care nu produc distrugeri psihice.

Termenul **comportament** este, de asemenea, larg, astfel încât să cuprindă nu numai inamicul, ci şi prietenii şi neutrii. El reflectă nu doar legăturile şi considerațiile care trebuie să rămână o fațetă importantă a succesului operațiilor de coaliție, ci lasă termenului *adversar* larghețea suficientă pentru a cuprinde atât un adversar într-o confruntare militară, cât şi un oponent într-o confruntare care nu reprezintă un conflict. Această distincție reflectă realitatea de astăzi a largului spectru al operațiilor militare şi, bineînțeles, larga varietate de utilizare a puterii militare de-a lungul istoriei.

Acțiunile pe care forțele militare sunt capabile să le execute, pot şi trebuie să cuprindă cu certitudine operații de luptă, şi anume, operații de lovire. *Dar forțele militare fac cu mult mai mult,* cele mai frecvente şi persistente misiuni militare fiind cele de prevenire a războiului, de obicei, prin descurajarea conflictului sau stoparea oricărei crize care ar putea escalada în război. În acest efort, forța militară este folosită, în mod obişnuit, împreună cu acțiuni politice şi diplomatice pentru a modela comportamentul observatorilor (prieteni, duşmani şi neutri), fie prin propriile acțiuni, fie prin simpla lor prezență în anumite zone. Şi pe plan istoric, autoritățile naționale au folosit aceste acțiuni în mod intenționat pentru a crea efecte particulare. Pe scurt, acțiunile din trecut ale forțelor militare au constituit, clar, operații bazate pe efecte, deşi nu au implicat acțiuni de luptă.

Pentru înțelegerea a ceea ce poate fi numit „spectrul complet al operațiilor bazate pe rețea”, trebuie, mai întâi, să ştim clar ce se înțelege prin ***efect.*** Termenul ***efect*** a fost folosit, în mod curent, în scrierile militare, pentru a defini totul, de la finalitate sau rezultate, până la obiectivele operaționale şi până la raza undei de şoc a componentei de luptă a armatei. Foarte frecvent, termenul *efect* este utilizat într-o conotație de planificare a efectelor probabile pentru a desemna impactul privind distrugerea unei anumite ținte asupra unei dimensiuni

strategice sau operaționale mai largi, remarcabil dezvoltată de colonelul John Warden, în conceptul privind *cercurile concentrice ale vulnerabilității* adversarului. În acest context, efectele nu sunt numai legate de impactul direct, care înseamnă distrugerea țintei, dar şi de cel al lanțului evenimentelor succesive sau al impactului indirect care apare. Procesul de identificare a nodurilor potențiale în acest canal sau în această cascadă de efecte ulterioare şi apoi exploatarea lor reprezintă baza pentru majoritatea eforturilor curente de urmărire nodală a țintelor.

În fiecare caz, într-o asemenea analiză nodală, bazată pe efecte, accentul se pune pe folosirea unei forme de distrugere a țintei ca agent pentru generarea cascadei de efecte ulterioare. Pentru scopurile acestei analize, vom lua obiective diferite şi vom explora conotația operațională mai generală, sugerată atât de cerințele mediului de securitate, cât şi de postulatul lui Sun Tzu, care spune: „*culmea îndemânării este a stăpâni un inamic fără luptă*".

Aceasta poate fi postulată mult mai simplu: *un efect este rezultatul sau impactul creat de aplicarea puterii militare sau a unei alte puteri.* Asemenea putere, desigur, poate fi aplicată la nivelul tactic, operațional, militar-strategic şi/sau geostrategic al conflictului. Cuprinderea acestei definiții presupune că efectele pot fi sau cinetice, sau noncinetice, sau pot fi, în aceeaşi măsură, fizice ori psiho-cognitive. Astfel, un efect poate fi distrugerea forțelor şi capabilităților adverse.

Dacă *operațiile bazate pe efect* sunt mai mult decât orice o teorie interesantă, din punct de vedere militar trebuie să definim un proces prin care să transferăm sigur acțiunile multiple în tipuri de efecte necesare pentru crearea comportamentului prietenilor, adversarilor sau neutrilor. Pe scurt, trebuie să planificăm şi să executăm, în realitate, operații bazate pe efecte, aplicând această teorie. Dirijarea acestor operații ca şi cum am avea o mare probabilitate de producere a efectului dorit

este o cerință mai uşor de afirmat decât de realizat. Stabilirea variabilelor descrise, referitoare la operația bazată pe efecte, chiar şi când le marcăm prin definirea elementelor acțiunilor militare sau prin trasarea tipurilor de efecte, rămâne complexă. Şi există cel puțin două niveluri adiționale ale complexității în problema pe care noi trebuie să o rezolvăm, înainte de a ne putea asuma planificarea şi execuția operației bazate pe efecte.

Un aspect al acestei complexități suplimentare **este totdeauna sugerat**. Orchestrarea pe care noi trebuie s-o realizăm nu presupune numai găsirea combinației corecte a acțiunilor, pentru a influența comportamentul „observatorilor" în direcția dorită, ci, de asemenea, identificarea şi evitarea acelor acțiuni care pot conduce comportamentul într-o direcție greşită.

În esență, dacă nu se reuşeşte organizarea corectă a eforturilor, variabilele pe care noi vizăm să le influențăm dau o expresie greşită a semnalelor asupra acțiunilor noastre şi vor tinde să se blocheze reciproc sau să îi nedumirească pe observatori, ca şi cum nu ar avea nici un efect, în final. Cu atât mai mult, acțiunile pot produce şi comportamentul care devine rapid opusul a ceea ce am intenționat.

Planificarea operațiilor bazate pe efect trebuie să fie în măsură nu numai să concentreze acțiunile noastre, ci, de asemenea, să le facă să nu fie în conflict de-a lungul a patru niveluri de comandă sau a trei sau mai multe zone ale operațiilor bazate pe efecte. Şi mai mult, acțiunile noastre trebuie să nu devină antagonice, nu numai din respect pentru observatorul singular, dar şi din respect pentru multiplele şi foarte diversificatele perspective sugerate de către „amici, inamici şi neutri" definiți în operația bazată pe efecte. Influențarea acestui comportament înseamnă a te confrunta cu percepția ființei umane, a cărei fiecare reacție va fi diferită şi care nu poate fi nici liniară şi nici predictibilă, în întregime. Deja, a planifica operația bazată pe efecte implică anticiparea

unui sistem complex, adaptiv, de observare a acțiunilor proprii, individuale sau colective, care să fie în măsură să se adapteze şi să răspundă solicitărilor stimulilor.

La prima vedere, această cerință sună ca o contradicție de termeni. Cum prezicem ce reacții poate avea un sistem complex şi adaptiv, care, prin definiție, nu este întru totul predictibil? Cum facem ca aceeaşi acțiune să pară diferită pentru diferiți observatori? S-a stabilit un standard imposibil pentru operațiile bazate pe efecte? Cerința de a coordona toate aceste elemente aşa încât să creeze un efect unitar, pare, cu siguranță, descurajatoare. Oricum, putem fi consolați din două puncte de vedere. **Primul** – un eşec în abordarea acestor niveluri de complexitate nu trebuie să le îndepărteze. Firește, logic, putem să anticipăm, în absența oricărui efort din parte noastră, modalitatea de a le orchestra, probabilitatea unor erori în acțiunile sau în efectele produse putând fi, totuşi, mare. **Al doilea**, faptul că exemplele folosite în această muncă au fost extrase din istorie poate transmite un mesaj. Coordonarea cu succes a efectelor nu este niciodată imposibilă şi nici nouă, marii conducători politici şi militari, în istorie, au fost „mari", în parte şi datorită faptului că au putut să pună toate aceste elemente la un loc. Problema noastră este, mai curând, cum noua revoluție tehnologică şi conceptele bazate pe rețea ne permit să răspundem acestei cerințe mai bine, mai repede şi cu mai mare precizie.

În planificarea unei operații bazate pe efecte ne preocupă provocarea alegerii unui canal de reacție controlat decât unul de reacție necontrolat, ale cărui consecințe nu le putem anticipa.

În acest scop, trebuie să ne punem două întrebări. **Prima:** cum s-a produs canalul sau cascada efectelor? **A doua:** cum poate această cascadă a efectelor să se producă, în contextul mecanismelor bazate pe efecte, subliniate în regula stabilită în cadrul celor de influențare a comportamentului?

Primul pas în confruntarea cu noile dimensiuni ale complexității este punerea la un loc a pieselor acestui puzzle bazat pe efecte, pe care noi îl vom explora. În această discuție privind evoluția generală a conceptului de operații bazate pe efecte există trei mari componente ale puzzle-ului care sunt împrăştiate:

Prima, privind ciclul cognitiv. Am început să descriem dimensiunea umană a procesului de luare a deciziei, urmărind modul în care ființa umană şi organizațiile percep acțiunile, le dau sens şi le înțeleg, pentru ca, pe mai departe, acestea să poată răspunde unei situații de criză. Acest proces cognitiv descrie nu numai variabilele inerente în procesul de luare a deciziei, dar, în contextul ciclului de reacție al operațiilor bazate pe rețea, se oferă o pătrundere a felului în care variabilele au influențat crearea comportamentului altora. Atât timp cât această pătrundere nu poate modifica complexitatea reacțiilor umane, ea ne oferă, pe o bază logică, viitoarele limite ale unei complexități întortocheate.

A doua, privind perspicacitatea câştigată de procesele cognitive, care permite definirea dimensiunii acestor acțiuni, şi efectul pe care-l au în mintea noastră. Aşa cum se prezintă în fig. 5, atributele acțiunilor descrise prin elementele acestora urmăresc modificarea percepției, afectarea deciziei şi producerea acelui gen de efecte care determină deciziile observatorului şi comportamentul acestuia într-o direcție anume.

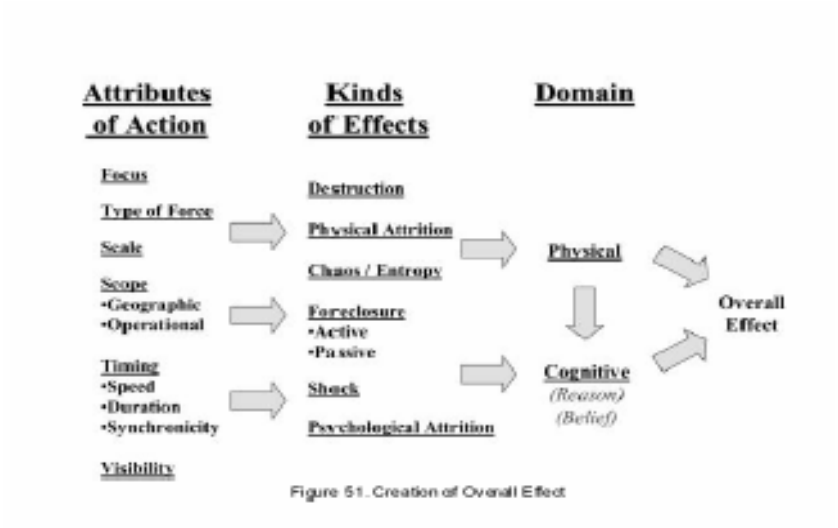
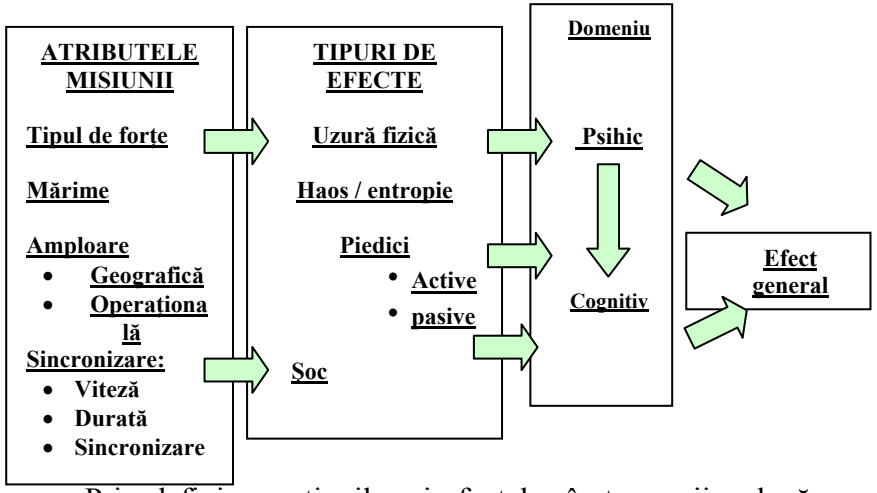


Fig. 5



Prin definirea acţiunilor şi efectelor în termenii a două variante de stabilire a variabilelor, mai curând cele care există ca o infinitate de varietăți ale posibilelor acțiuni şi efecte, noi

delimităm problema şi creăm astfel un meniu de opțiuni ale variabilelor, disponibil pentru orchestrarea efectelor necesare asigurării unor efecte finale unitare. Folosim adesea o serie de evenimente din crizele Orientul Mijlociu pentru a demonstra, din punct de vedere istoric, cum am folosit aceste opțiuni şi am modificat natura acțiunilor militare, pentru a crea efecte specifice. Această relație între acțiuni şi efecte oferă elementele de ansamblu pentru planificarea şi desfăşurarea operațiilor bazate pe efecte.

În ceea ce priveşte cea de-a treia componentă, aceasta vizează definirea ciclului mecanismului acțiune - reacțiune în operațiile bazate pe efecte. Regula bazării pe efecte stabileşte ceea ce ne conduce, în prezent: de la crizele Orientului Mijlociu şi o serie de exemple din anumite războaie, care înlătură ideea rigidă asupra modului în care ciclul acțiune - reacțiune lucrează, în lumea reală a operațiilor bazate pe efect. Regula astfel stabilită a început să definească structurile de decizie şi organizaționale utilizate în astfel de operații. Deşi această descriere funcțională a fost utilizată pentru prima dată în procesul de luare a deciziei de către partea americană a conflictului, interacțiunile crizei au demonstrat clar că pot fi, de asemenea, utilizate aproximativ la fel de către oricare stat-actor. Astfel, regulile stabilite mecanic oferă un cadru în care planificarea şi execuția operațiilor stat contra stat sunt bazate pe efecte şi pot fi luate în considerare. Aceste pătrunderi în procesul cognitiv şi în cadrul mecanismelor sistemului sunt, în particular, relevante pentru procesul de planificare şi execuție a operațiilor bazate pe efecte, aşa încât să se asigure impactul neliniar pe care-l vizăm. Multe dintre problemele cu care se confruntă procesele de planificare şi de execuție ale operațiilor bazate pe efecte conduc către necesitatea de a prevedea răspunsurile individuale sau ale organizațiilor pe care noi intenționăm să le stimulăm.

Dacă planificăm deliberat şi logic, trebuie să fim în măsură să anticipăm cum un efect inițial sau direct, creat de acțiunile noastre, va propaga efecte secundare. Acest pas este important, deoarece speranța noastră de a crea impacturi neliniare creşte, în cele din urmă, în parte, ca urmare a aşteptărilor ca acțiunile să deschidă un canal sau o cascadă a efectelor indirecte ale căror scop şi amploare pot reduce efectul creat inițial.

Două clarificări suplimentare sunt necesare aici:

Prima, *acțiunile pe care le-am avut în vedere sunt, prin definiție, de natură fizică.* Alternanța acțiunilor şi reacțiilor din punct de vedere fizic a fost reflectată în ciclurile acțiune – reacție în regulile stabilite. În mod similar, procesul cognitiv se desfăşoară prin aceleaşi acțiuni, care pot fi observate sau percepute în acelaşi mod, fiind chiar definite acțiunile în termenii acțiunilor sau evenimentelor fizice.

A doua impune *să facem, permanent, o distincție între efectele fizice directe* (impactul fizic imediat al unei acțiuni) şi *efectul indirect* (unul din seria celor produse sau din seria efectelor derivate din efectele directe). Acestea pot fi, de asemenea, de natură fizică, dar, în acelaşi timp, pot fi psihologice sau cognitive, care decurg din acțiunile fizice inițiale.

Ideea creării efectelor în cascadă nu este nouă. Bombardamentul din cel de-al doilea Război Mondial în sprijinul debarcării din Normandia este un exemplu bun de planificare deliberată a cascadei de efecte psihologice. Efectul psihic direct vizat de planificatorii campaniei aeriene aliate, aşa-numitul „Plan de transport", a fost distrugerea comunicațiilor Normandiei cu plajele. În expresia lui Churchill, bombardamentul a menit a crea o „cale ferată de deşert" în jurul Normandiei[18].

[18] W. CHURCHILL, **Closing the Ring**, p.528.

Obiectivele reale ale planificatorilor au fost două efecte fizice directe: să facă *indisponibil sistemul de cale ferată în nordul Franței* pentru ca manevra pe calea ferată să devină foarte grea sau imposibilă, *să prevină deplasarea diviziei de tancuri germană în zona Normandiei* în orele critice sau după ziua „D" a debarcării.

În loc de concluzii

a) Operațiunea „Scutul Deşertului" din 2003 a subliniat: importanța raportului dintre dimensiunea unei forțe stabilite pentru misiune şi posibilitățile de susținere şi operare în teatru şi posibilitatea de a acționa în comun, într-o operație întrunită la mare distanță, în afara granițelor statului căruia îi aparține forța.

b) Domeniul operațiilor bazate pe rețea a scos în evidență necesitatea ca, la nivelul Armatei, să se realizeze acele redimensionări necesare creării unor forțe expediționare în măsură ca, într-un interval foarte scurt de timp (zeci de zile), să treacă la îndeplinirea misiunii (începerea deplasării în teatru).

c) Un element important, care a condus la posibilitatea operării în comun, este necesitatea utilizării imaginii generale a câmpului de luptă, realizată atât de mijloacele de cercetare ale comandamentului multinațional (națiunii lider), cât şi de cele proprii, precum şi folosirea limbii engleze. Realizarea este posibilă, datorită utilizării în comun a aplicațiilor SATCOM APPLICATION şi a sistemelor integrate, compatibile la nivelul standardelor Alianței.

d) „Elementele de profunzime şi provocările *transformării bazate pe operația în rețea*[19] sunt: transformarea bazată pe Operația în Rețea (OBR) presupune toate liniile de

[19] În viziunea lui John Garstka.

dezvoltare; tehnologia este cea mai importantă capabilitate (beneficiu clar prin dirijarea investițiilor în elemente-cheie); schimbările doctrinare (ale proceselor) şi organizatorice sunt elementul de bază în realizarea capabilităților de operare în rețea; experiența operațională cu capabilități OBR este factor de bază în transformarea apărării pe baza capabilităților OBR; leadership-ul şi educația sunt elementele critice pentru a face posibilă transformarea bazată pe capabilități facilitate de rețea.

CONCEPTUL DE RĂZBOI BAZAT PE REȚEA – APLICAȚII ÎN OPERAȚIILE SPECIALE ŞI COMBATEREA TERORISMULUI

Colonel Marius CRĂCIUN

Şocul generat de evenimente internaționale de notorietate, precum atacurile teroriste, influențează decizii politice la nivel global, generează reacții în lanț, unde de şoc şi schimbări majore de strategie. Definit uneori ca un „război ascuns, nedeclarat" sau ca un „conflict de mică intensitate (cu obiectiv limitat)", acest fenomen a depăşit stadiul improvizațiilor, al unor „simple" asasinate sau atentate cu bombe.

Secolul XXI a adus, alături de elementele unei noi Revoluții în Domeniul Militar (RMA), şi manifestări violente asimetrice, greu de decodificat, precis orientate şi foarte bine organizate, care creează o psihoză generalizată a terorii, nespecifică pe timp de pace şi, cu atât mai mult, amplificată şi diversificată în situații de criză sau de război. În consecință, a apărut şi necesitatea unei noi abordări a acestor pericole.

Procesul de transformare pe care trebuie să îl parcurgă Armata României determină, pe de o parte, schimbări în plan doctrinar, conceptual, adoptarea unei noi viziuni asupra luptei, operației şi strategiei, în concordanță cu noile concepte strategice de ducere a războiului şi cu exigențele ce decurg din angajamentul României de a acționa ca aliat egal şi credibil în operații multinaționale în cadrul NATO sau al altor aranjamente politico-militare. Pe de altă parte, procesul de transformare impune reformă structurală, eforturi de integrare şi aliniere sistemică cu structurile similare. În acest context, introducerea şi aplicarea unor concepte moderne, precum cel al războiului bazat pe rețea, generalizarea treptată a tehnologiei

digitale în spațiul de luptă al secolului XXI, apariția noilor generații de arme inteligente, sistemele C^4I^2SR[20], tehnicile și tehnologiile războiului electronic, informațional şi psihologic nu mai pot lipsi din nici o confruntare armată şi este evident că vor fi folosite masiv în viitoarele operații.

Integrarea deplină a României în NATO impune atingerea, cu responsabilitate, a unui grad de interoperabilitate necesar, mai ales dacă nivelul de angajare este ridicat. Demersul, la prima vedere, destul de simplu, este, de fapt, o mare provocare şi o sarcină dificilă pentru toate structurile statului cu responsabilități în domeniul securității şi apărării colective, dar, mai ales, pentru Ministerul Apărării Naționale.

Tipul de război pentru care trebuie să se pregătească Armata Română nu este războiul prezentului, ci al viitorului, mai exact, al următorilor douăzeci de ani, războiul anilor 2015-2025.

Realitățile conflictelor din ultimele decenii, inclusiv ale acțiunilor teroriste şi antiteroriste recente, au arătat că, interetnice sau interconfesionale, cu trend-uri mai mult sau mai puțin naționaliste, cu caracter terorist sau aflate sub steagul „luptei pentru independență", conflictele asimetrice şi-au pus amprenta asupra sfârşitului şi începutului de mileniu.

Fenomen social de factură aparte şi „campion" în ierarhia conflictelor asimetrice, terorismul a dobândit, în acest început de secol şi mileniu, prin amploarea şi diversitatea formelor de manifestare, impactul mediatic şi viteza de circulație a informației, un caracter global, extins la scară planetară. Din ce în ce mai des pe ecranele media apar cuvintele "Breaking News", semnalând o nouă acțiune teroristă, de o violență în permanentă ascensiune, un nou vector de răspândire a groazei, care tulbură profund viața normală a

[20] **Command, Control, Communication, Computers, Information, Surveillance, Reconnaissance -** Comandă, control, comunicații, computere, informații şi informatică, supraveghere şi recunoaştere.

societății, punând în pericol chiar existența şi funcționarea unei democrații cu tradiții.

La început de secol, națiunile nu mai sunt aşa de preocupate de pericolul unei agresiuni de amploare, ci, mai degrabă, de tensiunile şi antagonismele generate de conflictele şi disputele etnice, terorism, crimă organizată, proliferarea armamentelor, migrarea neautorizată şi disputele economice. Pentru a rezolva aceste riscuri atipice, din ce în ce mai multe națiuni adoptă mijloace de contracarare atipice, din domeniul operațiilor speciale.

În mod tradițional, în combaterea terorismului, majoritatea statelor adoptau strategii reactive, iar unele chiar strategia de sanctuar, care prevede că o organizație teroristă este lăsată în pace de autorități atât timp cât nu desfăşoară nici un fel de acțiuni ostile pe teritoriul său.

După 11 septembrie 2001, tot mai multe voci au afirmat că, pentru a fi eficientă, combaterea terorismului trebuie să treacă de la caracterul reactiv la cel activ sau proactiv. În aceste condiții, structurile politice şi de securitate caută soluții care să asigure prevenirea, combaterea, gestionarea unei crize teroriste, chiar prin acțiuni preventive.

Pentru o perioadă relativ lungă, România a fost în general ferită de atacuri teroriste. Procesul de integrare politică şi militară pe care l-a parcurs România în ultimii 15 ani a creat însă şi posibilitatea de a avea pierderi de vieți omeneşti, din rândul conaționalilor, în afara teritoriului național.

În această lucrare ne propunem să identificăm elementele de bază ale conceptului RBR ce pot fi folosite în operațiile speciale şi în combaterea terorismului, precum şi responsabilitățile naționale în cadrul integrării în NATO.

1. Relația Câmp de luptă – Spațiu de luptă

În demersul ştiinţific de a prefigura modul de ducere a conflictelor şi principalele elemente ale războiului anului 2025, am ajuns la concluzia că tehnologiile militare ale viitorului vor avea un impact consistent şi remarcabil. Noile cuceriri tehnologice fac ca acțiunile militare să aibă, azi, dar probabil şi în viitor, o mare amploare în timp şi spațiu, forțe şi mijloace specializate, caracter întrunit, intensitate şi complexitate sporite, schimbări bruşte ale situațiilor la toate nivelurile, să fie duse în toate mediile, deosebit de manevrier şi cu o mare diversitate de procedee tactice.

Secolul XXI face din război spațiul de întâlnire al unor sisteme militare din ce în ce mai complexe şi performante, care implică tehnologii noi, militari superspecializați, acțiuni complexe, desfăşurate pe coordonate strategice şi tactice diferite de cele actuale.

Inovația tehnologică are drept obiectiv şi scop sporirea capabilității forței. Iar capabilitățile luptei moderne sunt influențate, cum apreciază analiştii conflictelor recente, de relativul echilibru tehnologic.

Pe de o parte, avansul tehnologic influențează şi va continua să influențeze hotărâtor evoluția conflictelor armate. Noile generații de arme inteligente, sistemele C4I, sistemele electronice de supraveghere, cercetare şi lovire, tehnicile şi tehnologiile războiului informațional şi psihologic nu mai lipsesc din nici o confruntare militară şi vor fi folosite masiv în viitoarele operații şi lupte. Sunt de remarcat amploarea pe care o au componentele dislocate în spațiul cosmic în desfăşurarea eficientă a operațiilor, accentuarea caracterului decisiv al confruntării, sincronizarea şi integrarea acțiunilor de luptă. Sistemele de arme ale armatelor moderne permit folosirea lor în orice punct al globului, fără ca distanța să mai constituie un impediment, cel puțin din punct de vedere al conducerii. Spațiul

de luptă al secolului XXI este termenul folosit din ce în ce mai mult de către țările cu un sistem militar modern. În doctrina americană, în timpul anilor '90, conceptul de spațiu de luptă (battle space) a înlocuit conceptul de câmp de luptă (battle field), care a definit conflictul armat din timpul campaniilor lui Alexandru Macedon până la al doilea Război Mondial.

În esență, conceptul de spațiu de luptă a permis o trecere de la organizarea lineară a trupelor către o concentrare a efectelor pe toate dimensiunile şi simultană (full-dimensional)[21]. Subscriem şi noi întru totul acestei concepții.

Pe de altă parte, tot mai multe state, printre care şi România, abordează concepte strategice globale, unde interesele naționale de securitate nu se mai rezumă la apărarea teritoriului național, vechile distincții între conflictul civil, cel național şi cel internațional, între securitate internă şi externă (internațională) au început să se disipeze.

Doi strategi chinezi au argumentat că păşim într-o eră în care „nu există teritoriu care nu poate fi depăşit; nu există mijloace care nu pot fi folosite în război; şi nu există teritoriu sau mijloc care să nu poată fi folosite împreună"[22].

Nu în ultimul rând, în cadrul RBR, „diferențele clare dintre elementele de dispozitiv, dintre față şi spate, sau dintre teatre de operații şi teatre de acțiuni militare strategice vor continua să dispară, pe măsură ce instrumentele războiului devin din ce în ce mai interdependente şi, valabil în cazul comunicațiilor şi sistemelor spațiale, pe măsură ce scad

[21] Pentru mai multe detalii cu privire la doctrina americană, a se vedea **Operations, Field Manual 3-0**,U.S. Army Dept., Washington, D.C., Department of the Army, June 2001, pp 4-20 - 4-21.

[22] LIANG, Qiao and XIANGSUI, Wang, *Unrestricted Warfare,* Beijing, People's Liberation Army Literature and Arts Publishing House, 1999, p.199, apud EVANS, Michael. *Military Theory and the Future of War*, Naval War College Review, Volumul 56/ 3, 21 iunie 2003, pp. 8-9.

diferenţele calitative şi financiare între sistemele militare şi cele comerciale”[23].

În consecinţă, în contextul actual, când inamicul poate fi prezent peste tot, inclusiv pe frontul mass-media, iar componenta de protecţie a forţelor, populaţiei şi centrelor de greutate proprii, strategice şi operative, devine din ce în ce mai importantă, implicit dependentă de tehnologia modernă şi mare consumatoare de resurse, considerăm că Teatrul de Operaţii Militare, ca instrument militar care defineşte o entitate geografică cu un anumit specific, s-a disipat şi îşi pierde din relevanţă.

2. Conceptul de Război Bazat pe Reţea (RBR)

O grupă de cercetare, aflată într-o maşină de luptă, în faţa forţelor principale, transmite instantaneu, prin staţia de la bord, prin accesarea reţelei de comunicaţii prin satelit, informaţii şi imagini digitale cu dispozitivul irakian pe una din căile de acces spre aeroportul internaţional din Bagdad.

Şeful G3 al unui batalion de tancuri, ale cărui elemente înaintate se deplasează în viteză pe autostradă spre aeroport, aflat în punctul de comandă mobil, vizualizează de la postul său de lucru imaginea digitală, tridimensională, a terenului prin care urmează să treacă în următoarele minute întreg batalionul, cu dispunerea tuturor elementelor din dispozitivul irakian.

Cu click-uri repetate de mouse, planifică pe harta digitală manevrele şi focul tancurilor, cu mult înainte ca obiectivele să intre în bătaia tunurilor de pe tanc sau a rachetelor de pe transportoarele Bradley.

Automat, misiunea este transmisă tuturor echipajelor, inclusiv elicopterelor de atac care asigură din aer deplasarea coloanei, iar sistemele amic-inamic încep dialogul prin care îşi

[23] CZEGE, HUBA Wass and Sinnreich, Richard HART, *Conceptual Foundations of a Transformed U.S. Army*, Institute for Land Warfare Paper 40, Washington, D.C., Association of the United States Army, March 2002.

precizează reciproc poziţiile în teren. Astfel, imaginea de la un UAV[24] de tip Predator, suprapusă peste harta digitală a Bagdadului, realizată anterior şi extrem de detaliat, cu ajutorul reţelei de sateliţi, la care se mai adaugă şi diferite informaţii obţinute din aer sau de la sol, prin observare şi înregistrare video, la care contribuie şi grupa de cercetare, compun o singură imagine compozită digitală tridimensională. Imaginea compozită descrisă anterior, pusă la dispoziţia conducătorilor coaliţiei în ultimul conflict din Golf, asigură, în opinia noastră, cel mai eficace instrument aflat vreodată la dispoziţia unui comandant.

Această capacitate de digitalizare uniformă, suprapusă, folosind aceleaşi caracteristici, informaţii provenite din mai multe surse, total diferite ca parametri tehnici, este considerată o mare realizare tehnologică, deşi, pe de o parte, nu a făcut vâlvă în rândul nespecialiştilor, inclusă fiind aici şi mass-media, iar, pe de altă parte, rămâne încă inaccesibilă tehnologic pentru majoritatea armatelor.

Conceptul RBR a fost creat şi folosit pentru prima dată în Statele Unite ale Americii, printr-o replică militară a unor acţiuni civile în domeniul afacerilor.

Conceptul a apărut în mod deosebit în cadrul forţelor navale americane, unde apărarea antiaeriană a unei grupări de nave, stabilită pentru escorta şi protecţia unui portavion, trebuia coordonată dintr-un singur loc, şi, cu viteza dată de timpul necesar pentru descoperirea şi indicarea ţintei, făcute transmiterea informaţiei şi lansarea loviturii selectate. Întrucât acest timp nu trebuia să fie mai mare de două minute, excludea intervenţia directă a omului.

Aşa a apărut conceptul de reţea de apărare antiaeriană, extrapolat la toate sistemele grupării de nave şi, ulterior, la alte platforme din categorii de forţe diferite.

[24] Unmanned Aerial Vehicle – vehicul aerian pilotat de la sol, avion fără pilot.

Conceptul orientează dezvoltarea sistemelor de apărare spre un nivel nou al acțiunilor întrunite şi interagenții, aşa cum este prefigurat pentru viitoarele conflicte.

Astfel, pentru viitorii 20-30 de ani, se pot anticipa schimbări fără precedent, care vor afecta profund organismele militare, implicând căi de operare încă neimaginate, angajând tehnologii încă neinventate, care oferă un potențial exponențial de creştere a capacităților de luptă.

Până la urmă, RBR nu este o problemă de tehnologie, cum s-ar crede, ci una organizațională[25], de a asigura o integrare totală în rețea a tehnologiei, o interoperabilitate deplină. Iar acest complicat proces trebuie început cât mai curând posibil, folosind toate resursele de răbdare şi inteligență.

Rezultanta acestei combinații este cunoaşterea în detaliu, în timp cât mai apropiat de cel real, a spațiului luptei, dar şi a „evenimentelor“ semnificative din alte zone, nu neapărat în aceeaşi zonă geografică, dar care prezintă interes pentru planificarea şi conducerea acțiunilor militare. Dezvoltarea componentelor RBR, adoptarea acestui concept şi de alte puteri militare, acoperirea deja globală a unor mijloace de lovire, care execută misiunile de luptă direct din baza de dislocare la pace, fără o desfăşurare strategică prealabilă, pericolul unor acțiuni asimetrice, de tip terorist, toate vor duce la transformarea globului pământesc în spațiu strategic unic.

Considerăm că RBR reprezintă un ansamblu de concepte operaționale şi capabilități militare, coagulate de o soluție tehnologică şi operațională de interconectare, care permite forțelor să folosească avantajul utilizării tuturor informațiilor disponibile, concomitent cu angajarea întrunită, coerentă, flexibilă, rapidă şi eficientă a mijloacelor de luptă.

[25] Apud general-locotenent Brian Joseph K. KELLOG Jr., citat de AKERMAN Robert K., în articolul *Military Cristal Ball Portends Network Centric Supremacy*, din revista Signal, 2001.

Obiectivele principale ale RBR sunt: creşterea ritmului operațiunilor, sporirea vitezei de reacție, reducerea riscurilor şi a costurilor pentru forțele proprii şi, pe cale de consecință, creşterea eficienței misiunilor.

Determinarea cu care o serie de mari firme americane, producătoare de echipamente militare, s-au lansat în operaționalizarea unor programe de integrare a conceptelor RBR, volumul impresionant al investițiilor şi folosirea tehnicilor de simulare pentru a putea determina tendințe în domeniu, inclusiv estimări de costuri şi programe de implementare, arată importanța acordată RBR.

Putem concluziona că Războiul Bazat pe Rețea este un război modern, în care se folosesc sistemele C^4I^2SR, organizate într-o rețea centrală, o rețea a senzorilor şi o rețea a platformelor de luptă, că se bazează pe tehnologia informației (IT), pe sisteme de armamente performante şi capabilități tehnice deosebite. Conceptul se fundamentează pe integrarea **sistemelor (senzorilor)** de culegere şi prelucrare a informației, a **sistemelor C^2** şi a **platformelor de luptă**, asigură scurtarea semnificativă a ciclului de conducere, astfel încât decalajul între informația despre obiectiv şi lovirea acestuia să fie redus la minim, până spre zero, dacă se poate, moment în care reacția este instantanee, generată de tehnologia informatică şi doar supervizată de om.

În războiul viitorului, proliferarea vehiculelor fără pilot, terestre, aeriene, maritime, a materialelor şi proiectilelor „invizibile” şi încorporarea acestora în rețea ar putea face ca un număr copleşitor de ținte să devină accesibile. Pentru exemplificare, folosim binomul aeronavă – blindat. În războiul clasic au existat întotdeauna măsuri şi contramăsuri între aceste două platforme.

Spre deosebire de un tanc-platformă de luptă, un tanc-element de rețea, cum este Sistemul de Luptă Viitor al Armatei

SUA[26], va fi constituit dintr-un sistem de sisteme, mai multe vehicule folosite ca unul singur. Dacă aceste vehicule sunt, de asemenea, proiectate să fie „invizibile", protejate prin contramăsuri active şi pasive şi coordonate cu grijă pentru mărirea avansului şi micşorarea vulnerabilităţii la atacurile aeriene, provocarea pentru forţele aeriene va creşte pe măsură. Mai multă muniţie va fi folosită pentru lovirea fiecărei ţinte şi mai multe ţinte atacate - atât de multe încât ele vor copleşi, prin numărul lor, capacitatea forţelor aeriene de a le opri înaintarea.

Acelaşi lucru s-ar putea spune, probabil, şi despre o forţă aeriană care foloseşte un număr mare de aparate de zbor mici, „invizibile", ieftine şi fără pilot sau nave maritime cu aceleaşi însuşiri ca şi aeronavele mai sus menţionate. Atacul roiurilor de microroboţi sau nanoroboţi va permite ca acest mod de abordare să fie dus la extrem.

Continuând analiza unui exemplu anterior, să presupunem că un analist al unei structuri de informaţii oarecare, aflat în faţa calculatorului, accesează imaginile oferite de un UAV de tip Predator, aflat în zbor deasupra Irakului. După mai multe ţinte vizualizate, acesta găseşte una pe care o consideră importantă. Creează în propriul calculator un dosar cu obiective, unde introduce datele respectivei ţinte şi a altor obiective de rezervă din zonă, pe care apoi îl trimite atât unui bombardier aflat în zbor deasupra Irakului, cât şi celulei de planificare a ţintelor. Analiştii acestei structuri, pe parcursul a câteva minute, verifică dacă pentru respectivul obiectiv au mai fost stabilite şi repartizate misiuni altor mijloace de foc, după care transmit către bombardier acceptul de a lovi respectivele obiective. Navigatorul bombardierului preia coordonatele, de fapt, acceptă transferul electronic al acestora în propriul computer de bord şi în calculatoarele bombelor sau rachetelor cu mare precizie de

[26] AFCS - US Army's Future Combat System. Pentru mai multe detalii a se vedea Charles J. DUNLAP, Jr., *21st-Century Land Warfare: Four Dangerous Myths*, Parameters, 27 (autumn 1997), pp. 27-37.

lovire şi, în câteva secunde, este în măsură să treacă la executarea un atac asupra obiectivului respectiv.

Sau, dacă, din diferite motive, bombardierul nu mai poate executa misiunea, transmite informaţiile în computerele din Centrul de Informaţii şi Luptă[27], de unde coordonatele obiectivului, tot în format electronic, ajung în sistemul de dirijare al unei rachete de croazieră Tomahawk.

După atac, Predatorul se întoarce şi trimite ultimele imagini, pentru procesul de analiză a îndeplinirii misiunii (Battle Dammage Assesment –BDA).

Softul existent în reţea permite analiza unor informaţii electronooptice, în spectru infraroşu sau imagine radar, stabilirea cu exactitate a coordonatelor tridimensionale: latitudine, longitudine şi altitudine. Iar când capacitatea de înmagazinare şi viteza de transmitere a reţelei sunt ridicate, atunci imaginile se pot suprapune peste imaginile stereoscopice din banca de date a Agenţiei Naţionale de Informaţii Geospaţiale, pentru a fi comparate[28]. Un exemplu de succes în aplicarea conceptelor RBR în folosirea aparatelor de zbor fără pilot, de tip Predator, care, pe lângă aparatura de detecţie şi localizare, mai au şi posibilităţi de atac deosebit de eficiente. Capacitatea de a supraveghea, pentru o lungă perioadă de timp, un obiectiv printr-un asemenea senzor, concomitent cu posibilitatea de a lovi eficace anumite ţinte din cadrul obiectivului, constituie un mare pas înainte, care duce la scurtarea radicală a ciclului de decizie.

Am concluzionat anterior că RBR este un concept care evidenţiază o modalitate nouă de a genera putere de luptă, prin integrare într-o reţea informaţională a senzorilor, decidenţilor şi executanţilor, în scopul cunoaşterii cuprinzătoare şi permanente

[27] CI – Combat and Information Center, Centrul de informaţii şi luptă, centrul nervos al unei nave de luptă.

[28] COLARUSSO, Laura, *Indicarea precisă a inamicului*, în Defense News, 4 ian 2005, p. 14.

a spațiului luptei, măririi eficienței conducerii, accelerării dinamicii operațiilor, realizării sinergiei efectelor planificate pe obiective, sporirii viabilității şi obținerii unui anumit grad de autosincronizare acțională.

Războiul bazat pe rețea reprezintă, în actuala eră informațională, o soluție militară de abordare a conflictului, similară conceptului de e-business în domeniul afacerilor.

Rețeaua de senzori cuprinde:

- componenta cosmică, dată de sateliții clasici şi, mai nou, de sateliții suborbitali, mult mai ieftin de lansat;
- componenta aeriană, dată de senzorii dispuşi pe avioane de cercetare şi radar, avioane fără pilot, elicoptere, baloane etc.;
- componenta navală, dată de senzorii de pe nave de cercetare şi supraveghere, de pe navele de luptă, sau dislocați pe sol, în apropierea unor puncte obligatorii de trecere;
- componenta terestră, dată de senzorii de pe mijloace de cercetare terestră şi antiaeriană, ai celor de pe platformele de luptă, ai forțelor speciale, ai unor tipuri speciale de muniție etc.;
- componenta instituțiilor (agențiilor) cu atribuțiuni specifice de combatere a criminalității transfrontaliere şi terorismului;
- componenta din ciberspațiu, dată de senzorii plasați în rețeaua Internet, cei de supraveghere a convorbirilor radio şi telefonice, senzorii de supraveghere a rețelelor proprii;
- elementul uman, adică operatorul.

Manevra acestor mijloace, gradul de utilizare (permanent sau secvențial), concentrarea lor în zonele de interes, interferențele de complementaritate permit o foarte bună cunoaştere şi actualizarea permanentă a situației în spațiul de luptă.

Rețeaua de decizie, comandă şi control este alcătuită din comandanți, comandamente strategice şi operaționale care, pe baza datelor şi informațiilor furnizate de subsistemul de detecție, decid, planifică şi alocă resursele necesare execuției.

Structurile de decizie au posibilitatea să primească date şi informații pe mai multe canale, de la o mulțime de senzori, să verifice rapid aceste date şi informații, să ia o hotărâre oportună, cu un suport informatizat permanent actualizat şi o bază de date funcțională, să transmită aproape instantaneu comanda şi să realizeze în permanență coordonarea. Cea mai mare parte a activităților din acest lanț se efectuează automat, potrivit unor standarde şi protocoale bine elaborate, verificate şi verificabile, capabile de perfecționare prin autoreglare.

Rapiditatea circulației informației şi posibilitatea practică de a lovi toate elementele de dispozitiv ale inamicului presupun:

- coordonarea C^2 asupra forțelor şi mijloacelor proprii şi aliate;
- generarea rapidă a informațiilor, introducerea în flux şi folosirea lor oportună;
- planificarea şi integrarea acțiunii tuturor elementelor şi introducerea modelelor de autosincronizare, pentru realizarea efectelor sinergice;
- interconectarea cu structuri şi agenții guvernamentale sau structuri civile.

Existența rețelelor şi a sistemelor moderne de comandă şi control, care fac posibil schimbul instantaneu de informații şi permit conducerea, indiferent de locul de dislocare pe glob, creând doar ceva probleme din cauza diferenței de fus orar, schimbă concepția clasică cu privire la locul şi rolul comandamentelor pe diferite trepte ierarhice.

Aceste rețele asigură cel puțin trei căi de transmitere date şi informații, inclusiv posibilitatea teleconferințelor, a transmiterii imaginilor despre inamic în timp real. Acoperirea globală dată de rețelele de sateliți impune schimbări majore în stabilirea unei viitoare arhitecturi de comandă şi control, inclusiv în locul de unde comandantul conduce lupta.

Una din cutumele trecutului spunea că un comandant de companie trebuie să-şi conducă subunitatea dintr-un punct de comandă aflat la maximum un kilometru de elementele de la contact, iar punctul de comandă al unei brigăzi trebuia dispus la o distanţă care să-l scoată de sub focul artileriei de un anumit tip. Considerăm că aceste cutume, ca unic factor pentru luarea în considerare a unei anumite soluţii, s-au disipat şi vor dispărea în viitorul apropiat, tocmai din cauza RBR.

Comanda si controlul, privite ca un proces de decizie, se materializează în planuri de operaţii sau strategice. Epoca informaţională, reprezentată de sistemele informatice interconectate prin mijloace de comunicaţii performante, permite un mare flux de date şi informaţii furnizate oportun de senzori multipli şi eficienţi.

Schimbarea importantă pe care o aduce RBR în strategia operaţională este înlăturarea datelor şi informaţiilor inutile (fiecare primeşte informaţia de care are nevoie), deci selectarea informaţiei, printr-un sistem de filtre, competenţe, funcţionalităţi şi protocoale de acces, asigurând astfel decizia rapidă, lovirea precisă şi, în tot acest timp, protecţia completă.

De asemenea, principalele aspecte care trebuie punctate în domeniul managementului informaţiilor sunt: existenţa unor conexiuni multiple între diferitele entităţi din câmpul de luptă, integrarea imaginilor operative standard (Common Operational Pictures-COP[29]), rezultând mai puţine asemenea imagini, fiecare dispunând însă de capacitatea de a asigura un număr sporit de secvenţe (vederi) operative; o asemenea secvenţă reprezintă, în mod obişnuit, un submeniu de informaţii din cadrul COP, cu detalii necesare planificării unei misiuni sau luării unei decizii. În consecinţă, considerăm că procesul COP are, în principal, rolul de a asigura consistenţă funcţională între diferite secvenţe operaţionale.

[29] Imaginea Operaţională Comună.

Reţeaua de execuţie este compusă, la rândul ei, din platformele de lovire, adică elemente întrunite, flexibile, interoperabile, capabile să aplice simultan şi, dacă este posibil, instantaneu, efectele, să prevină fratricidul şi să evite surprinderea. Crearea unei arhitecturi organizaţionale care să permită conectarea unor microstructuri luptătoare, de tipul forţelor speciale, dotate cu mijloace minime necesare îndeplinirii misiunilor, este un alt factor de multiplicare a puterii, întrucât aceştia, pe de o parte, pot beneficia de o cantitate enormă de informaţii utile şi oportune prin poziţionarea lor ca şi client în reţea, prin simpla conectare a unui laptop la staţia prin satelit şi accesarea Intranetului militar, şi pot genera, la rândul lor, informaţii, introducându-le instantaneu, în format digital, în aceeaşi reţea iar, pe de altă parte, pot acţiona numai ca element al subsistemului de execuţie, prin scoaterea din luptă a obiectivului primit.

Conceptul nu este însă infailibil sau lipsit de probleme! Spre exemplificare, problema tehnică cea mai importantă este lărgimea de bandă, care determină cât de multe date pot fi transferate rapid între două dispozitive electronice. Un studiu al firmei Rand Corporation estimează că, în domeniul militar, este nevoie de o bandă de 40-50 de ori mai mare decât cea folosită acum doi ani în ultimul război din Irak, adică o bandă care să permită, în termenii unui hacker, încărcarea a trei filme de 1.000 MB fiecare pe secundă! Într-un raport de tipul „lecţii învăţate în Irak", publicat în mai 2004 de Forţele Terestre ale SUA, se afirma că „nu vor exista probabil niciodată resurse suficiente pentru a realiza o reţea de comunicaţii completă şi funcţională, şi dislocarea de senzori şi sisteme de lovire oriunde în lume[30]".

În ultimul conflict din Irak s-au „jucat" noile concepte, mai mult sau mai puţin folosite şi experimentate, precum

[30] Pentru mai multe detalii, a se vedea *Pentagon Envisioning a Costly Internet for War*, The New York Times, 13 nov. 2004.

operația „Șoc și groază”, operația informațională, operația bazată pe efecte, războiul de manevră, războiul contra insurgenților, războiul expediționar etc. Totuși, putem trage câteva concluzii cu privire la desfășurarea acțiunilor militare:

a. Toate operațiile au avut caracter întrunit și combinat – evidențiate de folosirea tuturor categoriilor de forțe ale SUA și aliaților, cu o creștere semnificativă a celor speciale, cu o integrare de succes a forțelor militare străine, australiene, britanice, poloneze în planul de operații – urmată de integrarea a peste 27 de națiuni, inclusiv România, în operațiile militare postconflict.

b. Cooperarea dintre Forțele de Operații Speciale și forțele principale, la un grad nemaiîntâlnit, ilustrată de acțiuni neconvenționale, de tipul celor de căutare a conducătorilor Partidului Baas, un exemplu fiind cele de pe autostrada Bagdad–Tikrit, unde elemente ale unității Delta Force au primit în întărire un pluton de tancuri M-1, pentru a asigura protecția acestora la atacurile cu armament ușor și mijloace explozive improvizate.

c. Capacitatea de prelucrare și exploatare a unei cantități masive de informații[31], specifică RBR, executarea atacurilor cu sisteme de armament de mare precizie, a manevrelor rapide și aplicarea tehnicilor de luptă adecvate situației tactice au permis un efect sinergic, forțele americane reușind să obțină rezultate mai bune decât cele preconizate.

d. S-a pus în aplicare o puternică componentă informațională și psihologică, încercându-se folosirea mass-

[31] Pentru a procura și introduce în rețea informațiile necesare hotărârilor din teatrul de operații s-au folosit peste 40 de sateliți de observare și dirijare, sisteme de cercetare de tipul AWACS, JSTARS sau AEW&C, avioane fără pilot și mijloace electronice și optice din dotarea trupelor terestre sau forțelor speciale. Considerăm, totuși, că americanii au avut la dispoziție 12 ani pentru a identifica și localiza toate aceste obiective, lucru nemaiîntâlnit în istorie.

media ca vector al „încărcării” psihologice a forțelor proprii, menținerii sprijinului popular și a suportului internațional. Aici trebuie să scoatem în evidență că apariția unor noi jucători în plan mediatic, precum *Euronews* sau *Al-Jazeera* a făcut mult mai dificilă această întreprindere.

Ca parte componentă a conceptului „Șoc și groază”, care se dorea un concept cu efecte inclusiv psihologice, însă datorită mediatizării excesive înainte de declanșare și a imposibilității prezentării mediatice a efectelor, a căzut în desuetudine, folosirea armamentului cu mare precizie de lovire a fost generalizată. Dacă în primul Război din Golf numai 7% din armele folosite au fost de mare precizie, în prima săptămână a conflictului din Irak, procentajul loviturilor unde s-au folosit arme de precizie s-a ridicat la 95%.

3. Adoptarea RBR în NATO și UE

Și în cadrul procesului de transformare generală a NATO, efectele semnificative ale globalizării, apărute în mediile social, politic și de securitate ale Alianței, constituie provocări curente ale capacității de răspuns la amenințările și evenimentele în derulare.

Conform experților, teoria referitoare la potențialul „rețelei” este considerată esențială și în proiectele de transformare a Alianței.

Este preluată în strategia de dezvoltare și integrare a capacităților, sub denumirea „Capacități NATO facilitate de rețea” (NATO Network Enabled Capability - NNEC), pe baza principiilor definite în cadrul teoriei „operațiilor bazate pe efecte”. Conceptul promovat de Alianță identifică soluția integrării instrumentelor militare și politice, adoptarea unor noi metode și structuri organizaționale capabile să asigure rezultate rapide, decisive, la nivel operativ și strategic, în afara zonelor tradiționale de responsabilitate acoperite de Tratatul de la Washington.

În cadrul NATO, Comandamentul Aliat pentru Transformare (Allied Command Transformation – ACT) este structura responsabilă cu planificarea şi derularea acestui proces, care asigură finanţarea eforturilor de cercetare, dezvoltare de concept, experimentare şi implementare.

În viziunea comună a celor doi comandanţi strategici ai NATO (documentul intitulat "The Military Challenge") se estimează că viitoarele operaţii ale Alianţei vor avea caracter preponderent expediţionar, se vor angaja toate dimensiunile spaţiului de luptă, cu orientare clară spre efecte.

În plan militar, accesul tuturor aliaţilor prezenţi în respectiva operaţie la reţele asigură rolul de multiplicator al forţei, determinând reducerea costurilor individuale şi a celor comune ale Alianţei.

Pe plan strict economic, pe de o parte, nici o ţară din NATO sau din afara Alianţei nu este şi nu va fi aptă de a-şi dezvolta şi produce independent tehnologiile şi sistemele de arme necesare pentru a duce un RBR. În războiul de coaliţie, aceasta va pune probleme acute de compatibilitate, care vor trebui să fie depăşite, prin eforturi bugetare naţionale considerabile.

Pe de altă parte, competiţia producătorilor de echipamente militare este mai acerbă ca niciodată. În opinia noastră, unica soluţie de a ajunge la un nivel de interoperabilitate în cadrul RBR rămâne cooperarea militară şi industrială, tehnică şi tehnologică euro-atlantică.

Pentru implementarea unitară a conceptului, la nivelul Alianţei, s-au identificat câteva principii de funcţionare:

- interconectarea multiplă a componentelor forţei determină perfecţionarea schimbului de informaţii;
- schimbul de informaţii şi colaborarea determină perfecţionarea calitativă a informaţiilor şi a distribuţiei acestora;

- distribuţia facilitează colaborarea şi determină creşterea vitezei de decizie şi pe cale de consecinţă, creşterea rolului de multiplicator al forţei;
- dobândirea superiorităţii informaţionale se realizează prin capacităţi care să permită „vizualizarea" cu întâietate a potenţialului inamic;
- realizarea superiorităţii în procesul de cunoaştere a inamicului impune înţelegerea rapidă a intenţiilor acestuia şi urmărirea permanentă a situaţiei;
- realizarea superiorităţii decizionale impune atât un cadru legislativ şi regulamentar, cât şi proceduri clare, folosirea tehnologiei VTC şi a principiului enunţării clare a stării de finalitate[32] şi a intenţiei comandantului[33];
- realizarea superiorităţii acţionale, prin aplicarea principiilor operaţiilor bazate pe efecte şi al acţiunii decisive, pentru obţinerea unor efecte superioare;
- crearea capacităţilor de simulare şi distribuţia acestora la distanţă, cu rezultate spectaculoase în domeniul interoperabilităţii şi uniformizării instruirii.

Îndeplinirea acestor obiective se realizează prin asigurarea superiorităţii informaţionale, angajamentului eficient şi decisiv, din primele momente ale stabilirii contactului, executarea manevrei întrunite, perfecţionarea cooperării civili-

[32] Starea de finalitate reprezintă acea stare/statut în care trebuie să se regăsească forţa la sfârşitul campaniei, necesară pentru terminarea conflictului sau pentru rezolvarea acestuia în termeni cel puţin favorabili. Este primul element de bază, ajutător, al planificării, de la care trebuie să se plece, şi nu trebuie confundat cu obiectivele politico-militare pe care trebuie să le îndeplinească forţa pe timpul campaniei.

[33] Intenţia comandantului este viziunea personală a acestuia referitoare la motivele pentru care se desfăşoară operaţia şi ce anume trebuie realizat. Intenţia este o declaraţie clară, concisă, a obiectivului general al misiunii, a rezultatului final şi a tuturor informaţiilor esenţiale despre cum să se atingă scopul final şi trebuie să fie bine înţeleasă de comandanţii din subordine, pentru ca aceştia să-şi pregătească propriile ordine.

militari, a desfăşurării operaţiilor cu caracter expediţionar şi logistice întrunite, în cadrul cărora capacităţile facilitate de reţea reprezintă principiul-cheie. Desigur, există şi probleme, obstacole şi provocări, nu numai în domeniul tehnic şi tehnologic, ci şi în cel informaţional şi uman, în mod deosebit legate de implementarea conceptului şi accesul la tehnologie, pentru că o parte din naţiunile membre, din cele care dispun de tehnologie modernă, încă au o politică naţională restrictivă.

Un alt aspect destul de delicat este generat de evaluarea costurilor şi a necesarului de investiţii impuse de aceste programe de cercetare, dezvoltare şi implementare.

Concepţia ACT, care consideră că la acest proces trebuie să participe toate statele – mari sau mici –, asigurând angajarea tuturor capacităţilor industriale existente şi chiar dezvoltând noi oportunităţi, se opune tendinţelor protecţioniste ale statelor membre.

O altă idee valoroasă a Alianţei este aceea de a folosi Forţa de Răspuns (NATO Response Force - NRF), în rol de laborator de experimentare, evaluare, valorificare şi drept catalizator al implementării principiilor NNEC în sistemele militare ale statelor membre. Deşi Forţa de Răspuns NATO este concepută pentru toată gama de operaţii, ea a fost prevăzută în special pentru conflictele de mare intensitate, având ca misiuni:

- managementul consecinţelor unor atacuri teroriste (inclusiv cu NBC);
- impunerea păcii (inclusiv gestionarea migraţiei în masă);
- embargoul şi interdicţiile;
- intervenţii antiteroriste şi mai ales riposte contrateroriste;
- operaţiunile de evacuare a noncombatanţilor;
- apărarea antirachetă.

Deşi cele prezente aici par să ţină mai mult de domeniul viitorului, integrarea cât mai rapidă a unor concepte sau proiecte doctrinare, organizaţionale şi de planificare în cadrul

Alianţei se află în faze avansate de experimentare şi implementare.

Acest lucru se poate exemplifica prin unele proiecte aflate în derulare, cum ar fi sistemele pentru monitorizarea poziţiei forţelor proprii, până la nivel vehicul, distribuţia imaginii operaţionale comune compozite, mijloacele de identificare şi navigaţie, senzorii (pentru sprijinul deciziei sau managementul spaţiului de luptă), precum si armonizarea unor programe gen evidenţa computerizată a mijloacelor logistice.

Implementarea diferitelor programe NNEC impune coordonarea lor riguroasă, stabilirea clară a orientărilor strategice şi a autorităţii de execuţie, un program concret de educare şi instruire, precum şi o foaie de parcurs clară, pentru adoptarea graduală a conceptelor.

Putem concluziona că NNEC nu se referă numai la tehnologie, ci reprezintă o nouă filozofie, un nou mod de gândire şi acţiune şi chiar o modalitate politică de a împinge de la spate unele state mai puţin dispuse la cheltuieli militare suplimentare.

În cadrul programului de dezvoltare a viitoarelor sisteme de luptă[34], evitarea fratricidului este considerată un obiectiv esenţial. De fapt, la nivelul NATO, s-a decis uniformizarea cerinţelor tehnologice ale unui asemenea sistem de identificare în luptă. Astfel, a apărut STANAG 4579, care reglementează cerinţele şi parametrii dispozitivelor de identificare a ţintelor în luptă.

Unele state au combinat mai multe sisteme, ajungând astfel la sistemul MFRF (Multi-Function Radio Frequency - frecvenţă radio multifuncţională), care are funcţiuni de comunicare, radar şi identificare.

[34] Future Combat System (FCS), sistem de management tehnologic şi integrare în reţelele mari militare a tuturor sistemelor independente achiziţionate de Forţele Terestre ale SUA.

Alte țări planifică să adopte soluția ANSER (Air and Surface Electronic Responder), ce va permite vehiculelor pe care este instalat să asigure şi capacități de comunicare şi transfer de date, integral digitale, aşa cum este specificat în STANAG 4579.

În cadrul programului condus de SUA, pentru acțiunile postconflict din Irak, Coalition Combat Identification[35], s-a reuşit interconectarea în rețea a acestor sisteme. Astfel, state precum Marea Britanie, Franța sau Italia au reuşit, folosind propriile echipamente, să interacționeze cu alte sisteme.

Digitalizarea şi racordarea la rețea sunt prezente în cadrul categoriilor de forțe, pentru cât mai multe elemente sau segmente ale acțiunilor militare. Pentru misiunile de căutare-salvare a piloților doborâți de inamic, forțele SUA sunt în faza de studiu, achiziție şi implementare a unui nou sistem de stații radio portative, estimându-se achiziționarea a peste 46.000 de bucăți. Sistemul, denumit Combat Survivor Evader Locater (CSEL)[36], foloseşte rețelele de sateliți existente, inclusiv rețeaua GPS, şi va furniza permanent informații criptate despre poziția acestor piloți în teren, eliminând practic faza de căutare din cadrul misiunii.

În Programul de apărare împotriva terorismului, una din provocările Directorilor Naționali de Armament (CNAD) este găsirea soluțiilor pentru apărarea aeronavelor NATO împotriva sistemelor portabile de apărare antiaeriană şi a aruncătoarelor de grenade reactive.

Deoarece primele pot fi uşor contracarate (prin folosirea de contramăsuri electronice, ținte false, flăcări, poliedre etc.), în

[35] Coalition Combat Identification (CCCID), sistemul de identificare în luptă al forțelor de coaliție, creat spre a permite integrarea tehnologică a mai multor sisteme de identificare amic-inamic naționale.

[36] Combat Survivor Evader Locater (CSEL), sistem de localizare a supraviețuitorilor pe câmpul de luptă, conform DefenseNews, 4 apr. 2005, p. 18.

cadrul acestui subgrup de lucru, statele membre şi partenerii se concentrează asupra celui de-al doilea proiect. Pentru protecția împotriva AG-urilor se vor putea folosi ultrasunete sau alt gen de unde radio (care pot duce la explozia focoaselor la distanță suficient de mare pentru a proteja fuselajele), sau blindaje de 4-5 ori mai eficiente decât cele existente.

Alte subgrupuri de lucru în domeniul combaterii terorismului sunt cele care lucrează la proiecte precum:

- Protejarea porturilor şi navelor de suprafață împotriva atacurilor teroriste;
- Adoptarea unor măsuri pe termen scurt pentru îmbunătățirea şi protejarea capacităților de comunicații ale NATO în caz de atac terorist;
- Folosirea mijloacelor de detectare ale NATO (AWACS);
- Coordonarea programelor de instrucție şi educație în domeniul combaterii terorismului (COE-DAT, protecția forțelor, evaluare etc.), distribuirea acestora şi a simulărilor la distanță, folosind rețelele existente;
- Detectarea şi contracararea mijloacelor explozive improvizate;
- Creşterea rolului Forțelor Speciale în combaterea terorismului (subprogram pentru mărirea preciziei paraşutărilor);
- Detectarea, protejarea şi managementul consecințelor în urma unor atacuri teroriste cu arme nucleare, biologice, chimice şi radiologice;
- Tehnică de apărare împotriva loviturilor de aruncător.

În combaterea terorismului, schimbul de informații secrete rămâne veriga slabă, aşa cum demonstrează puținul interes care a fost acordat de statele membre ale **UE** structurilor antiteroriste, create în noiembrie 2001, ce nu s-au reunit practic, niciodată, de atunci. Singurul consens asupra acestui aspect a fost un acord de principiu privind crearea unei celule de schimb

şi de transmitere de informaţii între serviciile specializate ale statelor membre, în care diferitele servicii, cum ar fi poliţia, justiţia, serviciile secrete, ar putea să-şi compare datele de care dispun şi să transmită o listă de riscuri şi ameninţări comunităţii europene.

4. Aplicarea conceptului RBR în Operaţii Speciale

Îndeosebi în domeniul Operaţiilor Speciale se identifică o glisare spre tehnologie a instrumentelor războiului: armele sunt transformate în sisteme şi conexiuni de date mobile. „Precizia" ia locul puterii de foc şi acţiunile-şoc, rapide, în grupuri mici, iau locul distrugerilor masive. Iar aici este implicată decisiv tehnologia înaltă a obţinerii şi diseminării informaţiilor. Sistemul de Poziţionare Globală (GPS), sistemele de tipul JSARS[37], AWACS[38] sau ultramodernul AEW&C[39], asigură comandanţilor şi forţelor pentru Operaţii Speciale o capacitate excepţională de a culege, analiza, disemina informaţii şi acţiona asupra spaţiului de luptă.

În cele mai recente confruntări armate ale ultimului deceniu, avem o demonstraţie pertinentă că noua paradigmă a războiului combină integrarea „sistemelor spaţiale şi aeriene moderne, marea precizie distructivă a armelor convenţionale avansate şi viteza comunicaţiilor moderne într-o maşină de

[37] Joint Surveillance and Target Attack Radar System, sistem întrunit de supraveghere şi dirijare prin radar, dispus pe o platformă aeriană şi destinat detectării şi distrugerii obiectivelor inamicului de la sol.

[38] Airborne Warning And Contol Systems, sistem similar celui anterior, dar destinat supravegherii şi conducerii operaţiilor întrunite aeriene.

[39] Airborne Early Warning and Control, cel mai dezvoltat sistem de management al luptei, are capacitatea de a urmări simultan atât ţinte aeriene, cât şi terestre. De asemenea, asigură imaginea integrată a spaţiului de luptă, fiind considerat un nod de reţea în integrarea acestuia, conform Defense News, 7 februarie 2005.

război aptă să înfrângă rapid orice forţă lipsită de tehnologii moderne"[40].

Rolul jucat de forţele pentru Operaţii Speciale, atât în Afghanistan, cât şi în Irak, nu este încă cunoscut îndeajuns, din cauza restricţiilor de acces la informaţie. Din datele cunoscute, acestea au îndeplinit misiuni diversificate, dintre care se detaşează localizarea, indicarea (iluminarea laser sau localizarea precisă) obiectivelor în mişcare şi comunicarea coordonatelor bombardierelor strategice. Acest lucru a fost posibil nu numai datorită unei aparaturi extrem de performante cu care aceste grupuri au fost dotate, ci şi unei noi proceduri militare, denumită scotocire (*swarming*)[41], care se bazează pe cele trei tendinţe majore care au evoluat în ultimii 70 de ani: capacitatea crescândă de distrugere pe care o au grupurile mici, precizia tot mai mare a armamentului cu care acestea sunt dotate şi integrarea acestora prin reţelele de comunicaţii.

Campania din Afghanistan a marcat utilizarea extensivă a forţelor pentru Operaţii Speciale în sprijinirea acţiunilor forţelor aeriene, prin legătura directă a acestora cu avioanele de luptă. Eficacitatea loviturilor aeriene a sporit considerabil odată cu infiltrarea la sol a grupurilor din cadrul forţelor pentru Operaţii Speciale şi serviciilor secrete, care au asigurat date despre ţinte, în timp real, prin utilizarea indicatorilor cu laser sau prin transmiterea directă, la bordul avioanelor de luptă, a datelor obţinute, utilizând canale securizate radio, receptoare GPS şi transmiţătoare radio conectate la laptopuri, pentru codificare electronică şi criptografică.

Într-un alt scenariu ipotetic, ciclul descoperirii şi distrugerii unei ţinte poate fi următorul:

[40] M. KLARE, **Rogue States and the Nuclear Outlaws: America's Search for a New Foreign Policy**, New York, Hill and Hang Publishers, 1995, p. 95, citat de Th. BALZACQ, op. **cit.**, p. 4.

[41] John ARQUILLA, David RONFELDT, **Networks and Netwar**, RAND, Los Angeles, 2001.

- un satelit de cercetare detectează o emisie electro-magnetică de interes;

- prin intermediul unui satelit de comunicații, informația este transmisă la Centrul de Operațiuni Aeriene Multinaționale – CAOC – unde, automat, în Lista Mijloacelor Aeriene în zbor, sunt identificate şi alte platforme de senzori care pot investiga şi localiza cu precizie emisia respectivă, cum ar fi sistemele de avioane fără pilot (UAV);

- cu ajutorul senzorilor de la bord, UAV-ul confirmă poziția şi parametrii țintei şi, prin datalink[42], transmite informația la CAOC;

- la rândul său, un avion de cercetare Astor, care are capacitatea de a îmbunătăți precizia determinării poziției țintei, stabileşte dacă ținta detectată este mobilă sau nu;

- în cazul în care este mobilă, vor fi determinate viteza şi itinerarul său;

- întregul proces este monitorizat cu ajutorul datelor si informațiilor prezentate pe displayurile panoului de date din CAOC;

- ținta este evaluată, pentru a se stabili dacă este importantă şi dacă trebuie distrusă imediat;

- pe baza Listei Mijloacelor Aeriene în zbor sunt identificate avioanele disponibile în raionul respectiv, cu muniția adecvată, care pot fi angajate în acest scop;

- prin intermediul Sistemului Comun de Distribuție a Informațiilor Tactice, avioanele disponibile primesc toate datele necesare referitoare la țintă;

- printr-un subsistem datalink, avioanele comunică dacă ținta a fost distrusă;

[42] Expresie care reprezintă tipul de conexiune pentru transmiterea de date. Cifra de la sfârşit arată capacitatea conexiunii. De notat că cele mai moderne, în literatura de specialitate, sunt de nivel 26-28, permițând transferul de imagini digitale de mare rezoluție.

- în scopul evaluării distrugerilor produse asupra țintei, CAOC dispune trimiterea în zonă a unui alt UAV, de tip Predator, care, cu ajutorul senzorilor săi electrono-optici, poate furniza informațiile solicitate (BDA);

- Predator examinează raionul țintei şi, prin datalink, transmite imagini la CAOC, confirmându-se, astfel, distrugerea țintei.

Trebuie menționat aici că forțele pentru Operații Speciale bine instruite, sau chiar structurile insurgente sau teroriste, au nevoie de puține comunicații în timp real, deoarece, de obicei, după declanşarea misiunii, descentralizează controlul operațiunii. Teroriştii de la 11 septembrie 2001 au comunicat foarte puțin, dar au fost „superiori" în acea zi.

Sistemul şi elementele componente ale RBR nu sunt infailibile, întrucât lasă loc apariției erorilor, de cele mai multe ori umane. Astfel, în această campanie au fost mai multe cazuri de fratricid, printre care lovirea din aer a unei maşini a televiziunii ITN, aflată într-o coloană a forțelor speciale americane, sau bombardarea propriilor poziții.

Specialiştii consideră că, pe plan național, pe termen scurt şi mediu, România nu este amenințată de o agresiune armată directă împotriva teritoriului ei şi nu consideră nici un stat ca potențial inamic. Riscurile la adresa securității naționale sunt şi vor fi în principal de natură nemilitară şi neconvențională, folosirea mijloacelor militare rămânând o opțiune politică de ultimă instanță[43].

O altă opțiune, pusă la dispoziția factorului politic de armatele moderne, o constituie forțele pentru Operații Speciale. Considerăm că şi în România această ultimă opțiune trebuie bine analizată, argumentată şi cuprinsă, pe de o parte, într-o viitoare doctrină a operațiilor speciale, care să fie avizată de

[43] STANCIU, I. Aurel, **Terorismul internațional. Implicații strategice asupra securității statului**, Teză doctorat, Editura UNAP, 2005, pp. 201-202.

conducerea politică a țării, iar pe de altă parte, într-o viitoare inițiativă legislativă pe aceeaşi temă, la care se lucrează în prezent.

Fiecare militar din forțele pentru Operații Speciale este înzestrat cu o unitate IT portabilă care încorporează un calculator cu monitor rabatabil la casca de luptă, iar hărțile digitalizate de care are nevoie sunt încărcate în memorie, cu un sistem GPS, de poziționare prin satelit, şi o stație radio individuală. Putem emite ideea că soldatul este pe cale să devină un sistem, parte integrantă a altui sistem. Uniforma, propusă şi în cadrul proiectului SIPE - Soldier Integrated Protective Enable - sistem integrat de protecție al soldatului, are dublu rol. Pe de o parte, rolul de protecție şi de minimizare a posibilelor răniri pe câmpul de luptă, prin vestă antiglonț, cască, protecție crescută a costumului la armele NBC, sistem individual de încălzire etc.

Pe de altă parte, se urmăreşte creşterea eficienței în luptă, prin montarea mijloacelor de comunicație de tipul "handsfree", care să permită folosirea armamentului cu ambele mâini, în acelaşi timp cu convorbirile radio, operarea aparaturii de navigație şi de vedere pe timp de noapte, sistemul GPS de localizare, dar şi de semnalare a poziției.

Această dotare standard permite integrarea respectivului soldat în sistemul de recunoaştere amic – inamic, pentru a se evita astfel fratricidul.

În cadrul acestui proiect de echipament şi armament individual se generalizează calibrele mici, mijloacele miniaturizate, polivalența acțională a armamentului portativ (capabilități antipersonal, antiblindate, de operare în zone puternic urbanizate şi pe timp de noapte) cu sistem de ochire şi de ghidaj laser. Există chiar şi preocupări pentru crearea unui costum care să amplifice de câteva ori forța celui ce îl poartă.

În armata SUA, s-au elaborat cerințele pentru realizarea noului sistem al luptătorului, Land Warrior System. Acestea au fost:

Efect distructiv, de unde a rezultat necesitatea realizării unei game de armament cu sisteme avansate de control asupra focului, optimizate pentru lupta în mediu urban.

Posibilitate mărită de supraviețuire, respectiv, necesitatea creării unei ținute de protecție ultrauşoare, nevoluminoase, împotriva întregului spectru de amenințări.

C4I2SR (comunicații şi senzori), de unde a rezultat necesitatea interconectării în rețele a indivizilor şi echipelor/grupelor prin mijloace de comunicații, senzori de ultimă generație, sisteme tactice de culegere de informații aflate în organică, asigurând posibilitatea de planificare şi antrenare din mers, precum şi legăturile cu mijloacele altor categorii de forțe.

Surse de alimentare, adică sisteme sau elemente care să asigure o autonomie de 72 de ore, cu volum şi greutate mici, posibilități de autoîncărcare sau reîncărcare, solide şi sigure.

Mobilitate, performanțe umane superioare, respectiv, posibilitatea de deplasare pe timpul misiunii cu încărcătură la greutate maximă, pe verticală şi orizontală.

Concluzionând, sistemul integrat al luptătorului, o combinație de senzori, computer, lasere, sistem de locație terestră şi stație radio, aduce luptătorul în spațiul de luptă digital şi îi creşte capacitatea de cunoaştere a situației, permite înregistrarea şi transmiterea de imagini video, pe de o parte, şi conducerea efectivă a luptătorilor, pe de altă parte.

Costurile deosebite ale dotării unei asemenea unități, îndeosebi pentru crearea capacităților de acces la rețele, extrem de costisitoare pentru un buget limitat, şi-au pus deja amprenta asupra repartizării resurselor financiare în anul 2004.

În privința deciziilor dificile, impuse de continuarea reformei domeniului militar şi de necesitatea reducerii mai multor structuri militare, acestea au fost luate uneori fără a se

ține seama de nevoile şi fizionomia conflictelor militare ale următorului deceniu. Astfel, deşi opinii privind „creşterea rolului trupelor de desant aerian, aeromobile, de cercetare-diversiune şi al forțelor speciale" au fost exprimate în repetate rânduri, chiar şi în lucrări de specialitate de referință[44], când a fost vorba de transpunerea în practică a acestora s-au preferat alte soluții, „mai convenabile social", deşi, din punct de vedere financiar, costurile ar fi fost mai reduse, comparate cu capacitatea de reacție şi caracterul preponderent expediționar al celor dintâi, şi ne referim aici la cele câteva unități de operații speciale care existau deja.

5. Aplicarea conceptului RBR în combaterea terorismului

A devenit tot mai evident că, într-o eră în care forțe transnaționale şi substatale, bazându-se pe tehnologii şi echipamente comerciale sau obținute prin manufactură proprie, au căpătat aplomb şi au reuşit să depăşească granițele naționale, concepte precum războiul civil, terorismul şi proliferarea armelor de distrugere în masă nu mai pot fi limitate sau izolate în cadrul anumitor state sau regiuni.

Încă de la începutul anilor '90, aceste fenomene au izbucnit ca amenințări majore la securitatea globală, tocmai pentru că diminuează distincția făcută între crize interne şi externe. În aceste noi condiții, forțele transnaționale şi substatale amenință nu doar statele, ci chiar societatea democratică în ansamblul ei şi, prin aceasta, stabilitatea internațională în sine. În consecință, ideile tradiționale despre arta războiului sunt evitate, pe măsură ce dimensiunile politice, economice şi militare ale securității aproape au fuzionat, iar războiul dintre un stat şi un altul pare să fi fost înlocuit de noile

[44] BĂDĂLAN Eugen, Gl. div. dr., **Securitatea națională şi unele structuri militare româneşti la cumpăna dintre milenii**, Editura Militară, Bucureşti, p. 162.

forme de conflict substatal şi transstatal, mai convenabile din punct de vedere economic, politic şi militar.

Tendințele pe plan internațional

Pe plan internațional apar mutații considerabile în modul de abordare a operațiilor după aplicarea principiilor RBR. În Afghanistan se vorbeşte deja despre schimbarea caracterului operației, de la o operație antiteroristă cu forțe speciale dislocate pe sectoare la o operație bazată pe informații[45], unde sistemele şi procedeele de culegere a datelor şi informațiilor despre structurile teroriste şi operația informațională antiteroristă să constituie centrul de greutate.

Experiența unor state precum SUA, Marea Britanie, Germania sau Israel, în folosirea RBR pentru combaterea terorismului, este benefică şi trebuie luată în considerare. De asemenea, adoptarea la nivel NATO a unui concept de acțiune preventivă, pentru misiuni de combatere a terorismului şi unde vârful de lance îl constituie NRF, structură exponentă a conceptului RBR, trebuie analizată şi transpusă la nivel național, înainte de a da forțe în compunerea NRF.

În combaterea terorismului, elemente ale RBR se aplică de ceva vreme. Un exemplu sugestiv de folosire a principiilor şi tehnologiilor caracteristice RBR este cel al **specialiştilor britanici** ai unității C-7 din MI5, care, după declanşarea crizei teroriste din 30 aprilie 1980 (!), de la ambasada Iranului din Londra, au trecut la plantarea de microfoane, senzori de proximitate şi altă aparatură sofisticată, pe care le-au integrat într-o rețea ce le permitea acestora să ştie poziția exactă a teroriştilor, că „în camera telexului sunt strânşi majoritatea ostatecilor", dar dovedindu-se „eronate în privința unor camere de la etaj"[46].

[45] Intelligence Based Operations.
[46] Idem, p. 181

Israelul recurge frecvent la raiduri aeriene, bombardamente de artilerie, inclusiv comandouri de pedepsire, pentru lichidarea teroriştilor arabi, chiar retraşi în sanctuarele din Africa, Europa sau SUA[47], comandouri pregătite după „rețeta" de represalii a lui Golda Meir, şi anume, că nici un civil nu trebuie ucis, ci doar teroriştii, că aceştia trebuie să fie ucişi în acelaşi fel cum au murit victimele lor şi că, înainte de a muri, trebuie să ştie cine i-a răpus, iar că, în cazul acțiunilor „negre", în teritoriu ostil, cineva trebuie să şteargă urmele şi să inducă în eroare investigația organelor locale de anchetă. Trebuie să amintim aici şi de raidurile de tip ofensiv, de valoare tactică, dar cu impact strategic, sub acoperire sau desfăşurate în cadrul unei operații militare, o adevărată procedură contrateroristă pentru forțele speciale israeliene, aprobată şi susținută procedural de conducerea politico-militară a acestei țări.

O oficialitate din cadrul Forțelor de Apărare Israeliene (FAI) a afirmat, în luna noiembrie 2004, că o combinare a tehnologiei moderne cu concepte operaționale de acțiuni în rețea şi coordonarea între structurile de informații, inclusiv a celor din afara FAI, permit forțelor aeriene să preia o parte a sarcinilor îndeplinite în mod tradițional de forțele terestre. Acuratețea îmbunătățită şi coeficientul de siguranță al loviturilor aeriene de anihilare – pe care preferă să le numească operațiuni de lovire precisă – se datorează existenței unui concept operațional prin care se îmbină informațiile precise cu comanda, controlul şi tehnologia mult îmbunătățită. Acesta consideră că forțele aeriene pot preveni infiltrările, impune interdicții de circulație după lăsarea întunericului, pot fi folosite pentru lichidarea celulelor teroriste şi pot distruge depozitele ilegale de armament, reducând foarte mult necesitatea implicării forțelor terestre.

[47] ARĂDĂVOAICE G., ILIESCU D., NIȚĂ L.D., în **Terorism, antiterorism, contraterorism**, Editura ANTET, p. 143

Rezultatele obținute de FAI în loviturile date palestinienilor suspectați de terorism sunt relevante. În ultimele 6 luni ale anului 2004, între 60 şi 80% dintre combatanții palestinieni, ținte ale serviciului de securitate SHIN BET şi ale serviciului de informații al armatei, au fost ucişi în urma loviturilor aeriene, aproape 90% dintre aceştia în Fâşia Gaza.

„Acum 2 ani, când am început (utilizarea pe scară largă) a operațiunilor de lovire precisă, doar 15-20% dintre ținte erau lovite cu ajutorul forțelor aeriene şi chiar cu 6-8 luni în urmă, doar 30-35% dintre ele erau urmare a acestui gen de operații", a afirmat acelaşi oficial. „Ce am reuşit să realizăm în ultima jumătate de an este nemaipomenit. Am creat o situație în care realitatea este foarte aproape de imaginație"[48].

Oficialul a declarat că, în ultima perioadă, în cadrul FAI, s-a constituit o celulă specială de comandă şi control formată din 5 sau 6 ofițeri. Aceştia sunt singurii autorizați de comandamentul FAI să se ocupe de operațiunile de anihilare a țintelor teroriste. Acesta a mai afirmat că, în dezvoltarea conceptelor şi aplicațiilor RBR, o mare influență a avut-o industria locală de apărare şi laboratoarele ce lucrează în domeniul dezvoltării tehnologice, care au îmbunătățit sistemele existente şi au mărit precizia armamentului, urmărind şi costurile rezonabile. Un exemplu în acest sens îl constituie dispunerea senzorilor similari cu cei ai AWACS pe console purtate de un dirijabil, dar cu absolut aceleaşi rezultate.

Oficialul din cadrul FAI a declarat că, din momentul folosirii noilor tactici antiteroriste în 2003, numărul victimelor nevinovate a scăzut dramatic. „Anul acesta, la 12 terorişti s-a înregistrat aproximativ o singură victimă colaterală, pe când în trecut raportul era de aproximativ 1 la 1 şi continuăm să acționăm în acest sens, deoarece chiar şi o singură victimă înseamnă mult, şi situația trebuie evitată".

[48] Defense News, 7 martie 2005, pp. 1-8.

În domeniul diversificării şi integrării reţelelor de senzori, în cadrul conceptului RBR, Israelul este una din cele mai avansate naţiuni. Pentru exemplificare, proiectul FIREFLY, realizat pentru lansatorul standard de grenade M203 40 mm (montat pe puşca de asalt M16), este bazat pe conceptul de proiectil dual şi a constat în montarea unor senzori, mai precis a două camere de luat vederi de tip CCD (charge-coupled device), pe un proiectil exploziv, cu muniţie subcalibru şi bătaia de 600 m, acesta devenind astfel şi o sursă de informaţii (image-gathering round).

Pe timpul celor opt secunde pe care le face până la ţintă, FIREFLY poate transmite imagini color şi de înaltă rezoluţie.

Destinate trupelor de uscat şi forţelor speciale, imaginile sunt transmise în timp real, fiind recepţionate pe echipamente speciale (personal digital assistance) sau pe calculatoare portabile (pocket PC), prevăzute cu bloc de recepţie şi antenă. Servind şi ca relee, acestea retransmit apoi imaginile în interiorul reţelei, putând fi astfel accesate de oricare utilizator din zonă.

Însăşi structura RBR poate constitui ţinta unor atacuri, de cele mai multe ori teroriste. Strategi militari chinezi au scris că atacul asupra comunicaţiilor spaţiale şi reţelelor de calculatoare, incluzând infrastructura civilă, poate fi o parte a unei strategii de atac de succes[49].

În SUA, oponenţii conceptului RBR au remarcat limitările capabilităţilor proprii şi capacitatea reţelelor teroriste de a lovi puterea militară americană în aceste puncte sensibile.

În 1999, Departamentul Apărării al SUA a raportat 22144 de atacuri asupra sistemelor sale nesecrete şi cu peste 10% mai mult în anul următor[50]. Michael Vatis, fostul şef al Centrului Infrastructurii Naţionale de Protecţie, a afirmat că nu

[49] Shenxia ZHENG, Changzhi ZHANG, **The Military Revolution in Air Power**, NDU Press, Washington DC, 1997, pp. 3-5.
[50] *Infowar*, în www.infoguerre.com.

se cunoaşte nici o modalitate de protecţie împotriva acestui gen de atacuri. Reţelele declarate ca „sigure" sunt, de fapt, destul de vulnerabile. Personalul NSA a identificat posibile puncte vulnerabile ale server-ului SIPRNet, care deserveşte mare parte din comunicaţiile de comandă şi control ale armatei, prin Sistemul Global de Comandă şi Control, la fel ca şi multe alte informaţii importante. Crearea reţelelor mari creşte atât vulnerabilitatea, cât şi potenţialele pagube provocate de un militar incompetent, rău intenţionat, de către un agent inamic sau un terorist.

În plus, multe aspecte ale războiului neconvenţional nu pot fi monitorizate prin senzori tradiţionali. Luptătorii din forţele neconvenţionale, de gherilă sau teroriştii, pentru a reuşi să fie invizibili pentru senzori, pot foarte uşor să se amestece printre civili şi să aibă o disciplină a comunicaţiilor, aşa cum membrii talibani au demonstrat-o în Afghanistan. Muniţiile de mare precizie nu pot lovi ţinte care nu pot fi identificate. Combinaţia dintre evitarea senzorilor şi alte contramăsuri, nu foarte scumpe, face din războiul de uzură o strategie atractivă pentru potenţialii inamici ai SUA.

6. Aplicarea conceptului în domeniul combaterii terorismului

Misiunile pe care le pot îndeplini armatele (cu structurile actuale) pot fi, în principal, cele „în forţă", menite să ducă la distrugerea unora din elementele reţelelor şi organizaţiilor teroriste, acţionând, deci asupra efectelor, şi nu asupra cauzelor. Dintre acestea amintim:

- Detectarea, prin grila senzorilor şi prin forţele pentru Operaţii Speciale, a centrelor şi bazelor de antrenament ale organizaţiilor şi reţelelor teroriste;
- Lovirea, prin mijloace militare, îndeosebi cu aviaţia, rachetele de toate tipurile şi forţele

pentru Operații Speciale, a centrelor vitale, a bazelor de antrenament, depozitelor şi infrastructurilor organizațiilor teroriste, pe măsură ce acestea sunt descoperite şi identificate şi se obține acceptul țării sau țărilor în care se află acestea, de cele mai multe ori în cooperare cu forțele armate ale țărilor respective şi/sau cu alte forțe din zonă;

- Declanşarea războiului (luptei armate) de către coaliția antiteroristă, cu sau fără mandat ONU, împotriva țărilor şi regimurilor politice care practică, adăpostesc, finanțează şi susțin acțiunile teroriste;
- Participarea la acțiunile de căutare şi distrugere a rețelelor şi bazelor teroriste;
- Interzicerea sau limitarea accesului organizațiilor teroriste la rețele[51];
- Crearea unor protocoale de detecție, a unor „capabilități ale grilei senzorilor pentru a facilita descoperirea la timp a organizațiilor şi grupurilor teroriste şi a intențiilor acestora”[52];
- Desfăşurarea unor operații speciale împotriva teroriştilor, de eliminare a acestora ca entități.

7. Preocupări pe plan intern de aplicare a principiilor RBR în combaterea terorismului

În România secolului XXI s-au făcut progrese remarcabile în domeniul informațiilor, fiind chiar recunoscuți în NATO pentru capabilitățile şi experiența pe care am acumulat-o prin

[51] VĂDUVA Gh., **Războiul bazat pe rețea în fizionomia noilor conflicte militare**, Editura UNAp, Bucureşti 2005, p. 40.
[52] Ibidem.

participarea noastră la operații. Chiar şi după integrarea în NATO, Armata României rămâne garantul suveranității şi independenței naționale, al unității şi integrității teritoriale şi va continua să contribuie activ la stabilitatea şi securitatea regională, prin participarea la materializarea inițiativelor de cooperare în domeniul militar şi prin îndeplinirea obligațiilor şi sarcinilor ce-i revin, ca urmare a aplicării tratatelor şi înțelegerilor internaționale. În scopul creşterii capacității de combatere a fenomenului terorist, în condițiile participării mai multor structuri, este considerată ca prioritară asigurarea interoperabilității conceptuale şi acționale atât pe orizontală, la nivel național, cât şi cu structuri similare externe, din țări aliate ori partenere. În noile documente programatice de securitate națională, precum Strategia de Securitate şi Carta Albă, trebuie incluse aceste elemente şi capabilități cu caracter preponderent ofensiv.

Deşi Ministerul Apărării Naționale este la început de drum în domeniul combaterii terorismului, s-au făcut progrese notabile privind instruirea şi dotarea forțelor specializate pentru asemenea misiuni. Astfel, Detaşamentul de Intervenție Rapidă şi Batalionul de Informații dețin deja armament şi tehnică de luptă compatibilă, iar Batalionul Operații Speciale, în curs de operaționalizare, negociază în prezent achiziționarea unor mijloace performante.

Considerăm că o strategie națională proactivă pentru combaterea terorismului ar presupune crearea şi dezvoltarea unor capabilități de informații în domeniul acțiunilor asimetrice, a forțelor pentru Operații Speciale, capabilități de proiecție şi sprijin a acestor forțe şi chiar capacități de asigurare logistică pe termen mediu şi lung, care să asigure sustenabilitatea în afara teritoriului național şi, nu în ultimul rând, capabilități de conectare la rețelele aliaților.

În primul rând, estre nevoie de crearea, la nivel național, a unei noi arhitecturi a sistemului C4I, care să fie suficient de

permisivă pentru schimbul de informații pe orizontală, interagenții, dar care să permită şi conectarea instantanee la rețele informatice ale NATO, UE şi țărilor aliate. La nivelul MAI există structuri specializate care au atribuții de legătură în combaterea criminalității, în care intră şi terorismul, însă accesul la aceste rețele nu este încă perfectat.

Pentru armonizarea modalităților de combatere a terorismului şi standardizarea procedurilor de operare şi management al crizelor teroriste la nivel național, s-a constituit Sistemul Național de Prevenire şi Combatere a Terorismului (SNPCT), iar Serviciul Român de Informații a fost desemnat, la data de 19 octombrie 2001, drept autoritate națională în materie. Pentru coordonarea activităților operative curente la nivel național şi conducerea reacției antiteroriste/contra-teroriste, în cadrul SNPCT funcționează Centrul de Coordonare Operativă Antiteroristă (CCOA), pentru care MApN are un element de legătură. Legătura funcționează şi constituie un început, însă suntem încă departe de aplicarea tehnologiilor şi tehnicilor specifice RBR. De asemenea, la nivelul Brigăzii Antiteroriste a SRI există capabilități RBR. Capabilitățile existente asigură pentru executanți transmiterea rapidă a ordinelor şi informațiilor în condițiile realizării libertății de mişcare gen „mâini libere".

Forțele SRI dețin mijloacele tehnice necesare realizării acestor cerințe: autostațiile care reprezintă un punct de comandă mobil, dotat cu mijloacele tehnice de comunicații şi televiziune cu circuit închis. În acest fel, factorul de decizie vede practic ceea ce vede luptătorul antitero, datorită imaginilor transmise de o cameră video miniaturizată montată la cască sau poate vedea dacă entitatea teroristă este în vizorul trăgătorului de elită, grație unei camere video montate la puşcă. Astfel, elementul de decizie este în permanență în legătură cu elementele de execuție, iar ordinele ajung la acestea în timp real.

Concluzii

Experiența recentă cu răpirea jurnaliştilor români în Irak, chiar dacă nu se cunosc detaliile din motive de păstrare a secretului, ne duce la concluzia că interoperabilitatea elementelor din cadrul SNPCT este vitală.

La nivel național este necesară armonizarea cu cadrul NATO, proces care, în opinia noastră, trebuie să înceapă cu o dezbatere lărgită a conceptului, de către toți factorii de decizie, politici şi militari, din toate structurile cu responsabilități şi contribuții la securitatea şi apărarea națională, proces menit să asigure înțelegerea şi clarificarea conceptuală, determinarea nivelului național de ambiție pe baza proiecțiilor de resurse, inventarierea proiectelor naționale care sunt compatibile conceptului şi mai ales stabilirea unui set de cerințe care să devină obligatorii pentru toate proiectele viitoare.

Un lucru putem afirma cu certitudine: Strategia de Securitate Națională şi Strategia Militară trebuie să cuprindă un set de măsuri clare de implementare a conceptului RBR, trebuie să identifice şi legifereze posibilitățile de cooperare în cadrul organismelor NATO, UE şi în alte aranjamente făcute cu țările aliate. Aceste documente programatice mai trebuie să cuprindă referiri, atribuții, responsabilități şi termene clare pentru participarea la deciziile importante ale Alianței în ce privește aplicarea principiilor şi tehnologiilor specifice RBR în revizuirea structurilor de forțe şi a celor de comandă, a planurilor de modernizare (înzestrare), a planurilor de pregătire şi a politicilor şi doctrinelor de aplicare.

Nu în ultimul rând, opinăm că toate documentele de planificare strategică a resurselor ar trebui să cuprindă un subcapitol separat, în cadrul capitolului dedicat transformării, care să abordeze problemele RBR şi de interoperabilitate cu NATO, identificând şi fondurile necesare implementării.

RĂZBOI BAZAT PE REȚEA SAU REVOLUȚIE ÎN ARTA MILITARĂ

Dr. Nicolae DOLGHIN

Într-o lume aflată în proces alert de reconfigurare şi căutări, rămâne actuală vechea constatare că militarii se pregătesc întotdeauna pentru următorul război. Este una banală care explică de ce, în succesiunea evenimentelor, războaiele diferă unul de celălalt, dar au şi multe lucruri comune. Cu cât războaiele au fost mai apropiate în timp, cu atât asemănările sunt mai evidente. Excepție fac, probabil, cele două războaie din Irak, desfăşurate cam la un deceniu unul de celălalt. Deşi la ele au participat aproximativ aceiaşi actori principali, s-au întrebuințat într-o măsură covârşitoare aceleaşi categorii de armament, războaiele au diferit total ca desfăşurare. Diferențele esențiale au fost imprimate nu atât de tehnologia înaltă şi armamentul de înaltă precizie folosite masiv în conflictul din 2003, cât de integrarea tuturor componentelor luptei armate în concepția „războiului bazat pe rețea" (Network Centric Warfare) pe timpul celei de-a doua campanii din Irak.

Organizarea şi desfăşurarea operațiilor în cadrul RBR au permis cunoaşterea superioară şi permanentă a spațiului luptei, la un nivel nemaiîntâlnit până acum în războaie, oferind forțelor flexibilitate, inițiativă, viteză şi precizie în orice mediu, cum nici ele nu se aşteptau. Chiar şi sintagma „spațiul luptei", proprie conceptului RBR, reflectă revoluția produsă în reprezentările dimensionale despre constituirea vectorilor violenței armate. De asemenea, în cadrul coaliției antiteroriste, RBR, ori unele secvențe ale sale, şi-a dovedit superioritatea, oferind, practic, posibilitatea reacției instantanee la atacuri, teroriştii putând fi loviți chiar în momentul descoperirii sau pe

timpul acțiunii. După apariția primelor declarații despre aplicarea RBR în Irak, în 2003, s-a constatat că şi alte armate aveau preocupări asemănătoare.

În esența sa, RBR revoluționează planificarea şi desfăşurarea viitoarelor războaie, indiferent de amploare, oferind o bază principial nouă de conducere a tuturor componentelor statului participante la război, a forțelor aflate în teatru, dar şi a grupărilor operaționalizate şi rezervelor aflate la distanțe mari de teatru.

Această filosofie a fost posibilă datorită saltului, fără precedent, trăit de tehnologia informațională în ultimul deceniu, ceea ce a permis includerea într-un flux informațional unic a componentelor de **informații**, de **execuție** şi de **conducere** ale războiului. Prin realizarea şi desfăşurarea din timp, în teatrul de operații sau de război, a unor rețele computerizate ramificate de cercetare, informații şi conducere se creează un **câmp unic informațional şi de conducere**. Acest lucru permite ca elementele de lovire ale luptei armate, adică cele pentru a căror eficientizare se consumă resurse şi timp, să nu mai fie prezente fizic în totalitate în teatrul de operații. În schimb, îşi fac simțită prezența prin efectele asupra adversarului. Datorită acestui câmp unic, în campania din Irak din 2003, aviația a putut activa de pe teritoriul SUA şi altor aliați europeni, rachetele de croazieră au fost lansate din Marea Mediterană şi Marea Roşie, fluxurile logistice au putut fi gestionate şi conduse, practic, pe întregul spațiu de război. S-a realizat, astfel, un spațiu al luptei care a depăşit cu mult teatrul de operații şi s-a identificat practic cu cel de război, căpătând dimensiuni strategice. Informațiile se actualizează în permanență, circulă pe orizontală şi verticală şi sunt protejate împotriva acțiunilor inamicului. Aceasta permite cunoaşterea şi evaluarea unitară a situației, în dinamica evoluției sale, de către comandanții întregului lanț de comandă, adoptarea unor decizii în timp real, fără întârzieri, la

schimbările de situație şi transmiterea acestora rapid, la eşaloanele responsabile cu îndeplinirea lor.

La **nivel strategic**, RBR permite realizarea şi menținerea unei supremații informaționale şi de conducere asupra adversarului pe întregul spațiu de război şi pe toată durata desfăşurării acestuia, cucerirea şi menținerea inițiativei strategice, precum şi realizarea obiectivelor politice cu pierderi minime. Practic, în campania din Irak, toate elementele conducerii strategice, mare parte din forțele de lovire cu destinație strategică (aviația, portavioanele, submarinele, infrastructura economică), precum şi din logistică s-au aflat în afara posibilităților de lovire ale armatei irakiene. Totodată, în cadrul RBR, „*Economia, informația, cercetarea ştiințifică şi tehnologică devin astfel implicate direct şi permanent în filosofia şi fizionomia războiului ...*”[53].

La **nivel operativ şi tactic** se realizează continuitatea şi elasticitatea în conducerea operațiilor şi acțiunilor, capacitatea sistemelor de a se adapta la dinamica situației şi de a extinde competențele conducerii operative şi tactice la orice nivel, pe verticală şi orizontală, în funcție de cerințele planificării operației şi luptei.

RBR permite însumarea potențialului de luptă al tuturor capabilităților „dispersate” în teatru într-o „super-platformă” de luptă complexă, fără limitările specifice platformelor consacrate, realizând superioritatea şi asigurând îndeplinirea misiunilor prin concentrarea efectelor, coordonare şi cooperare. Astfel, se obțin efectele sinergetice. Succesul acțiunilor forțelor se obține datorită unor circumstanțe create prin aplicarea conceptului RBR:

- superioritatea informațională, constând în cunoaşterea profundă şi previzională a situației din spațiul luptei;
- concentrarea efectelor, nu a forțelor;

[53] Dr. Gheorghe VĂDUVA, **Războiul bazat pe Rețea în fizionomia noilor conflicte militare**, Editura U.N.Ap., Bucureşti, 2005, p.28.

- lipsirea adversarului de posibilitatea de a urmări un curs propriu, coerent al acțiunilor, prin lovirea sa oriunde s-ar afla în spațiul luptei.

În perspectivă, RBR dispune de potențialul necesar răsturnării fundamentelor organizării militare clasice, reprezentată ca un sistem ierarhic centralizat, în care eşaloanele inferioare execută directivele celor superioare. Această filosofie va fi înlocuită cu principiul **autosincronizării**, care ar însemna capacitatea unei structuri militare de a se autoorganiza, începând de la eşaloanele inferioare, alegându-şi formele, metodele şi momentul îndeplinirii misiunilor, în funcție de specificul spațiului luptei, dar respectând cerințele eşaloanelor superioare. Autosincronizarea va impune o revoluție în acțiune, dar şi exigențe suplimentare comenzii-controlului, planificării şi desfăşurării operațiilor.

Autosincronizarea, procedeu favorizat de superioritatea informațională, va permite intensificarea vitezei acțiunilor şi prevenirea ori stoparea inițiativelor şi opțiunilor adversarului[54].

În aceste condiții, se pot sesiza şi **direcțiile** evoluției acțiunilor militare:

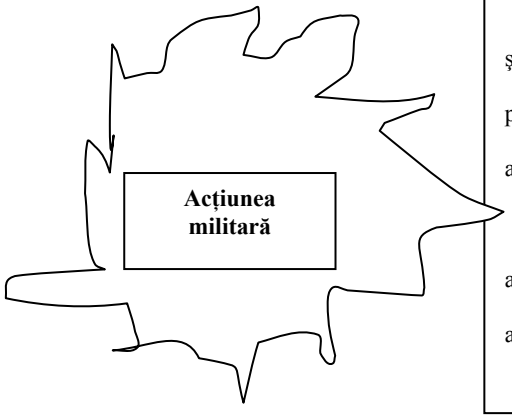
- micşorarea efectivelor participante, simultan cu creşterea mobilității şi a potențialului de luptă;
- înalta tehnologizare a planificării şi desfăşurării operațiilor;
- omogenizarea nivelurilor artei militare, mai ales prin reducerea diferențelor dintre tactică şi artă operativă;
- accentuarea rolului focului, îndeosebi a celui executat cu armamentul de înaltă precizie cu bătaie mare;
- lovirea preventivă a adversarului chiar în momentul descoperirii sale, cu toate consecințele pentru desfăşurarea unei operații;

[54] David S. ALBERTS, John J. GARSTKA, Frederick P. STEIN, **Network Centric Warfare: Developing and Leveraging Information Superiority**, 2nd Edition (Revised), 1999, p.55.

- protecţia trupelor proprii;

- accentuarea efectelor psihologice asupra adversarului în urma lovirii sale oriunde s-ar afla.

Efectele acestor direcţii ale evoluţiei s-ar manifesta în lovirea continuă şi precisă, în primul rând cu foc, a adversarului, prin folosirea complementară a tuturor capacităţilor aflate în spaţiul luptei, menţinerea permanentă a iniţiativei, protecţia absolută a trupelor proprii, diminuarea pierderilor provocate adversarului, concomitent cu demoralizarea sa totală.



Direcţii de evoluţie:

- Efective reduse, dar mobilitate şi potenţial de luptă ridicate;
- Înaltă tehnologizare a planificării şi desfăşurării;
- Omogenizarea nivelurilor artei militare;
- Accentuarea rolului focului;
- Lovirea preventivă;
- Copleşirea psihologică a adversarului;
- Depăşirea barierelor spaţiale ale dispozitivului;
- Comandanţi de tip nou

Efecte:

- Lovire continuă şi precisă;
- Complementaritate în acţiunile tuturor capacităţilor din spaţiul luptei;
- Iniţiativă permanentă;
- Protecţie absolută;
- Pierderi reduse;
- Demoralizare totală.

Desigur, toate consideraţiile în favoarea RBR s-au elaborat în condiţiile „experimentelor" de laborator ori din conflicte asemănătoare celor campaniei din Irak, unde disimetria dintre adversari a fost atât de covârşitoare, încât

rezultatul ar fi fost acelaşi şi fără RBR. Concepţia nu s-a aplicat în condiţiile în care adversarul ar fi aplicat aceleaşi „tehnici" ori ar fi avut posibilitatea de a acţiona/reacţiona pe întreaga adâncime a teatrului de război. Nu este exclus ca, într-un viitor nu prea îndepărtat, în cazul unui conflict major, RBR să constituie dominanta acţiunilor adversarului. În acest caz, îi vor fi căutate, identificate şi folosite **vulnerabilităţile**, înţelegând prin acestea disfuncţionalităţile care determină un sistem să acţioneze/reacţioneze cu dificultate. Printre cele mai semnificative vulnerabilităţi, le-am putea aminti pe cele generate de:

a) Dependenţe, care, în cazul unor conflicte majore, au naturi diferite:

- ***politice***, care încep din momentul instalării grilei senzorilor şi sfârşesc cu necesitatea armonizării permanente a intereselor partenerilor în cazul unor operaţii multinaţionale;

- ***tehnologice,*** determinate atât de sensibilităţile şi vulnerabilităţile IT, cât şi de diferenţele cantitative şi calitative dintre parteneri;

- ***operaţionale***, determinate de potenţialele de luptă diferite ale capabilităţilor aflate în spaţiul luptei;

- ***geofizice***, determinate de relief, climă, condiţii meteo etc.

b) Disfuncţionalităţi în procesul de transformare a datelor (valori fizice: obiecte, piese, oameni) în informaţii (concepte cu semnificaţii logice), prin analiză. În general, s-a recunoscut că, astăzi, pentru armate şi state, nu culegerea datelor din zonele de interes este o problemă, ci transformarea acestora în informaţii, prin analiză, pentru a putea fi introduse în fluxul informaţional. Este o problemă de timp, expertiză, formalizare. Un responsabil din comunitatea de informaţii a SUA afirma într-un articol[55]: „*Reuşim să procesăm mai puţin de 6% din semnalele culese şi*

[55] Robert David STEELE, **Listening to the Defeat, JFQ**, Autumn/Winter 1998-1999, p.82.

10% din cele de imagistică"[56]. Or, tocmai produsele realizate prin imagistică sunt cele mai folosite în RBR.

c) Inerție în realizarea autosincronizării, cel puțin în primele etape ale aplicării RBR în operații, deoarece comandanții tuturor eșaloanelor prezente în teatru trebuie să înțeleagă perfect „logica" operației, astfel încât să poată interveni instantaneu, pentru a nu permite abateri de la cursurile de acțiune alese.

d) Dezechilibre între costurile relativ mari ale operaționalizării RBR şi cele extrem de mici necesare contracarării acestuia: forme asimetrice de acțiune, tactici simple şi uşor de aplicat, mai ales în localități şi zone dens populate etc.

e) Punctele slabe ale IT în confruntarea cu omul, care poate apela la procedee uşor accesibile, aparținând războiului cibernetic, mascării, inducerii în eroare, folosirii imitatoarelor etc. Aceleaşi tehnologii, produse şi soluții, fundamentale pentru RBR, sunt accesibile şi unui potențial adversar.

Vorbind despre **viitorul RBR** asupra acțiunilor militare, probabil că ar trebui să vorbim despre un viitor apropiat şi altul îndepărtat.

Viitorul apropiat este cel deschis de campania din Irak, în care RBR a fost accesibil doar unuia dintre actori, şi acesta i-a folosit din plin avantajele. Probabil că şi în laboratoarele altora se experimentează RBR, dar numărul lor va rămâne restrâns. La direcțiile impuse acțiunii militare de RBR, actorii-țintă cărora, deocamdată, le este inaccesibilă implementarea conceptului vor avea răspunsuri simple, de aceea, eficiente:

- practici specifice insurgenței, gherilei şi, de ce nu, terorismului;

[56] Imagistică - reprezentări de obiecte reproduse electronic sau prin mijloace optice, filme, ecrane ori alte mijloace media)

- acțiuni purtate cu predilecție în mediul urban, unde grila senzorilor şi armamentul de înaltă precizie sunt mai puțin eficiente, iar oportunitățile pentru mascare mai evidente;

- acțiuni de durată, sub acoperirea mulțimii, desfăşurate de subunități reduse numeric, în tot spațiul luptei, cu efecte sinergetice comparabile cu cele obținute în cazul RBR; este posibilă o revenire la filosofia războiului popular, dar cu sensuri inversate, în care cel aparent slab se va apăra în oraşele încercuite de cel care va întruni toate caracteristicile puterii;

- implicarea societății civile din întregul teatru de război, pentru a influența desfăşurarea acțiunilor militare, atitudini, reacții etc.

În **viitorul îndepărtat**, probabil multe din vulnerabilitățile amintite vor dispărea, practicile şi procedurile RBR se vor generaliza. Istoria artei militare demonstrează că şi cele mai covârşitoare avantaje sunt neutralizate, mai devreme ori mai târziu. Raționamentele logice ar putea să ne sugereze că se va ajunge la o situație asemănătoare jocurilor de război în care învingătorul este stabilit de calculator, dar ar însemna să dăm dovadă de optimism deplasat.

Acțiunile militare vor continua să evolueze în direcțiile amintite, confirmând astfel că transformarea constituie un proces, nu o stare finală. Indiferent de gradul de tehnologizare la care se va ajunge, luptătorii vor rămâne cele mai complexe, cele mai adaptabile elemente ale acțiunii militare. RBR nu va face decât să acutizeze confruntarea umană, sub aparenta tehnologizare a ei, iar eroarea fundamentală care s-ar putea crea ar fi concluzia că rolul omului se diminuează.

Acțiunea militară va căpăta caracteristici suplimentare:

- spațiul luptei se va extinde, teoretic, putând acoperi întregul glob pământesc;

- nu vor exista locuri neexpuse loviturilor cu foc;

- confruntarea va fi punctiformă, omnidirecțională, între structuri reduse, ca efective, dar extrem de mobile, cu

potențial de luptă ridicat, capabile să execute o gamă largă de misiuni, inclusiv împotriva amenințărilor asimetrice, în termen scurt;

- principalele ținte urmărite vor fi nu atât prezențele fizice, cât impulsurile şi sistemele care le generează;

- comanda-controlul va suporta un mare grad de descentralizare, impus de imprevizibilitatea acțiunilor;

- se va urmări nu atât distrugerea fizică a adversarului, cât destabilizarea şi anihilarea psihică, punerea sa în imposibilitatea de a acționa/reacționa coerent;

- deplasările către un adversar descoperit vor fi înlocuite cu loviturile directe, ceea ce va modifica total reprezentările clasice despre dispunerea trupelor în dispozitive.

Elaborarea reprezentărilor despre modul în care se vor desfăşura viitoarele conflicte militare obligă analiştii din multe domenii sociale să se aplece asupra studiului folosirii forței într-o lume confruntată simultan atât cu integrarea, cât şi cu fragmentarea. Pregătirea acțiunilor militare nu va mai constitui doar o problemă a modului în care se organizează şi întrebuințează forțele pentru a învinge un inamic definit. Ea va include, de asemenea, modelarea şi gestionarea mediului strategic prin diplomație, respectarea legii, prevenire etc. RBR asigură condiții favorabile pentru atingerea acestor obiective, tocmai pentru că se bazează pe supremația informației.

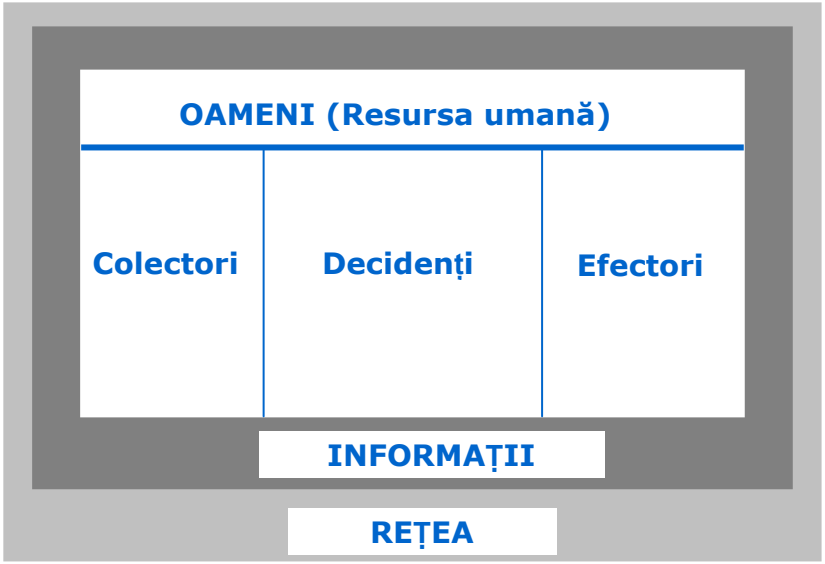
ASPECTE ACTUALE PRIVIND COMPONENTA UMANĂ ÎN CONTEXTUL "RĂZBOIULUI BAZAT PE REȚEA"

Col. ing. Aurelian IONESCU

Dimensiuni / componente

- Oameni (Resursa umană)
  - Individ
  - Organizație/organizare
  - Cultura organizațională
  - Procese activitate/afaceri
- Informația
  - Filosofia "Information Sharing" (accentul se pune pe împărtăşirea informației şi nu pe "zăvorârea" acesteia)
- Rețea
  - Mediul *sigur* pentru împărtăşirea informației

Cadrul Conceptual NNEC (NATO Networkd Enabled Capability



Dimensiuni / Componente (cont)

- Colectori
  - Surse de date variate/multiple: senzori tradiționali, servicii de informații, agenții nou create
- Decidenți
  - Colecție de capabilități şi procese privind evaluarea, predicția, simularea, planificarea şi luarea deciziei
- Efectori
  - Mecanisme la dispoziție pentru realizarea unor obiective planificate, utilizând toate instrumentele puterii (militar şi politic, economic şi civil)

Impactul asupra resursei umane

Individ
- Delegare de autoritate
- Organizație/organizare
  - Modele organizaționale
- Cultura organizațională
  - Inovare, Adaptivitate
- Procese activitate/afaceri
  - Tranziția spre "Process Age", Organizatii centrate pe procese

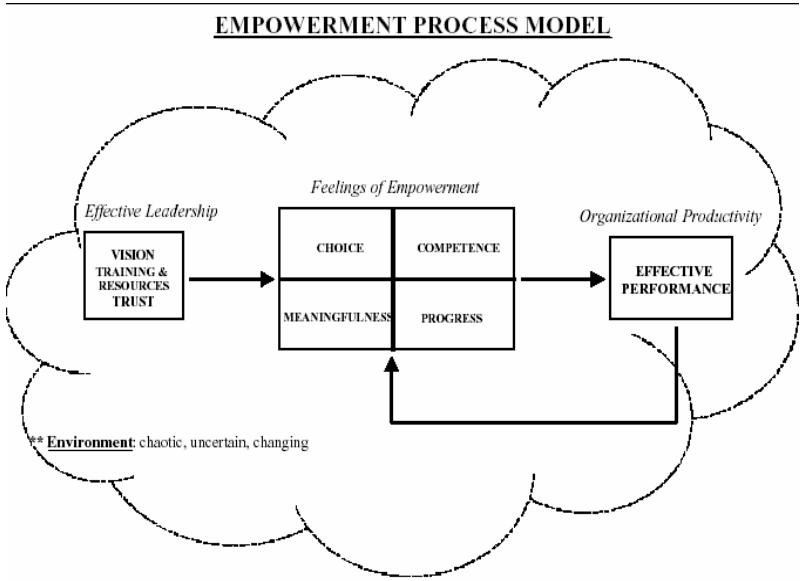
Delegare de autoritate *(empowerment / împuternicire)*

- Kouzes and Posner (1995): *a permite altora să acționeze*
  - *"Când oamenii au mai multă libertate de acțiune, mai multă autoritate şi mai multă informație, este mult mai probabil ca aceştia să-şi folosească energiile pentru producerea unor rezultate de excepție"*
- Conducere eficace → împuternicire
- Delegare de autoritate (D_a)
  - *Auto-direcționare, ce permite subiecților să participe la deciziile ce-i privesc*
  - *Stare mentală şi în acelaşi timp un rezultat al poziției, politicilor (policies) şi practicilor*
  - *Au fost dezvoltate modele teoretice de D_a:*

-interpretativ (focus pe aspecte psihologice)

-Thomas-Tymon (oamenii sunt energizați de sarcinile pe care le fac)

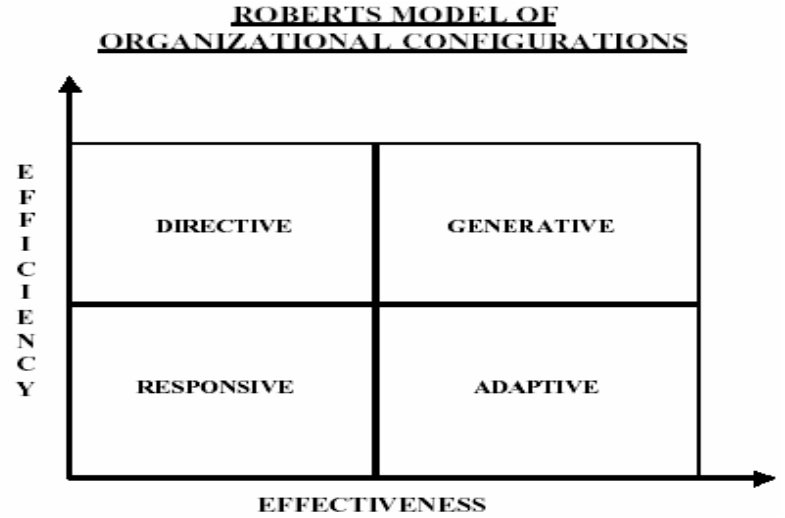
-sentimentul împuternicirii (alegere, competență, semnificație, progres)



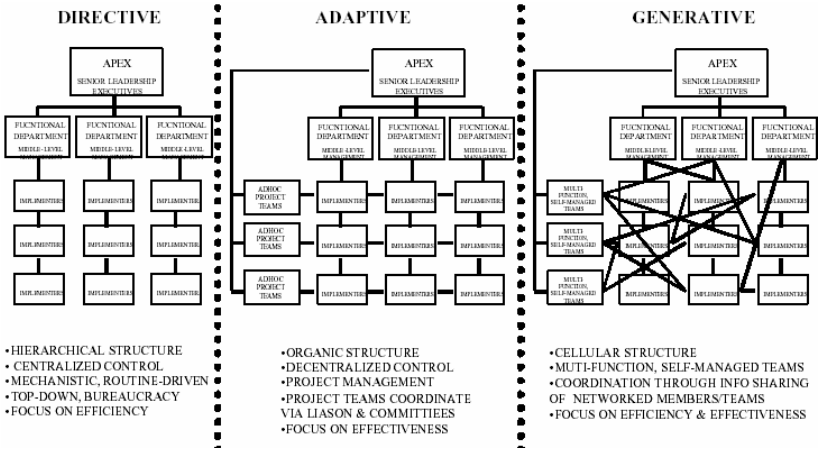
Definiția D_a

- *A permite subordonaților să acționeze într-o astfel de manieră care să le dea sentimentul că au "autoritatea" (choice) şi "abilitatea" (competence) de a "lua decizii" importante (meaningfulness) şi de a "determina efectele" acestor decizii (progress) asupra vieții personale, asupra vieții altora din sfera lor de responsabilitate, sau asupra operării organizației ca un întreg, având ca rezultat un nivel ridicat al performanței pentru întreaga organizație.*

MODELE ORGANIZAȚIONALE



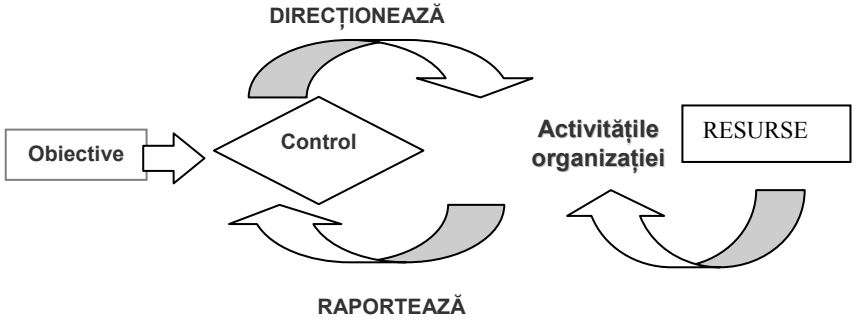
STRUCTURI ORGANIZAȚIONALE



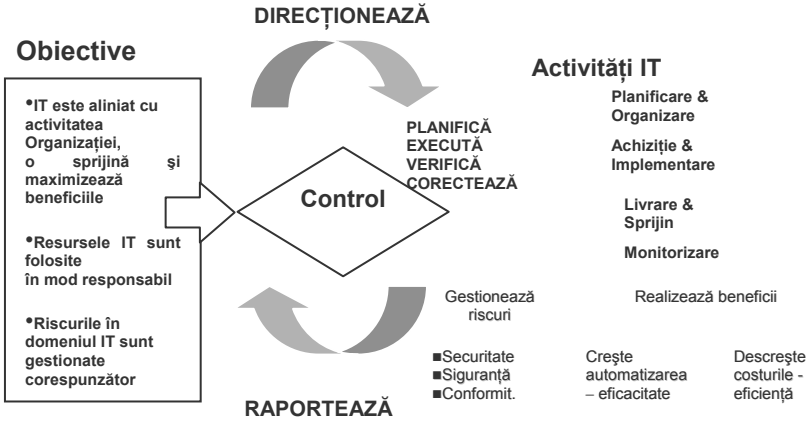
INFORMAȚIA CAPĂTĂ IMPORTANȚA STRATEGICĂ PENTRU SUCCESUL ORICĂREI ORGANIZAȚII

- **RESURSĂ: informația este o resursă ce trebuie administrată pentru a obține rezultate optime;**
- **VALOARE: informația are valoare, deşi nu este foarte simplu de determinat;**
- **COST: informația are un cost, iar producerea ei implică costuri;**
- **CICLU DE VIAȚĂ: informația are o viață utilă;**
- **IERARHIE: informația există într-o ierarhie cognitivă de date, informații, cunoştințe, învățăminte;**
- **GENERAREA INFORMAȚIEI: informația este un produs al unui proces de automatizare;**
- **ÎNLOCUITOR: informația înlocuieşte producția de masă caracteristică erei industriale atât în ceea ce priveşte produsele/serviciile cât şi procesele;**
- **BUN PUBLIC: informația contribuie la bunăstarea şi libertatea umană.**

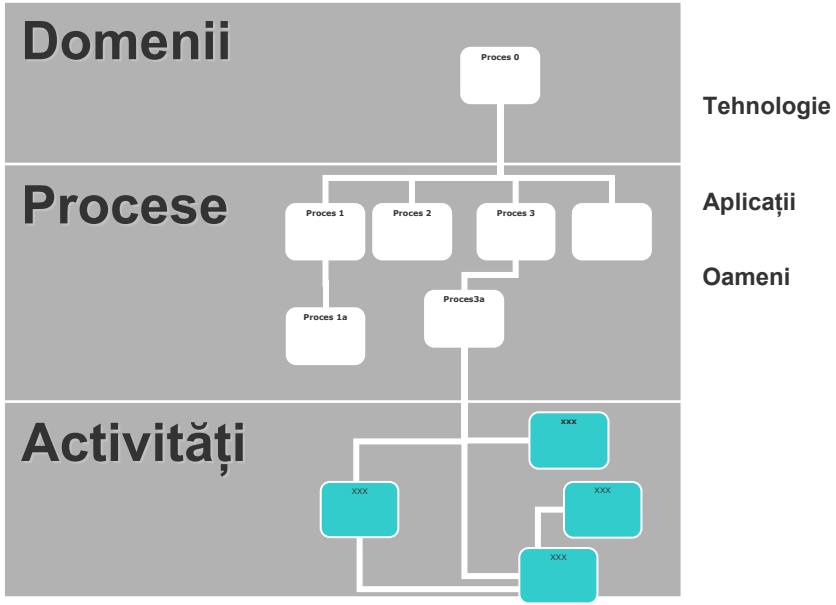
GUVERNAREA ORGANIZAȚIEI



GUVERNANȚA IT



STANDARDUL COBIT



RĂZBOIUL BAZAT PE REȚEA LA NIVELUL SOLDATULUI

Locotenent-colonel dr. ing. Liviu COȘEREANU,
Maior Tiberius TOMOIAGĂ

1. Războiul bazat pe rețea

O definiție a războiului bazat pe rețea a fost dată în 2000 de către David Alberts ș.a. din cadrul Programului de Cercetare Cooperativă pentru C4ISR al Departamentului pentru Apărare al SUA, în lucrarea „Network Centric Warfare 2nd Edition": „un concept operațional superior din punct de vedere informațional, care generează o putere de luptă sporită, prin integrarea într-o rețea informațională a senzorilor, decidenților şi executanților, în scopul cunoaşterii teatrului de operații, măririi vitezei conducerii, accelerării ritmului operațiilor, intensificării efectelor letale, accentuării protecției şi realizării unui anumit grad de autosincronizare".

Studiile de bază descriu rețeaua ca o matrice în care componente precum unități, arme şi sisteme de senzori sunt conectate la diferite noduri de acces. Acest lucru permite schimbul de informații, o înțelegere bună a scopului luptei şi conduce la o desfăşurare mai flexibilă a forțelor proprii în coordonate de timp, spațiu şi scop.

Cantitatea de informație, care va fi transmisă şi utilizată în timp real, va fi lărgită, în principiu, prin fiecare utilizator de rețea într-un mediu de luptă al viitorului.

De remarcat că forțele militare, ale căror aplicații implică resurse hard şi soft ce nu sunt întâlnite în sistemele comerciale, nu trebuie să dezvolte soluții exclusiv militare la costuri mari. Prin folosirea soluțiilor civile şi adaptarea lor la

cerințele militare, costurile şi timpul de desfăşurare pot fi reduse în mod eficient.

Rețelele de comunicații şi susținere a comenzii permit comunicarea de la cele mai înalte până la cele mai joase niveluri. Acest lucru determină o cunoaştere rapidă şi corectă a situației spațiului de luptă.

2. Sistemul de Comandă, Control şi Comunicații (C^3)

Sistemele C^3 pot fi definite în multe moduri. Definiția adoptată de NATO este următoarea: „Un sistem integrat în care sunt cuprinse doctrine, proceduri, structuri organizaționale, personal, echipamente, utilități şi comunicații, care furnizează factorilor de decizie de la toate nivelurile datele adecvate şi în timp util pentru a planifica, coordona şi controla activitățile pe care le desfăşoară ".

Comanda şi controlul, ca proces, a fost dintotdeauna caracterizat ca fiind o serie iterativă de acțiuni şi ordine. Cele mai cunoscute modele sunt următoarele:

- ciclul observare, orientare, decizie, acțiune (OODA);
- un model constituit din: stabilirea direcției, procesare, comparație, decizie şi acțiune;
- procesul HEAT (Headquarters Effectiveness Assessment Tool), care cuprinde: monitorizarea, înțelegerea, dezvoltarea alternativelor, predicția, decizia şi coordonarea.

Întregul proces de comandă şi control descris anterior devine greoi şi necesită schimbarea cu un nou concept mai rapid şi mai eficient. Războiul bazat pe rețea oferă o soluție în acest sens.

3. Sistemul soldat

Sistemul soldat este un sistem de luptă individual eficient, cu o forță de distrugere mare, integrat în totalitate, care include arme de luptă, comunicații în rețea, surse de energie, nivel crescut de performanță umană şi integritate corporală.

La ora actuală se află în desfăşurare numeroase programe care dezvoltă sisteme soldat. Cele mai cunoscute sunt:

- Statele Unite ale Americii - Land Warrior.
- Marea Britanie – FIST
- Australia – Project Land 125
- Franța – FELIN
- Germania – System Soldat – Idz
- Olanda – Soldier Modernisation Program
- Spania – Combatiente Futuro
- Suedia – MARKUS.

Toate sistemele soldat enumerate mai sus converg către aceeaşi idee, şi anume, creşterea eficienței acestuia pe câmpul de luptă şi sunt aproape identice sub anumite aspecte:

- sistemul de comandă şi control îmbunătăţeşte considerabil cunoştințele despre situația reală din teren ale soldatului şi oferă o posibilitate crescută de identificare amic-inamic;
- comunicația între grupul de luptători şi eşaloanele superioare se va face în rețea, prin intermediul unui vehicul de luptă sau al altui nod de acces la rețea;
- echipamentele de navigație bazate pe GPS vor furniza date pentru sistemul C^3 şi vor oferi soldatului informații precise privind poziția acestuia.

Fluxul de informație va fi transferat:

- orizontal – de la soldat la soldat
- vertical – de la soldat la comandant sau la un centru de comandă.

Comunicarea orizontală va avea ca preocupare esențială coordonarea operațiunilor în cadrul unității.

Comunicarea verticală, pe de altă parte, va fi compusă din raportări şi din achiziția unui tablou comun al situației, împreună cu informații şi recunoaşterea de la eşalonul superior.

4. Tehnici de comunicare

La proiectarea unei rețele de comunicații trebuie să se țină cont de volumul datelor ce vor fi transferate. Acestea includ: voce, text, video, navigație, poziționare, criptare şi corecție a erorilor. Ratele de transfer necesare pentru fiecare sunt prezentate în tabelul de mai jos:

Serviciu de date	**Contribuție la rata de transfer**
Voce	16 kbps
Text	128 kbps
Video: 640*480, 256 culori, 25 Hz Video: 640*480, full color, 60 Hz	1,23 – 2,5 Mbps * 8,8 – 17,7 Mbps **
Navigație şi poziționare	52,8 kbps
Criptare	Neglijabilă (32 – 512 biți)
Corecția erorilor	1,4 – 2,7 Mbps * 9,0 – 17,9 Mbps **
Total	***2,9 – 5,4 Mbps*** * ***18,0 – 35,8 Mbps*** **

Tabelul 1: Volumul datelor transferate în rețea

Aceste rețele pot fi fixe sau mobile, cu sau fără fir. Cele mai indicate pentru operațiuni militare sunt rețelele mobile fără fir, deoarece pot fi mutate împreună cu unitatea pe care o deservesc şi sunt uşor de instalat.

Comunicațiile de date fără fir pot fi realizate folosind şi următoarele standarde: BlueTooth, IEEE 802.11b, IEEE 802.11a, HiperLAN/2, UWB sau în banda de 60 GHz. La

alegerea unui standard trebuie să se țină cont de rata de transfer şi de distanța la care acestea pot asigura transferul de date.

Standard	Transfer	Distanță	Observații
WLAN - BlueTooth	720 kbps	100m	
WLAN – IEEE 802.11b	10-11 Mbps	100m	
WLAN – IEEE 802.11g	100 Mbps	100m	
WLAN – IEEE 802.11a	31 Mbps	50m	
HiperLAN/2	34 Mbps	150m	În dezvoltare
UWB	60 Mbps	600m	În dezvoltare
60 GHz	10-40 Mbps	2-3 km	Nu este comercial (deocamdată)

Tabelul 2: Standardele pentru rețelele fără fir

Este foarte important ca datele transferate să asigure buna desfăşurare a operațiunilor şi să evite, în acelaşi timp, supraîncărcarea rețelei cu informații care, fie sunt inutile, fie nu pot fi procesate în timp util.

5. Concluzii

Una din provocările actuale ale armatei române este dezvoltarea unui astfel de soldat-sistem, care va deveni pionul războiului bazat pe rețea şi va trebui să fie compatibil cu sistemele similare dezvoltate de celelalte țări. Pe lângă sistemele de armă, protecția individuală şi diverşi senzori ce vor face parte din acest sistem, trebuie depăşite unele bariere tehnologice în ceea ce priveşte informatizarea şi sistemele de comunicații de date.

Principalele probleme tehnice, din punct de vedere al integrării soldatului într-o rețea care va sta la baza coordonării unor acțiuni de luptă, sunt date de:

- securitatea datelor;
- stabilirea priorităților în fluxul informațional;
- lărgimea de bandă pentru comunicațiile cu eşalonul superior, de la soldat la companie, batalion sau brigadă;
- proiectarea unei interfețe om-maşină, astfel încât implicarea soldatului să fie cât mai mică.

BIBLIOGRAFIE:

HASSGARD Ulf, **The lowest echelon in Network Centric Warfare**, Swedish National College, 2002.

DEZBATERI

Gl. lt. dr. MEDAR: Unii au încercat să rezolve problema volumului foarte mare de informaţii automatizat prin selectarea lor automatizată. Rezultatele au fost dezastruoase, pentru că se pierdeau frânturile esenţiale de informaţii. Deci, la aşa ceva nu există decât o singură soluţie: mărirea capacităţii de analiză. La ora actuală, la noi există un asemenea centru de informare operativă, care lucrează 24 de ore din 24. Vă daţi seama că vin acolo zeci de mii de informaţii, hai să zicem, mii de informaţii în 24 de ore. Dar, acesta este un element. Un alt element este ca, pe parcurs, să mai existe filtre formate tot din analişti. O să vă dau un exemplu: la acest Centru de Informare Operativă nu vine nimic din surse deschise. Toată culegerea din surse deschise se face de către alte structuri, de analiză numai a surselor deschise, prin motoare de căutare. Ei sunt analişti foarte buni şi deja fac primul filtru, prima discernere între informaţii, între ceea ce înseamnă informare şi dezinformare. Sursa deschisă, pe care foarte multă lume o consideră, la ora actuală, ca un element important al culegerii de informaţii, este cea mai parşivă sursă posibilă. Când noi vrem sau altcineva vrea să acţioneze asupra unei forţe oponente, să încerce să îl distrugă sau să îl anuleze, diminueze, capacitatea unei structuri de informaţii oponente, foloseşte sursele deschise. Nu numai că îl inundă pe acesta cu un volum foarte mare de informaţii, dar şi cu informaţii contradictorii, atribuite, artificial, altor surse; de asemenea, o informaţie, care este, de fapt, o dezinformare, se introduce într-un sistem de surse deschise, dându-i-se surse diferite, şi, în felul acesta, cel de acolo o vede prima. Peste 10-15 minute, peste o oră, aceeaşi informaţie îi apare atribuită altei surse. Şi gata, se confirmă. Şi, de fapt, ea este generată din acelaşi loc. Nu sunt deloc un mare partizan al surselor deschise, ci spun că sunt necesare, e bine ca ele să fie abordate, dar cu

foarte mult discernământ, mai ales ţinând cont de faptul că sursele deschise sunt un mâncător uriaş de timp. De aceea, avem Centrul de Informare Operativă şi un alt centru pentru surse deschise. Sursele deschise sunt accesate de acolo, apoi sunt transmise numai informaţiile prelucrate. Soluţia este creşterea numărului de oameni, prin crearea unor asemenea cascade de analiză, mai ales pe surse deschise. Pe sursele închise nu este nevoie, pentru că acolo volumul nu este chiar exagerat de mare, acolo ceea ce se poate obţine poate fi păstrat şi controlat, atât cantitativ, cât şi calitativ.

Gl. mr. SAVU: În ceea ce priveşte culegerea de informaţii de către senzorii tehnici şi analiza lor automată, aşa cum a menţionat dl. general Medar, în lumea reală s-a constatat că a fost o catastrofă în ultimele conflicte. De aceea, factorul uman, „ochi în teren”, şi analiza acestor informaţii a transferat partea automată către cea umană, ceea ce a generat constituirea unor noi structuri. De exemplu, la nivelul corpurilor sau diviziilor în armatele care participă în coaliţie, americane sau britanice, s-au constituit subunităţi de tip companie care aveau 150 de analişti în companii de informaţii militare. Ei pot lucra concentrat sau dispersat în structuri de companie, batalion, brigadă, dar valoarea lor este dată tocmai de această capacitate de a se interconecta, de a analiza împreună informaţiile, evenimentele şi a prezenta comandanţilor numai acele informaţii relevante pentru operaţie. Este vorba despre creşterea numărului de analişti, ofiţeri de informaţii. Aceasta este soluţia care s-a găsit la momentul de faţă.

Gl. lt. dr. MEDAR: Pe vremea când eram inginer, acum nu mă mai consider, făcusem un program similar, un program de optimizare a soluţiei. În toate sistemele de analiză, ca şi în acela, trebuie ca omul să dea ponderi anumitor intrări şi să spună: intrarea asta are ponderea 0,1, intrarea asta are 0,15, asta 0,8 ş.a.m.d. În funcţie de cum ai dat ponderi, dirijezi sistemul automat către soluţia pe care o vrei. Şi nu este normal,

nu este un lucru real. Aşa cum spunea dl. general Savu, şi la sistemele de analiză computerizată şi la sistemele de colectare prin senzori - aceasta a fost o muncă extraordinară pe care au făcut-o alte state, pentru că erau informaţii analogice, digitale, informaţii prin imagine, informaţii tip raport scris şi toate acestea au trebuit aduse în acelaşi format-, iar selectarea şi interpretarea lor se fac automat. S-a făcut şi rezultatul a fost catastrofal.

Dr. DOLGHIN: Principalul avantaj pe care l-a determinat Războiul bazat pe Reţea, acolo unde a fost folosit, este capacitatea de a lovi adversarul, practic, în timp real. Exploatarea deplină a acestui avantaj pune în discuţie ciclul de transformare a datelor în informaţii, deci, procesul de analiză. Logica te îndeamnă să crezi că, cu cât ciclul este mai scurt, cu atât avantajul pe care ţi-l oferă Războiul bazat pe Reţea este mai evident. Dar apare o situaţie paradoxală: fie comandantul acţionează ca ofiţer de informaţii, fie ofiţerul de informaţii acţionează ca un comandant. Ce părere aveţi?

Gl. lt. dr. MEDAR: Orice element de lovire, chiar şi în Războiul în Reţea, are două etape: o primă etapă de cunoaştere a existenţei inamicului, pentru că nici în Războiul în Reţea, atunci când am o grupare de 8 oameni, sau de 12, şi ştiu că am în faţă o brigadă, nu mă apuc să o lovesc. În această primă etapă, acel comandant are nevoie de informaţii şi de imaginea întregului câmp de luptă, în care primeşte informaţii şi are nevoie de acest proces, de analiză, chiar dacă el durează 24 de ore sau 5 zile sau 8 ore ş.a.m.d. Cel de al-doilea element este exemplificat de ceea ce se întâmplă acum în Irak. Noi asigurăm cu informaţii sectorul polonez. Zilele trecute, polonezii au desfăşurat o operaţiune neaşteptată pentru insurgenţi, în care au reuşit capturarea a peste 150 de insurgenţi. Mai întâi, am furnizat datele despre ceea ce exista acolo, după aceea a început acţiunea propriu-zisă. Informaţia participă şi la procesul de conducere a acţiunii propriu-zise, dacă vreţi, pentru că în timp

ce polonezii acţionau, noi aveam alături grupurile HUMINT, care le transmiteau informaţii în timp real, erau înaintea lor, şi transmiteau – „Sunt în acea casă, acum au intrat, acum au ieşit etc.”, iar ei veneau cu forţa de lovire. Aveam capabilităţi SIGINT care erau în ascultare pentru toată zona şi transmiteau comandantului polonez permanent informaţii, iar zona era survolată de un avion fără pilot, de unde veneau informaţii care se transmiteau tot comandantului polonez şi îi spuneau: „Ies, au luat-o la fugă pe strada X, blocaţi-i dincolo, vedeţi că au ieşit din oraş cu două camioane, trebuie blocaţi la intersecţia Y sau pe şoseaua Z”. Informaţiile se transmit atât în pregătirea unei operaţii, cât şi pe timpul desfăşurării ei. Este cea de-a doua categorie de informaţii, care, practic, participă direct la conducerea operaţiei în desfăşurare. Comandantului i se spune: „Acum este acolo, vezi că celălalt e dincolo, vezi că şi-a adus încă forţe suplimentare care sunt mai puternice decât ale tale”. Astfel, comandantul decide: „Mă retrag”, sau „Lovesc”, „Ocolesc”, „Evit”.

Dr. ALEXANDRESCU: Sursele de obţinere a datelor despre adversar şi forţele proprii sunt multiple în cadrul Războiului bazat pe Reţea. Am înţeles că prelucrarea lor în informaţii trece printr-un ciclu, prin mai multe filtre până când ajunge într-un centru de stocare. Din acest centru de stocare, cum sunt puse informaţiile la dispoziţia executanţilor din teatrul de acţiune - sunt direcţionate către aceştia sau se oferă un cadru larg din care cei interesaţi să îşi poată lua diferite informaţii? Dacă sunt direcţionate către anumite entităţi organizatorice, cine este cel care le dirijează? Este ofiţerul de informaţii capabil să pună la dispoziţia anumitor entităţi organizatorice informaţiile de care au acestea nevoie? Poate el să intuiască intenţia comandantului? Este uşor să manevrezi anumite lucruri din informaţii. Nu cumva apare riscul ca unele păreri, mai puţin augmentate, ale ofiţerului de informaţii să fie inoculate în decizia comandantului?

Gl. lt. dr. MEDAR: Aţi vorbit despre accesul la informaţii în reţea, în baza de date. În baza de date sunt, în general, informaţii care sunt puse la dispoziţia analiştilor pentru viitoarele şi actualele analize, deci, nu informaţia despre care spuneam că are nevoie comandantul acum. La ora actuală, baza de date a Direcţiei de Informaţii nu poate fi accesată decât din Direcţia de Informaţii, iar în viitor numai aşa va fi, pentru că este o bază de date internă, ea dă şi sursa, deci, nu pot fi accesate decât de acolo şi într-o modalitate care să asigure toate protecţiile necesare. Acolo nimeni nu poate accesa orice din baza de date. Fiecare îşi poate accesa doar domeniul lui de activitate. Din baza de date informaţiile nu pot să ajungă decât la cel care se ocupă de pregătirea viitoarei structuri care pleacă. Din baza de date se scot lecţiile învăţate, datele necesare pentru pregătirea viitoarei rotaţii sau a unei dislocări într-o ţară pe care deocamdată nu o ştim nici unul. Acolo există deja informaţii adunate în baza noastră de date despre posibile viitoare ţinte, în care, dacă mâine se ia o decizie ca România să trimită trupe în ţara X, măcar să putem da informaţiile de bază, necesare pentru luarea deciziei, despre ce ar trebui făcut pentru a acţiona în acea ţară sau în aria de responsabilitate Y. Acesta este un tip de informaţii. Pentru comandant este lucrul despre care vorbeam. Este obligaţia noastră, a celor din structurile de informaţii şi obligaţia UNAp să se facă o pregătire de informaţii a comandanţilor. De mai multe ori am vorbit despre acel curs de informaţii pentru comandanţi pentru că este esenţial pentru acesta să ştie cum să-şi ceară informaţiile şi ce anume să ceară. Referitor la posibilitatea de a influenţa decizia prin informaţii, da, categoric, aşa este în toată lumea. De aceea, este absolut nevoie ca structurile de informaţii, întotdeauna, la nivel central, ca şi cele din teatru, deci, cel care se ocupă de informaţii în teatru, să fie un om echilibrat, care să îşi dea seama de responsabilitatea muncii lui atunci când îi transmite informaţia comandantului, iar la nivelul structurilor centrale, la fel, trebuie

să existe nişte oameni echilibraţi, care să nu aibă absolut nici un fel de implicaţii politice şi capabili să furnizeze întotdeauna informaţia cât mai plată. Când mă duc la şeful Statului Major General sau la ministru, şi îi transmit datele, mă străduiesc să nu folosesc cuvinte care să-l ducă spre o decizie sau către alta. O teorie veche spunea că atunci când merge la Şeful Statului Major General sau la ministru, un şef al unui serviciu de informaţii trebuie să îi spună: „Asta este informaţia”. Şi atunci când personalitatea de decizie politică sau militară întreabă: „Ei, şi ce zici? Ce ar trebui să facem acum?”, răspunsul ar trebui să fie „Sir, my job is over”. V-am dat informaţia, de aici încolo e treaba dumneavoastră. Tendinţa actuală nu mai este aceasta. Modalitatea actuală de transmitere a informaţiilor factorilor de decizie ar fi: cel care se duce să prezinte această informaţie, trebuie să aibă 1,2,3,4,5, variante posibile de acţiune şi atunci când este întrebat „Ce trebuie să facem acum?”, să răspundă: „Dacă luaţi această decizie, acestea vor fi posibilele consecinţe”, ş.a.m.d. şi să prezinte o paletă de proiecţii din care, poate, că nu va fi aleasă nici una. Dar aceasta nu mai este treaba celui care prezintă informaţiile.

Cu privire la imaginile prin satelit, din punct de vedere al informaţiilor, interesul pentru acea imagine, chiar dacă este în amănunt, se află undeva în jur de 10% - 15% pe o scală de valori. Ceea ce mă interesează este să am acea imagine a zonei în dinamică, dacă se poate, la 24 de ore, la 4 ore, la 6 ore. Au fost unii, acum câţiva ani, care aşa şi făceau. Aveau acea imagine şi la 24 de ore, când trecea satelitul, mai luau o imagine şi toate erau în regulă, când, de fapt, acolo era un loc de instruire pentru arme nucleare. Se ştia că, atunci când trece satelitul să ia imaginea, le ascundeau. După ce ştiau că a trecut conul satelitului, continuau activitatea, le pregăteau pentru lovituri ş.a.m.d. Asta s-a întâmplat acum câţiva ani. Chiar la 24 de ore e puţin, o imagine dată în acest fel are o anumită valoare, iniţială, pentru că, ulterior, trebuie verificată cu mijloace

HUMINT. Esențial, în conflictele asimetrice, care au ele însele o dinamică foarte mare, este necesară imaginea la un interval de timp cât mai mic. Dacă dl. general Sandu îmi propune o soluție eficientă cu o imagine de acest gen, eu o să-i mulțumesc şi o să-i spun că vreau un terminal. Dacă poate să facă aici, în România, un terminal cu care să poată fi accesați sateliții comerciali - poți să obții imagini dintr-un port rusesc, de pe un satelit rus, de ce nu? Deci, pot fi accesate şi plătite canale pe orice satelit, dar imagini dintr-o anumită zonă şi, dacă se poate, cu un terminal aflat în țară, pentru că imaginea de informații necesară este una care trebuie să vină la interval scurt.

Dr. ALEXANDRESCU: O întrebare pentru dl. general Sandu. Desigur, putem discuta foarte multe despre Războiul bazat pe Rețea, despre concept, despre schimbarea mentalității oamenilor, despre multe alte lucruri care se pot realiza. Problema cea mai importantă este a domeniului dumneavoastră. Mă refer la faptul că în spatele tuturor acestor lucruri stau nişte mijloace tehnice pe care noi putem să le asigurăm sau nu în cadrul Alianței, mă refer la nivel de Alianță. Desigur, conceptul de Război bazat pe Rețea, deocamdată, aparține unor state puternic industrializate, care sunt şi capabile să le pună în operă. În viitor, presupun că şi noi vom fi capabili să realizăm elemente din acest sistem bazat pe rețea. În aceste condiții, el are caracter național sau de Alianță. Dacă are caracter național, vom fi vreodată în stare să ajungem la nivelul Alianței, cu tot ce asigurăm, ca să fim interoperabili cu Alianța. În cadrul conceptului universal plug and play, vom avea un sistem adecvat cu care să ne interconectăm la sistemul Alianței, atunci când considerăm noi că este necesar? Sau se vor stabili, la nivelul Alianței, anumite ochiuri din această plasă, din această rețea care sunt obligatorii pentru noi de realizat iar noi, în cadrul acestor rețele, vom face lucrurile naționale la nivel național?

Gl. fl.aer. dr. ing. SANDU: Nu vom ajunge niciodată la nivelul pretențiilor Alianței din mai multe motive. Noi va trebui să fim, însă, conectați, apropo de Războiul bazat pe Rețea, la tot ce se întâmplă în Alianța Nord-Atlantică. De exemplu, referitor la ce spunea domnul general Medar, despre avioanele fără pilot este o realitate. Dacă informația ajunge din Irak la Bucureşti, fiți sigur că ea poate să ajungă şi de la Bucureşti la Bruxelles şi tot în timp real. Un al doilea exemplu pe care vreau să vi-l dau, pentru a arăta legătura dintre național şi internațional, sau multinațional, se referă la cel mai important proiect al Alianței, sistemul AGS - Alliance Ground Surveillance. România contribuie la realizarea sa printr-o contribuție financiară evaluată la mai mult de trei milioane de euro, dar România nu va cumpăra niciodată un sistem AGS. Ca țară membră NATO, contribuim la realizarea unei capabilități de luptă comune, vom putea beneficia de ea, de toate informațiile pe care NATO, ca structură, le poate obține cu acel sistem. Va trebui, însă, să avem grijă, şi avem grijă, ca informațiile de care avem nevoie să le putem lua în formatul, pe canalul, la dimensiunea absolut necesare şi să le utilizăm în scopuri naționale, dacă acele scopuri naționale vor exista. Elementele pe care le-am prezentat - de exemplu, echipamentul cu soldatul viitorului – sunt o contribuție națională la realizarea acestui element component dintr-o rețea. Soldatul viitorului lucrează în rețea, atât cu avioanele fără pilot, cât şi cu transportoarele, tancurile şi cu alte elemente. Avem în vedere ca acest echipament, al soldatului viitorului, să poată fi interconectat cu celelalte capabilități, celelalte sisteme de armament realizate până în momentul de față la noi în țară. Avem grijă ca ceea ce realizăm - elemente, subcomponente, bucățele din Războiul bazat pe Rețea - să rezolve probleme la nivel național, dar care să poată fi folosite oricând la nivel multinațional, atât în cadrul NATO, cât şi, sperăm cât mai

curând, în cadrul Uniunii Europene, pentru că aceste capabilităţi vor fi absolut necesare.

Referitor la întrebarea dacă Războiul bazat pe Reţea este un nou tip de război sau o modalitate de ducere a războiului, părerea mea e că conceptul de Network Centric Warfare este suportul care sprijină ducerea acţiunilor de luptă. Deci, nu este un nou tip de război. Referitor la împărţirea procentuală între contribuţia factorului tehnic şi a factorului uman în acest nou concept, cred că aproximativ 70% are importanţă zona tehnică, 30% este important factorul uman, deşi în prezentare am subliniat faptul că factorul uman este un element critic al Războiului bazat pe Reţea.

Gl. mr. SAVU: Se păstrează principiul unităţii de comandă; imaginea operaţională comună - nu înseamnă că dacă sunt şapte şefi ierarhici fiecare dă alte ordine -, chiar dacă se dau simultan - aici e vorba de separarea ierarhiei organizaţionale de cea informaţională. Cea organizaţională îşi păstrează structura, iar la cea informaţională se ajunge direct şi la cel care trebuie. În imaginea operaţională comună are o singură informaţie, nu şapte. Cea de-a treia observaţie se referă la cunoaşterea intenţiei comandantului – el ştie ce i-a transmis comandantul să îndeplinească, lăsându-i un anumit grad de libertate pentru a duce la îndeplinire misiunea.

Col. HORNEA: Cred că întrebarea domnului colonel a vizat concluziile prezentării mele, în care defineam tehnologia ca o capabilitate. Suntem în secolul XXI, era informaţională şi dezvoltarea tehnologiei impun transformarea acestui concept. Una din modalităţile de transformare este şi organizarea structurală, educaţională, de schimbare a mentalităţii în conceptul Războiului bazat pe Reţea. De aceea, tehnologia este importantă şi văzută ca o primă capabilitate. În acelaşi timp, nu poţi să discuţi despre tehnologie fără oameni capabili. Noi am exclus că în Armata României se poate întâlni o situaţie în care oamenii să fie incapabili să folosească tehnologie înaltă.

Armata României a dovedit că, indiferent de unde s-a cumpărat sau s-a produs tehnologia, în timp foarte scurt a deservit-o. Luaţi exemplul acestor UAV-uri, au fost antrenaţi în trei săptămâni şi au plecat în teatru şi dau imagini şi acum, iar alte ţări dezvoltate nu sunt în stare să opereze UAV-uri în teatru. Din punct de vedere al cerinţelor de capabilităţi, noi le stabilim pe standarde NATO. Când vorbim de o capabilitate airlift, sealift, vorbim de capabilităţile aprobate la Praga.

Dr. ALEXANDRESCU: Dacă şi cum se justifică sacrificarea cercetării în folosul obţinerii informaţiilor? Mă refer la faptul că se introduc noi concepte şi modalităţi de folosire a cercetării tehnice. Cercetarea prin luptă, ca procedeu de cercetare, a devenit istorie, iar angajarea cercetaşilor în acţiuni directe, din câte ştiu, nu este recomandată în nici un manual al acestora din armatele moderne. Întrebarea mea este: se justifică această sacrificare a celui mai specializat luptător în schimbul unor informaţii care puteau fi procurate şi cu alte mijloace?

Gl. mr. SAVU: Referitor la prima întrebare, forţele pentru personal, mentenanţă şi participarea Universităţii la exerciţiul Romex, evident, costurile pentru selecţia, pregătirea şi menţinerea nivelului de instruire a personalului, în cazul unei asemenea brigăzi, este mult mai mare decât în brigăzi cu o organizare structurală clasică şi cu o dotare nedigitizată. Selecţionarea personalului, la fel ca şi în Forţele Terestre, are nişte criterii, nişte standarde de selecţie extrem de ridicate, pregătirea personalului se face pe o durată de aproape trei ori mai mare, cu costuri semnificativ ridicate. Mentenanţa este simplificată datorită calităţii materialelor utilizate. De exemplu, pentru Stryker se foloseşte un motor care merge garantat un milion de kilometri. Sunt utilizaţi combustibili şi sisteme integrate de ultimă generaţie atât în ceea ce priveşte mecanica, transmisia şi partea de electronică extrem de costisitoare, care folosesc materiale. Aşadar, pregătirea personalului presupune

criterii de intrare, selecție, pregătire ca specialişti şi după aceea de menținere a acestei specializări, mult mai ridicate decât într-o unitate clasică. Se are în vedere exact raportul cost - calitate şi eficiența misiunii. Pentru unii, acest lucru nu contează foarte mult. Ca să dau un singur exemplu, digitizarea Diviziei 1 cavalerie, începută în 1999, a avut un cost estimat de 340 de miliarde de dolari, ajungând la sfârşitul anului 2001 la 680 miliarde. Referitor la exercițiul românesc, s-a inclus în orarul desfăşurării activităților o perioadă de participare efectivă la exercițiu, au început deja pregătirile, până la începutul lunii iulie se vor face toate amenajările logistice. În această perioadă există şi o zi a distinşilor vizitatori, - personalul Universității Naționale de Apărare poate să participe la acea zi, când se prezintă esența acestui exercițiu. Dacă se doreşte, se poate participa pe toată durata exercițiului, se pot urmări procesul de planificare, procesul de integrare a subunităților româneşti cu cele americane, echipamentele folosite şi alte detalii. După cum ştiți, americanii vor determina nişte zone cu acces restricționat, în general, punctele de comandă, partea de comunicații cu bazele din Germania sau din Alabama, Texas. La întrebarea referitoare la informatizarea părții logistice, batalionul logistic este integrat în structura unității, a marii unități, aşa cum este şi la noi. Diferența constă în faptul că este complet informatizat. Batalionul logistic are capacitatea de a afla în orice secundă, de exemplu, care sunt consumurile pe toate clasele de materiale, începând de la 1 la 9, după terminologia americană, în momentul în care muniția este scoasă, de exemplu, din locul ei; dacă vorbim de rachete sau de proiectile de calibru mare, automat, senzorul respectiv, prin computerul de bord, transmite, celui care se ocupă de aprovizionarea cu muniții, care este nivelul de consum. Există mijloace blindate automatizate, cu un profil foarte scăzut, care pot transporta muniția chiar la locul de executare a focului, chiar dacă acestea se află în mers. S-a ajuns până la realimentarea din mers, exact ca la avioanele la

care se poate face realimentarea în aer; există dispozitive speciale de realimentare, pentru că acestea sunt puse în containere, iar muniția este cuplată în ele. La fel se face şi pentru combustibil şi pentru alte categorii de materiale. Asistența medicală este de mare vârf. Au fost mai mult de 200 de cadre în brigada Stryker, în prima brigadă, în care ofițerii care au luptat în primul război din Golf, care şi-au pierdut membre - o mână, un picior, au fost duşi, demonstrativ evident, pentru încurajarea celorlalți, în cele mai sofisticate centre, în aşa-numitele forward logistic base - nişte spitale înaintate, situate pe nave - unde se aplică proteze funcționale de ultimă generație. Proteze funcționale înseamnă că o mână, chiar dacă este retezată, este funcțională, cu anumite limite, poate să ridice greutăți, până la câteva kilograme, se interconectează nervi, exact ca la un android.

Singura unitate de tip batalion, care nu este integrată organic în brigadă, este unitatea de aviație. Acest lucru nu înseamnă că nu se fac antrenamente, nu se pregătesc şi nu operează împreună. La noi există deja un program de integrare, cel puțin pentru forțele speciale, unitățile pentru intrare şi extragere din teatru, se încearcă o dotare, cel puțin la nivelul mijloacelor de comunicații, compatibilă cu grupurile de diferite tipuri - Alfa, Bravo ş.a.m.d. - pe care le au forțele speciale. Este o primă încercare. Oricum, integrarea unităților de aviație este o cerință fără de care nu se poate acționa. Deplasarea şi mobilitatea cea mai mare sunt conferite de unitățile de aviație. Şi această problemă se rezolvă în comun. Probabil că unul dintre modelele pe care le vom urma va fi cel al infanteriei marine americane, în care piloții sunt antrenați împreună cu unitățile luptătoare direct. Viitorul pilot este un simplu soldat într-un vehicul Stryker şi face exact ceea ce face un soldat. Mai mult, înainte de a se califica pilot, este trimis într-o operație, vede tot ce se întâmplă şi apoi operează împreună cu cei pe care îi sprijină. Ei sunt, totuşi, considerați sprijin de luptă. La noi, a

fost sesizată această chestiune în urmă cu vreo 2-3 ani în urmă; integrarea unităților de aviație de diferite tipuri şi dimensiuni, nu numai la nivelul conectivității, al mijloacelor de comunicații, ci şi acțional - este vorba de acel mental care trebuie să fie comun pentru toate unitățile integrate în acest sistem. Referitor la cercetaşi, nu este vorba de sacrificarea lor. Capacitățile lor sunt de a determina locul, poziția şi intenția, aşa cum se ştie dintotdeauna, a forțelor principale ale inamicului. În dotarea lor există asemenea capacități, astfel încât ei pot să determine inamicul, forțele sale principale, să fie angajate de acest batalion de cercetare, prin mijloacele pe care le au, sau să îl determine să-l modeleze, aşa cum se spune. Au muniții inteligente pe care le pot amplasa în diferite locuri, au senzori care pot fi amplasați din timp pe viitoarele căi de comunicații, iar învingerea cercetaşilor adverşi este unul din obiective, nu în sensul de nimicire fizică. Învingerea înseamnă aflarea informațiilor înaintea acestora, prin senzorii şi capacitățile pe care le au. Cel mai important element constituent al brigăzii Stryker este considerat cercetaşii, acest batalion de cercetare prin luptă, care poate angaja lupta; dar, tot atât de rapid, pe cât angajează lupta şi determină locul, mijloacele şi intențiile inamicului, o poate dezangaja la fel de rapid. Mijloacele pe care le au la dispoziție, tehnologic vorbind, sunt superioare celorlalte trei batalioane pe care le are brigada. Mijloacele lor au calibre mai mari, au alte sisteme de armamente şi de senzori, pot să se angajeze şi să se desprindă foarte rapid când este vorba de contact de luptă. De fapt, acesta este un principiu american mai vechi - unitățile lor de cavalerie, care sunt unitățile de cercetare de la noi -, tot timpul au determinat capacitățile inamicului, locul şi intențiile sale, sau l-au indus în eroare, pentru a putea angaja ulterior, pentru a avea această libertate de mişcare a comandantului, care are forțele de manevră în subordine, pentru a angaja sau evita forțele principale ale inamicului.

SPONSORI:

IBM ROMÂNIA

C.N. ROMTEHNICA S.A

EDITURA UNIVERSITĂȚII NAȚIONALE DE APĂRARE

Redactor: CORINA VLADU
Tehnoredactor: MIRELA ATANASIU

Bun de tipar: 25. 07. 2005
Hârtie: A3 Format: A5
Coli de tipar: 12,375 Coli editură: 6,1875

Lucrarea conține 198 de pagini
Tipografia Universității Naționale de Apărare

CENTRUL DE STUDII STRATEGICE DE APĂRARE ŞI SECURITATE
Şoseaua Pandurilor, nr. 68-72, sector 5, Bucureşti
Telefon: (021) 319.56.49
Fax: (021) 319.55.93
B. 1291/2005 C. 308/2005