



## DIMENSIUNEA INFORMAȚIONALĂ A SPAȚIULUI DE LUPTĂ MODERN

### INFORMATIONAL DIMENSION OF THE MODERN BATTLE-SPACE

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

**Rezumat:** În lucrare autorul prezintă, pe scurt, unele aspecte mai importante ale „Dimensiunii informaționale a spațiului de luptă modern”, luând în considerație învățămintele desprinse din ultimele conflicte militare care au avut și au loc, în această perioadă, precum și realitățile, în domeniu, din unele armate moderne.

Sunt trecute în revistă principalele activități informaționale, definite procesele și mediile informaționale și prezentate calitățile și limitele sistemelor moderne de informații.

**Cuvinte-cheie:** resursă informațională, activități informaționale, procese și medii informaționale, C4I.

**Abstract:** In this paper the author briefly presents some of the main aspects of "Informational dimension of the modern battle-space" by taking into consideration the lesson learned from the late military conflicts that were taken and take place in the time being as well as the realities in the field of some modern armed forces.

Inhere, there are also presented some main informational activities, there are defined the informational processes and activities, there are reviewed the features and limits of the modern information systems.

**Keywords:** informational resource, informational activities, informational processes and environments, C4I.

Cele mai semnificative schimbări în evoluția umanității sunt cele determinate de apariția și dezvoltarea societății bazate pe informație, care netezesc calea spre globalizare. Internetul, sistemele informatice, tehnologia informației și comunicațiilor permit deja reducerea decalajelor existente, dezvoltarea economică, apariția unei industrii software românești, a infrastructurilor informaționale naționale, precum și integrarea mai accelerată în comerțul electronic și era digitală.

Trebuie remarcat că societatea informațională reprezintă, pe de o parte, o oportunitate, o cale de instruire și educație, iar pe de altă parte, un risc potențial, o

---

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



cale de amenințare și agresiune (A se lua act de intensul război informațional dus, în ultimul timp, de către Federația Rusă, inclusiv împotriva României). Informația a fost întotdeauna vizată de țări, lideri politici și comandanți militari. Revoluția tehnologică în domeniul comunicațiilor și informației a condus la creșterea importanței acesteia din urmă prin posibilitățile create de colectare, prelucrare, stocare sau diseminare, dar și de atac. În societatea informațională modernă se ignoră frontierele și se trece peste orice constrângeri de ordin spațial, temporal sau moral.

Sistemele și tehnologiile informaționale, echipamentele tehnice și software-ul aferent, atât de necesare sunt, în același timp, vulnerabile la penetrări neautorizate, la distrugeri și modificări accidentale sau voite, de date și programe. Tendința actuală privind amplificarea conectivității, în special la Internet și în rețele Intranet mărește riscul de vulnerabilitate, fiind tot mai greu să se localizeze un punct de acces ilegal în rețea sau un utilizator cu un comportament agresiv. Vulnerabilitatea sistemelor informaționale actuale poate antrena pierderi imense de ordin financiar sau de alt tip, direct sau indirect, prin „scurgerea” de informații confidențiale cu caracter personal, economic sau militar. Intensificarea atacurilor cibernetice din partea unor actori statali ar trebui să ne îngrijoreze.

Din punct de vedere tehnico-militar, importanța comunicațiilor și informațiilor constă, pe lângă valoarea lor indiscutabilă, în faptul că există mai multe ținte vulnerabile, accesibile rapid și pe scară largă care necesită tot mai multe mijloace și procedee de protecție. Armatele moderne și-au făcut din câștigarea bătăliei informaționale un obiectiv primordial al strategiei de dezvoltare. Baza câștigării acestei bătălie o reprezintă aplicarea cu succes a tehnologiei informaționale pe întregul spațiu de luptă, respectiv digitizarea spațiului de luptă și acțiunilor de natură informațională. Din punct de vedere tehnic, problemele referitoare la echipamente, tehnologii, proceduri, metodologii și algoritmi în cadrul operațiilor informaționale (ofensive și defensive) sunt posibile de realizat și controlat.

Conflictele de după cel de-al doilea război mondial, prin conținutul, obiectivele, amploarea și modalitățile de desfășurare care au beneficiat de realizările tehnicii și tehnologiilor proprii epocii informaționale - ale cărei contur se precizează tot mai mult - evidențiază în mare măsură ceea ce va fi definitiv pentru acțiunile militare ale viitorului precum:

- desfășurarea acțiunilor în toate mediile: pe uscat, în aer, pe apă, sub apă și în cosmos;
- utilizarea de forțe și mijloace diversificate, cu o mare mobilitate, putere de foc, bătaie, precizie, efect de nimicire și distrugere;



- folosirea unor arme și sisteme de armament foarte performante și cu precizie deosebită;
  - transparența spațiului de luptă datorită conjugării activității sateliților de observație, radarelor aeropurtate și mijloacelor de detecție prin contact - active și pasive;
  - lovituri aplicate atât la contact cât și în adâncime, concomitent cu existența unor măsuri de protecție eficiente;
  - dispersarea și concentrarea rapidă de forțe și mijloace;
  - existența spațiului comun de dispunere și de manevră pentru adversarii care se confruntă;
  - spațiul de luptă suprasaturat de mijloace electronice;
  - mare consum de muniție, carburanți și alte resurse, uriașe pierderi materiale (căi și noduri de comunicații, lucrări de artă), dislocări însemnate de populație pe criterii etnice, religioase etc.;
  - tendința de a se evita confruntările directe, frontale, dintre forțe și mijloace numeroase, accentul punându-se pe acțiunile duse de formațiuni mici, cu o mare putere de foc, autonomie relativă în acțiune, o mare diversitate de procedee tactice. În special la flancuri, în intervale și în adâncimea dispozitivului adversarului; angajarea în luptă a unor adevărați profesioniști.
  - utilizarea tehnicilor și procedeelelor așa zisului „război hibrid” (a se studia cazul conflictului din Ucraina cu implicarea majoră, neasumată de către Federația Rusă). Este cazul aici să se identifice și să se ia din timp măsuri de contracarare.
  - analiștii militari apreciază că războaiele viitoare vor avea un caracter integrator, în sensul participării la conflict a tuturor categoriilor de forțe ale armatei care vor acționa în toate mediile. La acestea se adaugă cele cosmice de observare, dirijare și comunicație.
- În războiul viitorului, spațiul de luptă cibernetizat va deveni o realitate. Acest fenomen ridică, între altele, două aspecte cu semnificații aparte:
- integrarea procesului de informatizare a comenzii trupelor cu sistemele de armament, apariția și utilizarea roboților, vehiculelor telecomandate și munițiilor inteligente;
  - metodologia lucrului în condițiile cibernetizării, elaborarea scenariilor tactice și operative specifice și, mai ales, a desfășurării unor acțiuni de luptă cu utilizarea simultană a trupelor și a elementelor prin care se monitorizează activitatea adversarului, reacțiile trupelor proprii, influența condițiilor de mediu, oportunitatea și eficacitatea deciziilor elaborate.
  - necesitatea identificării din timp și luarea unor măsuri concrete pentru continuarea comenzii și controlului forțelor militare în cazul căderii mijloacelor automatizate (sistemelor C4ISR).



Lupta modernă, dusă de unități de diferite tipuri, necesită preluarea și transferul rapid al informațiilor în întregul spațiu de luptă.

Spațiul de luptă cibernetizat dezvăluie deja suficiente elemente care-l conturează și-i conferă numeroase posibilități de dezvoltare precum:

- ⇒ multitudinea sistemelor automatizate și de armament;
- ⇒ realizarea coordonării unor diverse categorii de forțe și armament în luptă, în condițiile impuse de comprimarea timpului operativ;
- ⇒ multifuncționalitatea forțelor luptătoare pe timpul desfășurării ofensivei, cât, mai ales, pe timpul apărării;
- ⇒ conservarea forțelor umane și folosirea lor numai în situații deosebite sau pentru consolidarea succeselor;
- ⇒ compensarea limitelor fiziologice ale comandanților, luptătorilor și operatorilor prin utilizarea sistemelor automatizate de luptă;
- ⇒ folosirea roboților pentru activități care cer eforturi mari, timp îndelungat, sacrificii sau acțiuni în condiții complexe.

Referitor la fizionomia viitoarelor războaie, analiștii militari occidentali au definit următoarele cinci tendințe: letalitate și dispersare crescute; volum și precizie a focului mărite; integrarea masivă a tehnologiilor noi; realizarea unui efect distructiv mai mare; perfecționări în asigurarea invizibilității mijloacelor și în detectarea obiectivelor.

De asemenea, are loc o redimensionare a noțiunii de conflict prin adăugarea unor noi atribute:

- ⇒ *permanența* - aplicarea unei strategii globale care integrează permanent toate procesele informaționale, nu numai în perioadele de criză sau conflict;
- ⇒ *transversalitatea* - influențarea societății în ansamblul ei și fundamentarea pe multidisciplinaritate și conceptele de integrare a sistemelor;
- ⇒ *dualitatea* — dispariția deosebirilor dintre sfera militară și cea civilă (la nivel național, centrul de greutate se mută spre alte domenii - bancar, financiar, energetic, în general spre infrastructura civilă a cărei apărare, cu forțe și mijloace convenționale, devine foarte dificilă).

**Resursa informațională este principala categorie de resurse a războiului modern și vizează următoarele domenii:**

- politic, economic, social și militar necesare comenzii și controlului la nivel strategic;
- capacitatea militară a potențialilor adversari și dinamica pregătirilor pentru război;
- doctrinele militare, organizarea și pregătirea strategică a sistemelor militare, a teritoriului, economiei și populației pentru apărare;



- posibilitățile sistemelor de armament și tehnicii de luptă, utilizarea și integrarea acestora în concepțiile de ducere a războiului;
- activitatea de cercetare științifică dedicată apărării;
- orientarea mass-mediei și reacția populației față de conflictele militare (Evenimentele din ultimii doi ani demonstrează efectul pervers al războiului mediatic asupra unui segment important al populației, ușor de influențat, datorită nivelului scăzut de informare corectă);
- sfera și structura informațiilor de comandă, cooperare și înștiințare, organizarea și utilizarea sistemelor informaționale;
- caracteristicile generale, utilizarea și evaluarea rezistenței sistemelor criptografice;
- capacitatea de contracarare a acțiunilor de spionaj, diversiune, teroriste și prin răspândirea știrilor false;
- nivelul de pregătire și moralul trupelor;
- informațiile generale de natură politică, economică, financiară, socială, diplomatică etc.

**Tehnologia informației și comunicațiilor oferă** posibilitatea de informare în timp real, afectează opinia publică națională și mondială, modelează acțiunile politicianilor și produce o întrepătrundere accentuată a nivelurilor tactic, operativ și strategic. Se relevă tot mai clar că o clasă politică lacomă și imposibilă poate fi un factor major de vulnerabilitate a unui stat.

Comandanții de la orice nivel trebuie să fie conștienți că într-o lume a comunicațiilor directe, în timp real, orice eveniment izolat poate fi cunoscut simultan la toate cele trei niveluri.

În armata secolului, la începutul căruia suntem, operațiile militare se vor baza pe cunoașterea rezultată din date și informații precise, exacte și relevante, culese, analizate și difuzate printr-un „sistem de sisteme” tehnice.

Sistemele informaționale integrate de tip C4I (Comandă, Control, Computere, Comunicații și Informații) vor asigura comandanților posibilități de a vedea, simți, interpreta, decide și angaja acțiuni în orice punct al fâșiei de acțiune sau în zona de responsabilitate informațională (informativă).

Era informațională are drept conținut creșterea explozivă a utilizării informaticii, comunicațiilor și mijloacelor de luptă cibernetizate, informația devenind obiectul, mijlocul și procedura unui nou domeniu de acțiune - cel informațional. Dacă aceste acțiuni sunt desfășurate la momentul oportun și cu succes, ele pot preveni conflictele, reduce pierderile sau stabiliza rapid condițiile de desfășurare a acțiunilor militare.

Din păcate, în prezent nu există o deplină înțelegere a faptului că dimensiunea informațională nu este una fabricată, ci este cât se poate de reală și de



actuală. Totodată, informația nu este percepută la adevărata ei identitate: ca armă, factor de risc, instrument operațional și tehnologic.

Principalele caracteristici ale acțiunilor informaționale sunt următoarele:

➤ volumul informațiilor necesare elaborării deciziilor și ducerii acțiunilor militare sporesc de 10-15 ori și mai mult față de cel vehiculat în al doilea război mondial;

➤ crește posibilitatea de informare și, ca urmare, mijloacele specifice devin din ce în ce mai performante;

➤ influența benefică a prelucrării informațiilor asupra capacității sistemelor de armament, dar și cea nefastă a dezinformării sau a virușilor informatici asupra proceselor specializate realizate cu calculatoare și software adecvat;

➤ creșterea explozivă a cantității de informație necesare luptătorului pentru a face față solicitărilor din spațiul de luptă modern;

➤ integrarea și utilizarea armamentului și tehnicii de luptă inteligente;

➤ dezvoltarea și perfecționarea structurilor specializate pentru asigurarea securității informațiilor;

➤ caracterul cibernetic al acțiunilor militare și apropierea tehnologică și informațională dintre comandă și execuție;

➤ unele dificultăți în precizarea adversarilor;

➤ multitudinea țintelor vizate;

➤ absența unor indicatori specifici și clari de avertizare;

➤ persistența efectelor și lipsa unor metode rapide de remediere a consecințelor pe care le generează;

➤ utilizarea unor tehnologii relativ simple, ieftine și larg răspândite;

➤ dispariția deosebirilor dintre nivelurile de comandă.

### **Principalele activități informaționale**

Lucrările de specialitate definesc principalele concepte utilizate în acest domeniu, astfel:

➤ *datele* - fapte individuale sau statistice într-o formă necorelată;

➤ *informația* - o comunicare, veste, știre care pune pe cineva la curent cu o situație;

➤ *cunoștințele* - rezultat al prelucrării informațiilor, proces în care intervin intuiția și gândirea umană.

Există și patru stadii cheie ale ciclului de viață al informației: crearea, culegerea, diseminarea și utilizarea ei. Aceste stadii sunt distincte, deși au multe caracteristici în comun.

Dezvoltarea tehnologică a afectat viteza și volumul culegerii și diseminării informației.



Revoluția informațională a condus la dezvoltarea unor sisteme moderne interconectate și interdependente, care nu mai pot fi conduse manual.

Informația, ca un bun militar strategic, a fost întotdeauna recunoscută ca atare de către comandanți, mai ales în ideea unei bune cunoașteri a intențiilor adversarului și, în același timp, a unei protecții proprii, a planurilor și stadiului operațional al acțiunilor militare. Dacă această informație este disponibilă în domeniul militar, de la nivelul strategic de comandă la comandanții de la nivel tactic, pot apărea o serie de probleme în privința încrederii acestora în integritatea, relevanța și acuratețea informației prezentate.

Activitățile informaționale din spațiul de luptă modern implică obținerea, transportul, prelucrarea, conversia, distribuția, utilizarea, protecția, exploatarea și managementul informațiilor, succint conținutul lor constând în:

❖ **Colectarea** - achiziția și filtrarea inițială a datelor pe baza nevoilor planificate și prezentarea lor într-o formă adecvată transmierii. Aceste informații vizează misiunea, adversarul, trupele proprii, terenul, starea vremii și timpul la dispoziție. Procesul de obținere a informațiilor se realizează cu ajutorul sistemelor electronice, al activităților operative de cercetare și recunoaștere, al cercetării strategice, operative și tactice, prin conlucrarea cu organele de poliție și mass-media etc.

❖ **Transportul** - comunicarea informațiilor și a datelor la dispozitivele de recepție ale destinatarilor.

❖ **Prelucrarea datelor** - stocarea, extragerea din dispozitivele de memorie, actualizarea, filtrarea și sinteza lor pentru a rezulta minimum de informații într-o formă utilizabilă.

❖ **Conversia informațiilor** - transformarea acestora dintr-o formă în alta fără pierderi și fără modificarea preciziei lor în scopul transmierii și afișării sub formă de text, de imagini în format fix și în mișcare, de date pentru calculatoare etc.

❖ **Distribuția (diseminarea) informațiilor** - transmiterea informațiilor prelucrate potențialilor utilizatori.

❖ **Utilizarea informațiilor** (după ce datele sunt obținute, analizate și verificate) - actualizarea și cunoașterea situației reale pentru a perfecționa continuu sau pentru a adapta deciziile, planurile și acțiunile militare.

❖ **Protecția informațiilor** - analiza vulnerabilității forțelor și mijloacelor proprii de comandă și control la acțiunile de natură electronică, de distrugere fizică, inducere în eroare, și de propagandă ale adversarului precum și stabilirea mijloacelor, aplicarea și verificarea măsurilor de contracarare. Elementele de infrastructură ce trebuie protejate sunt bazele de date, rețelele de calculatoare, sistemele de comunicații, de cercetare și mijloacele auxiliare din cadrul acestora.



❖ **Exploatarea informației** - acțiunea prin care se obțin avantaje pentru scopurile operaționale militare din orice informație achiziționată. Aceasta implică interceptarea și analiza mesajelor adversarului, extragerea informațiilor din bazele lui de date, întreprinderea măsurilor de denaturare, degradare sau manipulare a capacităților informaționale ale acestuia.

❖ **Denaturarea informațiilor adversarului** - măsurile de atac la adresa comenzii și controlului vizând influențarea, degradarea sau distrugerea informației și a sistemelor informaționale (C4I) ale acestuia.

❖ **Managementul informației** - coordonarea și sincronizarea atenției a informației și a sistemelor informaționale (C4I) și cuprinde: managementul spectrului electromagnetic, alegerea surselor și a sistemelor ce se utilizează, asigurarea unor fluxuri informaționale fiabile (cu integrarea pe verticală și orizontală), interceptarea informațiilor de la mai multe surse.

#### **Procese și medii informaționale**

Pentru analiza pertinentă a dimensiunii informaționale a spațiului de luptă modern este foarte util să caracterizăm succint mediile informaționale care au un impact important asupra organizării și desfășurării acțiunilor militare, astfel:

❖ **mediul informațional global** - cuprinde personalitățile, organizațiile, sistemele etc., multe dintre ele în afara controlului militar sau al autorităților naționale de comandă, care colectează, prelucrează și distribuie informațiile la nivel național și internațional;

❖ **infrastructura informațională națională** - cuprinde rețelele de telecomunicații publice și private, tehnologiile de satelit, terestre și radio care deservește persoanele fizice și juridice, informațiile și conținutul acestora, bazele de date, terminalele hardware și produsele software pentru accesul la informații, personalul care colectează, prelucrează, stochează și generează noi informații etc.;

❖ **infrastructura informațională a apărării** - cuprinde resursele necesare pentru transferul, prelucrarea, stocarea și afișarea informațiilor, mijloacele tehnice pentru comandă și control, cercetare și alte categorii de mijloace pentru transmiterea vocii, imaginilor fixe și în mișcare, servicii multimedia deosebit de utile domeniului militar;

❖ **mediul informațional militar** - constă din sistemele informaționale și structurile proprii și ale adversarului, militare și de alte categorii, care sprijină sau influențează în mod semnificativ operațiile militare;

❖ **sistemele informaționale (C4I)** - constau din infrastructura, structurile, personalul și componentele care colectează, prelucrează, stochează, transmit, afișează, distribuie și acționează în conformitate cu informațiile obținute.





Dezvoltarea intensivă a tehnologiei informației și comunicațiilor a creat noi procedee de gestionare și prelucrare a datelor. Acestea includ imagini, grafică, scheme, hărți digitizate, baze de date care se combină cu tehnici moderne de comunicații (sateliți, stații radio cu salt de frecvență, radiorelee pe microunde, stații radio troposferice și ionosferice) și asigură infrastructuri globale, naționale și militare.

### ***Sisteme moderne de informații***

La baza funcționării sistemului de comandă și control stau informațiile despre evenimente, mediu, adversar și trupele proprii, care influențează sau pot afecta acțiunile militare și care în urma proceselor de prelucrare, analiză, stocare și valorificare fundamentează decizia și contribuie substanțial la obținerea supremației informaționale.

„Supremația informațională - reprezintă gradul de dominare informațională care oferă personalului posibilitatea de a utiliza sistemele informaționale (C4I) pentru a obține avantaje operaționale în conflict sau pentru a controla o anumită situație, concomitent cu reducerea posibilităților adversarului de a utiliza informațiile necesare proceselor similare pentru trupele sale”<sup>1</sup>.

Realizarea superiorității informaționale cuprinde două componente egale ca importanță - acumularea și protecția capacităților informaționale proprii și degradarea capacităților informaționale ale adversarului.

### **Superioritatea informațională depinde de:**

- capacitatea de a accesa o cantitate mare de informații din mai multe surse și medii (politic, social, economic, militar, religios etc.), cu privire la adversar și la trupele proprii, informații necesare în zona de responsabilitate a actului de comandă și control;
- reducerea posibilităților de utilizare a informațiilor false sau cu valoare de interes nulă, prin folosirea unor tehnici și proceduri eficiente de culegere și autentificare;
- performanțele sistemelor de senzori de a culege, a prelucra și de a transmite pe canale de comunicații informații în diferite formate;
- capacitatea sistemelor de comunicații de a vehicula, în timp scurt, întregul flux de informații, atât pe verticală, cât și pe orizontală;
- capacitatea organelor de comandă de a utiliza informațiile în elaborarea deciziilor astfel încât să devanseze acțiunile probabile ale adversarului;
- nivelul de protecție și de securitate a datelor și informațiilor cu privire la trupele proprii și acțiunile acestora.

---

<sup>1</sup> Joint Doctrine for Operations Security, Department of Defense, Washington, DC, 1994, p. 63.



Asigurarea superiorității informaționale se realizează prin mai multe procedee, astfel:

⇒ creșterea fluxului prin utilizarea sistemelor de comunicații cu topologie, folosirea unităților speciale, a ofițerilor și a echipelor de cercetare. Inovațiile din sistemele de senzori, procesoare, comunicații și calculatoare pot oferi comandamentelor o bună cunoaștere a situației operative prin accesul imediat la informațiile despre adversar și trupele proprii;

⇒ „vizualizarea” spațiului de luptă prin cunoașterea situației curente a trupelor proprii în conexiune cu cea a adversarului și cu condițiile de mediu;

⇒ proiectarea situației finale dezirabile - îndeplinirea misiunii - vizualizarea secvențială a activităților pe care forțele proprii le îndeplinesc, din situația inițială până la cea finală;

⇒ cunoașterea situației prin analiză, însușirea intenției comandantului și concepției luptei (operației) în legătură nemijlocită cu dispunerea și posibilitățile adversarului și ale forțelor proprii;

⇒ managementul permanent al informațiilor, în condițiile colectării și prelucrării unor cantități foarte mari de informații, reducerea duratei ciclului de comandă, elaborarea deciziilor în timp scurt.

Esențială pentru asigurarea și exploatarea superiorității informaționale este materializarea conceptului care evidențiază „acțiunile de atac orientate pe centrele rețelei informaționale”<sup>2</sup>.

Acest concept este aplicabil la toate nivelurile ierarhice și contribuie la întrepătrunderea strategiei, a artei operative și a tacticii. Acesta își găsește substanțialitatea în integrarea și coordonarea unor forțe bine informate și logic dispersate în spațiul de luptă.

Elementele care contribuie la realizarea acestui deziderat sunt trei<sup>3</sup>:

⇒ rețea informațională (C4I) cu performanțe superioare care rezistă și supraviețuiește întregii game de amenințări fizice și operații informaționale;

⇒ sistemele de senzori capabile să realizeze un înalt nivel de cunoaștere a spațiului de luptă sincronizat cu desfășurarea operațiilor militare;

⇒ îmbunătățirea capacității de exploatare a forțelor și mijloacelor prin rețelele de angajare moderne și eficiente (asigurarea unor noi capacități operaționale pentru planificarea preventivă, managementul integrat al forțelor, micșorarea timpului de atac al țintelor).

<sup>2</sup> John Garstka, *Information and Network – Centric Warfare*, J 6 Presentation, Washington, DC, 1998, p. 4.

<sup>3</sup> *Joint Vision 2010*, Department of the Army, Washington, DC, 1998, p. 36.



Mulți specialiști cred că deplasarea fundamentală de la acțiunile bazate pe platforme spre cea pe centre, cu superioritatea informațională, constituie o revoluție în domeniul militar și se află în centrul acestui proces de transformare.

Perfecționările tehnologice au dus la creșterea considerabilă a calității, preciziei și oportunității informațiilor puse la dispoziția compartimentului informații, precum și a produselor informative destinate utilizării de către comandant.

Toți ofițerii de stat major trebuie să înțeleagă principiile și tehnicile activității informaționale dacă se urmărește ca planurile să fie realiste. În același timp, este important să reținem faptul că informațiile oferite de personalul din compartimentul informații sunt rezultatul unei analize fundamentate atât pe datele avute la dispoziție, cât și alți factori fie variabili, fie doar presupuși.

**Pentru facilitatea înțelegerii problematicii specifice trebuie cunoscuți termenii uzuali folosiți în domeniul informativ:**

⇒ *datele* - materiale specifice neevaluate rezultate din diferite descrieri care pot fi utilizate în realizarea produselor informative;

⇒ *informația* - rezultatul prelucrării datelor;

⇒ *produsul informativ* - rezultatul obținut în urma analizei și prelucrării informațiilor;

⇒ *sursă* - o persoană sau un obiect de la care pot fi obținute informații;

⇒ *agenția* - structură organizatorică sau persoană angajată în colectarea și/sau prelucrarea informațiilor pentru scopuri informative;

⇒ *supravegherea* - observarea sistematică;

⇒ *zona de influență* - spațiul geografic în interiorul căruia comandantul este implicat nemijlocit în influențarea acțiunilor militare prin manevră și sisteme de sprijin cu foc aflate sub comanda și controlul lui;

⇒ *zona de responsabilitate informativă* - spațiul geografic alocat unui comandant în care acesta este responsabil pentru asigurarea informațiilor, utilizând mijloacele la dispoziție;

⇒ *zona de interes informativ* - spațiul geografic despre care un comandant cere informații privind factorii care pot afecta acțiunile militare, prezente și viitoare, și evoluția acestora.

Unele valori privind zone de responsabilitate tactice menționate sunt prezentate în tabelul următor<sup>4</sup>.

---

<sup>4</sup> *Intelligence Handbook*, Romania and UK, Regional Training Centre, Bucharest, 1998, p. 1-2.



Nr. crt.	Marea unitate, unitate sau formațiune	Zona de influență (km)	Zona de responsabilitate informativă (km)	Zona de interes informativ (km)
1.	Batalion	0-6	0-6	0-20
2.	Brigadă mecanizată	0-20	0-12	0-50
3.	Divizie mecanizată	0-30	6-50	0-150
4.	Corp de armată	0-100	50-150	0-250

Ciclul informativ cuprinde mai multe etape<sup>5</sup>:

- *Cerințele informaționale* ale comandantului asigură orientarea, planificarea și conducerea activităților informative, curente și viitoare, în acord cu prioritățile stabilite de către acesta.

- *Colectarea* reprezintă etapa în care datele și informațiile sunt exploatate și livrate statului major pentru a fi analizate și pentru a obține produsele informative dezirabile.

- *Prelucrarea și exploatarea informațiilor* reprezintă procesele prin care datele (informațiile) colectate sunt evaluate, analizate și transformate în produse informative care se utilizează în procesele informațional-decizionale.

- *Realizarea produselor informative* constă în colectarea, evaluarea, analiza, integrarea și interpretarea informațiilor dintr-una sau mai multe surse, cu scopul obținerii unui produs final. Constrângerile de timp și evoluțiile din spațiul de luptă modern determină întrepătrunderea tot mai consistentă a fazelor de prelucrare și sinteză.

- *Distribuția și integrarea produselor informative* se realizează prin transmiterea acestora organelor care le-au solicitat pentru a fi utilizate în procesul de elaborare a deciziei și de planificare a acțiunilor militare. Personalul din compartimentele de informații de la toate nivelurile evaluează desfășurarea ciclului informativ și rezultatele obținute.

*Sistemul de informații* ca element component al sistemelor C4I, este reprezentat de ansamblul constituit de personalul, mijloacele, procedurile și tehnicile prin care se obțin și se prelucrează datele, prin care se transmit informațiile și produsele informative compartimentelor și persoanelor implicate în procesele de comandă și control. Rezultă că un ciclu informativ începe prin formularea cerințelor specifice din procesele de comandă și control și se încheie cu

<sup>5</sup> JP 2-01, *Joint Intelligence Support to Military Operations*, Joint Staff, Washington, DC, 1996, Cap. II, p. 1-3.



furnizarea produselor informative. De asemenea, trebuie remarcate interdependențele și corelațiile strânse ale sistemului de informații cu celelalte subsisteme componente din sistemele C4I: cel de comandă și control, rețelele de calculatoare, sistemele de comunicații, sistemele de armament etc.

*Recunoașterea spațiului de luptă* implică misiuni pentru a obține, prin observare vizuală sau prin alte metode de detecție, informații despre activitățile și resursele adversarului, precum și despre caracteristicile meteorologice, hidrografice și geografice ale unei zone bine definite.

*Supravegherea spațiului de luptă* reprezintă observarea sistematică a acestuia pentru a se asigura informații oportune privind desfășurarea acțiunilor de luptă.

După modul de proveniență a datelor și informațiilor, sursele pot fi constituite din: cercetarea semnalelor electromagnetice; elemente umane și organe diverse; cercetarea prin satelit.

*Cercetarea semnalelor electronice* urmărește descoperirea, localizarea și evaluarea radiațiilor electromagnetice de toate categoriile și cuprinde:

❖ cercetarea comunicațiilor - care vizează căutarea, interceptarea, localizarea, analiza și exploatarea traficului radio al adversarului, asigurând evaluarea pe această bază a dispunerii, deplasărilor și intențiilor forțelor acestuia;

❖ cercetarea electronică - care cuprinde activitățile de culegere și de prelucrare a radiațiilor electromagnetice potențial ostile (cu excepția celor ale mijloacelor de comunicații), emenate de exploziile nucleare și sursele radioactive.

*Cercetarea executată de oameni* și organele specializate acoperă toate aspectele specifice, ca de exemplu: interogarea prizonierilor; observarea activității adversarului; patrulare; detașamente etc.

*Cercetarea imagistică* include formele de cercetare obținute prin fotografiere, observare termică și alte echipamente care captează imagini.

*Cercetarea acustică* obține date prin colectarea și analizarea fenomenelor acustice. Sensorii utilizați în acest scop pot fi pasivi (recepționează zgomotele) sau activi (transmit unde acustice pulsatorii și ulterior recepționează ecoul). Sursele de cercetare acustică pot fi staționare sau instalate pe nave, platforme plutitoare, în imersiune sau pe fundul mării.

*Sursele de informații* pot fi: subunități de cercetare (puncte de observare, patrulare și detașamente de cercetare), subunități de cercetare ale armelor, avioane, elicoptere și avioane fără pilot, mijloace de natură electronică, prizonieri și refugiați.

*Agențiile* sunt asimilate cu: structurile de informații (informații, artilerie, geniu); operații, aviație și sisteme de cercetare electronică; elemente de cercetare în dispozitivul adversarului; structurile care interoghează prizonieri etc.



*Tehnicile utilizate* în supravegherea spațiului de luptă modern vizează<sup>6</sup> modul de utilizare de către adversar a spectrului electromagnetic: În infraroșu - imaginile obținute prin recepția radiațiilor emise sau reflectate de suprafața obiectivelor în segmentul de la 0,72 la 1  $\mu\text{m}$ ; imagini termice radiate în infraroșu care pot distinge diferențe de 0,1°C. Aceasta permite ca țintele să fie detectate sub formă de imagini prin vizualizarea sau monitorizarea cu televizorul; vizual, inclusiv fotografia; în ultraviolet prin reflexia radiațiilor în acest domeniu; diverse tipuri de radiolocateare; exploatarea undelor acustice sau seismice.

Eficiența acestor tehnici poate fi îmbunătățită prin: utilizarea platformelor aeriene cu și fără pilot capabile să asigure informații de timp aproape real până la comandamentele tactice; utilizarea senzorilor tereștri; prelucrarea semnalelor.

Aceste sisteme tehnice pot fi active sau pasive. Sistemele active radiază energie spre țintă cu scopul de a o ilumina și de a o descoperi. Sistemele pasive recepționează energia radiată de către țintă.

Unele limitări în utilizarea acestor tehnici sunt determinate de vizibilitatea directă spre țintă, de condițiile atmosferice și meteorologice, de caracteristicile țintei (mărimea, capacitatea de a reflecta sau radia energia) și contrastul acesteia cu mediul ambiant, precum și de unele contramăsuri specifice (mascare, furnizare, tăcere radio, inducerea în eroare, restricții în manevră).

*Instrumentele optice* sunt pasive, ieftine, ușoare și fiabile, dar sunt ineficiente pe timp de noapte. Aceste sisteme amplifică lumina ambientului cu mijloace electronice, astfel încât observatorul poate vedea ținte slab luminate.

*Laserii* sunt sisteme active și au două aplicații: de descoperire cu o precizie de  $\pm 5$  m până la distanță de 20 km; marcarea țintelor prin iluminarea acestora.

*Radarele* transmit un impuls electromagnetic care este reflectat de țintă și recepționat din nou de radar. Unele radare detectează deplasarea autovehiculului până la 24 km și a oamenilor până la 3 km.

Dispozitivele de alarmare funcționează pe bază de senzori seismici sau în infraroșu.

*Cercetarea în dispozitivul adversarului* se realizează cu mijloace pentru distanțe medii (6-50 km) și mari (peste 50 km).

Mijloace eficiente de cercetare sunt și sateliții care realizează fotografierea și cercetarea prin radiolocație etc.

Din punctul de vedere al funcționării eficiente a sistemelor de cercetare se impune, dacă se poate în timp real, utilizarea unor mijloace tehnice specializate

<sup>6</sup> JSP 120 (3) *Manual of Service Intelligence*. Department of Defence, United Kingdom of Great Britain, London, 1997, p. 39.



performante, interfețe de adaptare a senzorilor cu canalele de comunicații digitale cu mare viteză de transmitere și precizie maximă.

De asemenea, compartimentul informații trebuie să dispună de mijloace tehnice de automatizare (calculatoare performante) și software specializat care să permită prelucrarea datelor și a informațiilor în timp oportun, creșterea nivelului de informare a comandamentelor și reducerea nivelului de risc al managementului informațional.

Am încercat în această primă parte să readuc în atenția celor interesați de probleme militare, unele aspecte ale rolului și locului, sistemelor informaționale actuale în războiul modern luând act și de evoluțiile și învățămintele desprinse din ultimele conflicte, inclusiv din criza ruso-ucraineană. Îmi propun dacă se va putea, să continui, într-un viitor număr al revistei, cu celelalte elemente componente ale sistemelor informaționale, analizate prin prisma unor informații recente.



## BIBLIOGRAFIE

- \*\*\* Legea privind protecția informațiilor clasificate, nr. 182/2002, M. Of. 248/2002.
- \*\*\* Legea privind securitatea națională a României, nr. 51/1991, M. Of. 163/1992.
- \*\*\* Securitatea informațiilor, Centrul de Expertiză în Domeniul Securității, București, 2008.
- \*\*\* Sisteme informaționale – Sesiunea anuală de comunicări științifice cu participare internațională, Editura UNAp, București, 2007.
- \*\*\* Joint Doctrine for Operations Security, Departament of Defense, Washington, DC, 1994.
- \*\*\* *Joint Vision 2010*, Department of the Army, Washington, DC, 1998.
- \*\*\* *Intelligence Handbook*, Romania and UK, Regional Training Centre, Bucharest, 1998.
- \*\*\* *JP 2-01, Joint Intelligence Support to Military Operations*, Joint Staff, Washington, DC, 1996, Cap. II.
- \*\*\* *JSP 120 (3) Manual of Service Intelligence*. Department of Defence, United Kingdom of Great Britain, London, 1997.
- ALBERTS, Davids S., Richard E. HAYES, *Planning – Complex Endeavours*, CCRP.



- ALEXANDRESCU C. și alții, *Supremația electromagnetică*, Editura UNAp, București, 1999.
- ALEXANDRESCU C., *Amenințări informaționale asupra sistemelor de comandă și control în acțiunile militare moderne "SI-2007"*.
- ALEXANDRESCU C., TEODORESCU C., *Războiul electronic contemporan*, Editura Sylvi, 1999.
- ALEXANDRESCU Constantin, ILINA Decebal, MINCU Constantin, *Bazele matematice ale organizării sistemelor de transmisiuni*, Ed. Militară, București, 1994.
- ALEXANDRESCU Constantin, ALEXANDRESCU Gelu, BOARU Gheorghe, „*Sistemele Informaționale Militare*” – *servicii și tehnologie*, Editura UNAp „Carol I”, București, 2010.
- DUMITRU Cristea, prof. univ. dr., *Infrastructura de rețea și informațională în cadrul războiului bazat pe rețea*, Editura CTEA, București, 2008.
- DUMITRU Cristea, prof. univ. dr., *Sisteme C4I*, Editura Militară, București, 2005.
- EUROCOM D/1 Tactical Communications Systems. Basic Parameters, 1986.
- FRIEDMAN George, fondatorul STRATFOR, „*România trebuie să învețe să fie mai periculoasă pentru a exista, să fie un risc pentru ruși, germani și de ce nu, americani*”, interviu NotNews.ro, 16 noiembrie 2010, București.
- FM 34-1 Intelligence and Electronic Warfare Operations, Headquarters Department of the Army, Washington DC.
- GARSTKA John, *Information and Network – Centric Warfare*, J 6 Presentation, Washington, DC, 1998.
- MINCU Constantin, dr., GREU Victor, dr., ROTARIU Costel, ing., *Salt de frecvență și contrasalt de frecvență*, Editura Militară, București, 1998.
- MINCU Constantin, dr., TIMOFTE Gruia, dr., *Compatibilitatea Sistemelor Radioelectronice*, Editura Olimp, București, 1999.
- MUREȘAN M., VĂDUVA Gh., *Războiul viitorului, viitorul războiului*, Editura UNAp, București, 2005.
- PÂRLOG Nicu, Armele Viitorului, <http://us.mg6.mail.yahoo.com>.
- Serviciul Istoric al Armatei – *Enciclopedia Armatei României*, colectiv de autori, Editura CTEA, București, 2009.
- Simpozionul Jubiliar AFCEA, Washington DC, 18-19 Iunie 2006.
- TOFFLER Alvin și Heidi, *Război și anti-război*, Editura Antet, București, 1995.





TOFFLER Alvin, *Powershift, puterea în mișcare*, Editura Antet, București, 1995.

**Reviste de specialitate**

Gândirea Militară Românească, anii 2001-2015

Buletinul Universității Naționale de Apărare “Carol I”, 2008-2015

Revista Forțelor Terestre, anii 2005-2015

Impact Strategic, anii 2006-2015

Revista de științe militare, anii 2006 – 2015

Romanian Military Thinking Journal, anii 2005 – 2015

Revista comunicațiilor și informaticii nr. 2 (10)/2009 – număr special

Revista comunicațiilor și informaticii – număr special, 14 iulie 2008

