



# CONCEPTUL DE OPERARE ISR

## ISR OPERATION CONCEPT

Lt.col.drd. Florin ALEXANDRU\*

Secolul XXI a adus în atenția strategilor militari provocarea anticipării viitoarelor conflicte militare atât din punct de vedere al introducerii în luptă a noilor echipamente, ca de exemplu, dronele independente sau comandate de la sol, dar mai ales din punct de vedere al actualizării vechilor tactici în contextul modernizării și globalizării conflictelor militare. În esență, conflictele militare au avut și vor avea ca element de bază informația și rezultatul folosirii informației.

*The 21st century has brought to the attention of military tacticians the challenge of anticipating future military conflicts, related to new weapons, like autonomous or controlled from the ground drones, but especially related to the updating of the old strategies in the context of the modernization and globalization of military conflict. Basically, military conflicts had and will have as starting point intelligence and the result of using intelligence.*

**Cuvinte-cheie:** conceptul ISR (informații, supraveghere, recunoaștere); ISTAR; securitate; avertizare.

**Keywords:** ISR concept (Intelligence, Surveillance, Reconnaissance); ISTAR; security; warning.

Eficiența sprijinului cu informații în operațiile militare întrunite, în condițiile integrării depline a Armatei României în structura NATO, este determinată, într-o mare măsură, de interoperabilitatea și de compatibilitatea cu structurile militare din armatele celorlalte țări aliate.

În conformitate cu Strategia Militară a României din 2007 și pentru ca forțele și mijloacele puse la dispoziția NATO pentru apărarea colectivă să fie eficiente, se impune o nouă arhitectură a structurilor de informații/supraveghere/cercetare, care să fie în conformitate cu ultimele concepte ale Alianței. Cantitatea crescândă de informații necesare sprijinului de informații al operațiilor a impus conceptul unui sistem integrat de lucru al tuturor senzorilor. Astfel, dacă la nivelul structurilor de conducere s-a implementat conceptul ASIC (All Sources Information Cell), la nivelul structurilor de execuție trebuie implementat conceptul IS(TA)R.

„Într-un astfel de context tensionat și complex, securitatea fiecărei țări, precum și a comunității internaționale în ansamblu, depinde nu atât de capacitatea de reacție și adaptare cât, mai ales, de capacitatea de anticipare și de acțiune proactivă.

Într-o lume complexă, dinamică și conflictuală, aflată în plin proces de globalizare, înțelegerea profunda a tendințelor majore de evoluție a lumii și a modului în care fiecare țară are șansa să devină parte activă a acestui proces este o condiție esențială a oricărui progres”<sup>1</sup>.

Informații, Supraveghere, (Identificarea, Selectarea și Combaterea Țintelor), Cercetare – IS(TA)R reprezintă culegerea, procesarea și diseminarea coordonată, periodică, precisă, oportună și sigură a datelor și informațiilor primare/brute (Information) și a informațiilor prelucrate (Intelligence) în sprijinul operațiilor întrunite. Pentru o înțelegere exactă a ceea ce se dorește a fi capacitatea ISR, cele trei componente (intelligence, surveillance și reconnaissance) nu trebuie privite separat, ci ca un sistem unitar de colectare de date și informații despre un adversar, sau potențial adversar, care vor fi aduse la cunoștința factorului de decizie militar sau/și politic, indiferent la ce nivel este situat acesta.

În ansamblu, capacitatea ISR reprezintă un sistem de sisteme care trebuie să ofere o perspectivă globală asupra amenințării, să fuzioneze toate tipurile de informații într-o singură imagine comună completă, să permită accesul la informații detaliate despre inamic și să monitorizeze ținte specifice pentru perioade lungi de timp.

\*Ministerul Apărării Naționale  
e-mail: florin19al@yahoo.com



Definirea conceptului de sistem de informații ISR este determinată de principalele misiuni pe care sistemele ISR trebuie să le îndeplinească. Aceste sunt, fără a fi o abordare exhaustivă, următoarele:

- avertizarea timpurie;
- sprijinul cu informații a procesului de planificare a operațiilor;
- asigurarea informațiilor despre adversar și mediu pentru a realiza Imaginea Operațională Comună – COP (Common Operational Picture) și cunoașterea situației – SA;
- asigurarea datelor și informațiilor despre ținte;
- evaluării efectului la țintă;
- sprijinul operațiilor informaționale;
- asigurarea informațiilor necesare evaluării situației și a riscurilor;
- protecția forței.

Sistemele ISR trebuie să răspundă acestor misiuni în toate tipurile de operații.

Conceptul ISR nu poate fi definit prin abordarea separată a părților componente, întrucât acesta nu reprezintă doar suma părților, ci și efectul sinergic al intensificării acțiunilor care se execută în același sens, rezultat din lucrul integrat al sistemelor de senzori.

Informațiile culese de sistemele ISR sunt destinate sprijinului direct al mai multor beneficiari și trebuie să contribuie la actualizarea situației curente, să sprijine identificarea indiciilor pentru emiterea avertizărilor privind amenințările și să sprijine direct procesul de management al țintelor prin componenta de descoperire, identificare și localizare a țintelor/Target Aquisition – TA.

În opinia mea, avertizările pot fi strategice și operativ-tactice.

Avertizarea strategică este definită ca fiind avertizarea oportună cu privire la inițierea de către un stat sau organizație a unui act ostil.

Aceasta presupune indicii și/sau indicatori care relevă faptul că urmează să se întâmple ceva, cum ar fi mobilizarea armatei și a rezervei, campanii naționale de recoltare de sânge, dislocarea de unități militare în afara garnizoanelor de reședință, măsuri de securitate neobișnuite, constituirea unor rezerve de resurse critice (carburanți, lubrifianți) etc.

Pentru a participa la un război, o țară sau organizație trebuie să se pregătească. Aceste pregătiri furnizează analistului argumentele necesare, pe baza cărora să emită o avertizare strategică către factorul de decizie politic sau militar.

Avertizarea tactic-operativă este definită ca fiind avertizarea după inițierea unei amenințări sau act de ostilitate, bazată pe date și informații din toate sursele posibile.

Un exemplu de astfel de avertizare ar putea fi informația conform căreia o țară/organizație adversă a lansat o rachetă intercontinentală, un bombardier a decolat, sau informația cu privire la apropierea acestora de spațiul aerian național. Timpul scurs de la momentul lansării rachetei și până la momentul atingerii țintei este foarte scurt și limitează posibilitățile de decizie elaborată a factorilor militari responsabili.

Părțile componente ale conceptului ISR<sup>2</sup> sunt definite astfel:

a) *Informații/Intelligence* reprezintă produsul rezultat din procesarea informațiilor privind statele, forțele sau elementele ostile ori potențial ostile, sau zonele actuale ori potențiale de operații. Termenul este utilizat și pentru a desemna activitatea care are ca rezultat produse de informații, precum și pentru a desemna organizațiile specializate pentru astfel de activități;

b) *Supravegherea/Surveillance* reprezintă observarea sistematică a spațiului aerian, a zonelor de suprafață, subterane/subacvatice, locurilor, persoanelor sau obiectelor prin mijloace vizuale, acustice, electronice, fotografice sau de altă natură. Supravegherea se poate realiza pasiv, pentru zone largi sau activ prin acoperirea unor zone de interes specificate. Ea poate pune în evidență modificările survenite față de situația inițială, contribuind astfel la avertizarea timpurie, monitorizarea misiunilor, protecția forței și planificarea misiunilor ISR viitoare;

c) *Descoperirea, identificarea și localizarea țintelor/Target Aquisition – TA* reprezintă culegerea sistematică de informații detaliate despre forțele adverse, inclusiv persoanele cheie, sau sistemele de armament ale acestora, pentru a permite decidenților militari să aleagă cele mai adecvate mijloace de combatere. Identificarea și localizarea țintelor trebuie făcute cu maximă precizie pentru a permite angajarea mijloacelor de lovire proprii pentru neutralizarea acestora. Informațiile trebuie să furnizeze și datele necesare evaluării efectului la țintă/Battle Damage Assessment – BDA. În sfera informațiilor despre ținte nu sunt cuprinse numai datele de localizare geografică, ci și datele tehnice, fizice, economice, sociale și chiar istorice. TA este



parte a managementului țintelor și este strâns legată de analiza misiunii;

d) *Cercetarea / Reconnaissance* reprezintă o misiune întreprinsă pentru a obține, prin observare vizuală sau alte metode de detecție, informații despre activitățile și resursele unui adversar sau potențial adversar sau de a procura date referitoare la caracteristicile meteorologice, hidrografice sau geografice ale unei anumite zone.

ISR reprezintă activitatea de informații care sincronizează și integrează planificarea și exploatarea tuturor sistemelor de senzori cu funcțiile de procesare, valorificare, fuziune și diseminare a informațiilor, pentru sprijinul direct al decidenților, la toate nivelurile de comandă. ISR funcționează ca un sistem care integrează etapele ciclului informațional, datele furnizate de senzori, disciplinele și capacitățile de informații.

Misiunile sistemelor ISR vizează spațiul aerian și cosmic, terestru, maritim, submarin și mediul electromagnetic. ISR este o activitate executată de personal specializat, cu folosirea senzorilor integrați în sisteme de exploatare și analiză specifice. Senzorii ISR pot fi statici sau mobili, instalați pe platforme aeriene, vehicule terestre, nave etc.

Elementele de culegere ISR sunt forțele, mijloacele și sistemele de senzori utilizate pentru a observa, supraveghea, identifica, înregistra și comunica date și informații referitoare la fapte, evenimente, situații și condiții. Informațiile culese de acestea provin din mai multe tipuri de surse, numite discipline de culegere.

Domeniile de culegere<sup>3</sup> sunt:

a) informații din surse acustice/Acoustic Intelligence – ACINT – sunt informații provenite din culegerea și procesarea fenomenelor acustice. Datorită naturii originii sunetului, ACINT vizează în primul rând mișcarea și informațiile derivate din aceasta;

b) informații din surse umane/Human Intelligence – HUMINT – sunt informații culese și asigurate de sursele umane. Orice persoană, din forțele proprii, adverse sau neutre poate reprezenta o sursă HUMINT. Culegătorii HUMINT sunt persoane specializate în obținerea de informații de la sursele umane ca răspuns la cerințele de informații și includ personal pentru chestionare și personal de culegere. HUMINT au valoare particulară în confirmarea sau completarea informațiilor obținute prin utilizarea altor discipline de culegere;

c) informații obținute din imagini/Imagery Intelligence – IMINT – derivă din imaginile obținute de camere fotografice, radare, senzori electrono-optici și termali, care pot fi terestri, maritimi sau montați pe platformele aeriene și spațiale. IMINT folosește imaginile pentru a localiza și identifica activitățile, facilitățile, infrastructura și echipamentul adversarului. De asemenea, asigură comandanților informații despre mediu care pot avea impact asupra acțiunilor militare. Informația transmisă de o imagine este clară, concisă, fără echivoc și, în cele mai multe cazuri, este folosită pentru confirmarea informațiilor din alte surse;

d) informații din măsurători și amprente caracteristice țintei/Measurement and Signature Intelligence – MASINT – sunt informații științifice și tehnice obținute din analiza cantitativă și calitativă a datelor derivate de la instrumentele de detecție în scopul identificării oricărei caracteristici distincte asociate cu sursa, emițătorul sau expeditorul și de a facilita identificarea ulterioară și / sau o măsurătoare de același fel. Prezența sistemelor tehnice adversare în zona acțiunilor militare este detectată pe baza amprentelor termice, seismice, electronice etc., care demască folosirea lor. MASINT derivă din culegerea și compararea unei mari varietăți de emisii cu o bază de date tehnice și științifice cunoscute, pentru a identifica echipamentul și sursa emisiilor;

e) informații din surse deschise/Open Sources Intelligence – OSINT – reprezintă informațiile derivate din informațiile publice disponibile și informațiile neclasificate cu diseminare sau acces public limitate. OSINT sunt culese din surse, cum ar fi: radio, televiziune și presa, propaganda de stat, jurnale științifice și lucrări tehnice, Internet, manuale tehnice etc. Orice structură de informații folosește permanent sursele deschise în obținerea de informații. OSINT este o sursă de bază în informații, deși, cu capacitățile echipamentelor moderne de culegere a știrilor, vor exista situații când o știre de la televizor va fi folosită imediat pentru a produce informații;

f) informații culese prin radar/Radar Intelligence – RADINT – sunt informații obținute prin utilizarea radarului ca instrument de detecție, precum identificarea și localizarea unei ținte care poate fi recunoscută sau nu, pe o anumită direcție și la o anumită distanță sau simpla detecție a mișcării unei ținte. Acest aspect este diferit de exploatarea datelor radar de către IMINT. Colonelul dr. Ioan

Dodon, un fin analist al domeniului undelor – radiolocația, aprecia, în lucrarea sa de doctorat, că „informațiile despre situația aeriană reprezintă 70% din totalul informațiilor care circulă în sistemul de comandă-control al Forțelor Aeriene”<sup>4</sup>, iar acest sistem vehiculează mult mai multe informații decât sistemele similare ale Forțelor navale sau Forțelor Terestre, și cu o viteză superioară. Consider reală această afirmație și accentuez faptul că importanța informațiilor este mult mai mare astăzi, când vitezele dezvoltate în spațiul aerian și cosmic sunt net superioare celor din mediul terestru sau naval.

g) informații din mediul electromagnetic/SIGINT și Război Electronic. SIGINT sunt informații obținute prin culegerea și exploatarea semnalelor de comunicații (COMINT) și a emisiilor electromagnetice de noncomunicații

În consecință, IS(TA)R este un „sistem de sisteme” care înglobează toate capacitățile de culegere a datelor și a informațiilor din câmpul de luptă, având și capacitatea de procesare a acestora asigurând o imagine completă asupra situației operaționale curente – COP (Common Operational Picture).

Sistemul ISR permite satisfacerea cerințelor de informații pentru îndeplinirea misiunilor prin interoperabilitatea elementelor componente. În cazul în care componentele individuale ale sistemului nu sunt capabile să interopereze, sinergia derivată din sistem nu se produce.

Pentru o operare eficientă a sistemului ISR este necesar ca toate elementele componente să opereze după o doctrină și un standard comune. Când operațiile ISR sunt conduse de o structură

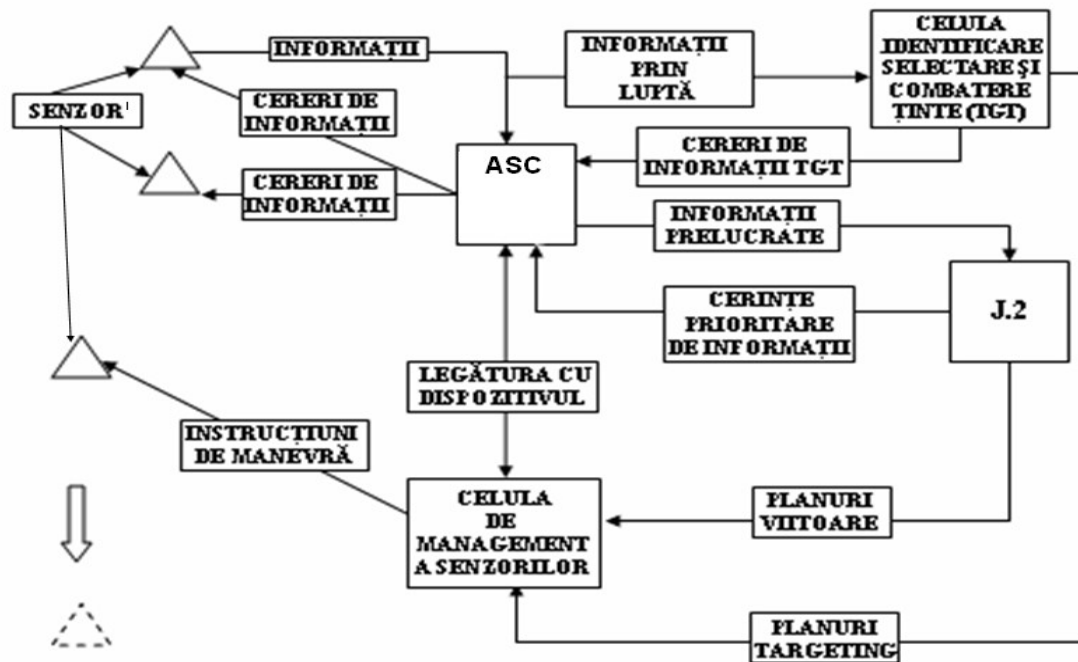


Fig. 1 Fluxul informațional IS(TA)R<sup>6</sup>

(ELINT) străine. Războiul electronic este acțiunea militară care se bazează pe exploatarea energiei electromagnetice cu scopul cunoașterii situației și obținerii de efecte ofensive și defensive;

h) informații obținute prin analiza echipamentelor tehnice/Technical Intelligence – TECHINT – reprezintă informațiile cu privire la dezvoltările tehnologice, precum și la capacitățile de performanță și operaționale ale materialului, care au sau, eventual, pot să aibă o aplicare practică în scopuri militare.

multinațională, aceste cerințe sunt esențiale pentru succes.

Pentru adoptarea principiului conducerii și coordonării centralizate trebuie să existe comandă unică pentru întreg sistemul: comandantul/șeful structurii ISR. În conformitate cu misiunea comandantului sprijinit, el va avea întreaga responsabilitate pentru conducerea activităților în cadrul ISR.

Structurile ISR trebuie să asigure sprijinul de informații atât pentru conducerea acțiunilor curente,



cât și planificarea acțiunilor viitoare, concomitent cu asigurarea informațiilor despre țintele din câmpul de luptă. Din acest motiv, conceptul de operații ISR se bazează pe existența următoarelor componente funcționale<sup>5</sup> (Figura 1):

1. Celula pentru Coordonarea tuturor Surselor – *All Sources Cell (ASC)*;
2. Celula pentru Managementul Senzorilor;
3. Celula pentru Identificarea, Selectarea și Combaterea Țintelor – *Targeting Cell (TGT)*.

La nivelul tuturor comandamentelor se va constitui, din timp de pace, un centru ISR cu misiunea de a exercita comanda și controlul sistemului ISR din subordine sau pus la dispoziție.

Centrul ISR este o capacitate de comandă și control pentru toate operațiile/acțiunile. Sistemul ISR are trei elemente principale:

1) *Informația*. Aceasta va exista fie sub forma datelor și informațiilor primare/brute, fie ca informație prelucrată /procesată – *intelligence*;

2) *Procesele*. Sistemul ISR integrează ciclul informațional cu părți ale OPP și ciclul de identificare și de selectare a țintelor;

3) *Arhitectura* sistemului ISR. Aceasta cuprinde capacitățile de culegere și structurile care le coordonează și controlează, compartimentele de analiză, beneficiarii datelor și informațiilor și infrastructura CIS la toate nivelurile de comandă.

Sistemul IS(TA)R acoperă cele patru domenii funcționale specifice: informații militare, supraveghere, identificare și selectare a țintelor, cercetare și trebuie să îndeplinească o serie de capacități. Cerințele de capacitate ale sistemelor ISR sunt:

a) sistemele ISR trebuie să satisfacă nevoile de informații ale comandanților/decidenților și structurilor de planificare, conducere și evaluare a operațiilor, astfel încât ei să poată planifica, comanda, coordona, executa și evalua spectrul complet al operațiilor curente și viitoare;

b) sistemele ISR trebuie să sprijine operațiile militare convenționale, de răspuns la criză, de stabilitate și de sprijin, umanitare și asimetrice, concomitent cu misiunile de protecție a forței. De asemenea, trebuie să asigure înțelegerea factorilor de mediu nontradiționali;

c) informațiile culese trebuie să fie oportune, corecte și distribuite în formatul cel mai util beneficiarilor. Datele ISR, sursele și interfețele trebuie să fie proiectate pentru asigurarea interoperabilității, prin adoptarea și integrarea standardelor corespunzătoare;

d) un sistem ISR eficient se bazează pe NEC și necesită o gamă amplă de surse, senzori, platforme, procese, deprinderi, conectivitate și instrumente de lucru interoperabile. Aceasta reprezintă cheia pentru stabilirea cantității și calității adecvate a senzorilor ISR, precum și mecanismele de sprijin necesare, pentru a permite continuitatea, verificarea încrucișată a informațiilor și culegerea din medii ostile;

e) pentru a permite utilizarea celor mai eficiente practici de management al informațiilor care să facă disponibile informațiile relevante, prevenind în același timp supraîncărcarea, trebuie implementate politici de asigurare a securității și a schimbului de informații.

În concluzie, indiferent cum va fi abordată în viitor problematica conceptelor ISR vs IS(TA)R, consider că aceste două procese sunt în strânsă interdependență și o abordare separată a acestora nu ar cuprinde toată problematica în ansamblul ei. În condițiile realităților câmpului de luptă modern, informația este considerată drept arma decisivă, iar sistemul ISR devine instrumentul cheie prin care se realizează sprijinul cu informații pentru obținerea situației curente a inamicului. În consecință, realizarea și utilizarea unor astfel de sisteme, ce permit abordarea multisursă a informațiilor, devine obligatorie și trebuie abordată la cel puțin două niveluri – tactic/operativ și strategic.

Dacă problema este abordată la nivel tactic/operativ, provocarea este de a maximiza efectele sistemului, în momentele critice ale operației. Altfel spus, trebuie asigurată informația necesară, la momentul oportun, structurii potrivite pentru a îndeplini cu succes misiunea.

Dacă problema este abordată la nivel strategic, atunci provocarea este de a conecta diferitele sisteme ISR pentru mai multă eficiență, economie și performanță.

Forțele și mijloacele unităților de cercetare și supraveghere prin radiolocație și avertizare timpurie din serviciul de luptă permanent Poliție Aeriană (SLP-PA), precum și cele de război electronic din serviciul de luptă permanent Supraveghere Electronică (SLP-SE), reprezintă capacități de culegere ISR, pentru acoperirea cerințelor de informații din mediul aerian și electromagnetic.

Forțele și mijloacele se integrează cu succes în arhitectura sistemului C4I2SR<sup>7</sup> din Armata României fiind elemente centrale și punctul de pornire în realizarea sistemului ISR.



**NOTE:**

1 *Strategia de Securitate Națională a României*, București, 2007, p. 3.

2 Mihai Duță, *Considerații privind dezvoltarea sistemului de Informații, Supraveghere și Cercetare în Armata României*, Editura UNAp „Carol I”, București, 2013, p. 5.

3 Mihai Duță, *op.cit.*, p. 7.

4 Colonel Ioan Dodon, *Contribuții la perfecționarea cadrului organizatoric și funcțional al sistemului unic de înștiințare despre situația aeriană, în condițiile integrării zonale a surselor de informații, prin utilizarea unor rețele de microcalculatoare*, Teza de doctorat, AÎSM, București, 1993.

5 Studiul: *Necesitatea implementării sistemului ISTAR pentru asigurarea unor capacități de informații operaționale și interoperabile cu structuri similare NATO, MApN*, București, 2007.

6 *Ibidem*, p. 32.

7 *C4I2SR – Comandă, Control, Comunicații, Computere, Interoperabilitate, Informații, Supraveghere, Cercetare*.

**BIBLIOGRAFIE**

\*\*\* *Doctrina Națională de Informații pentru Securitate*, București, 2004.

\*\*\* *Obiectivul Forței EL – 0583 „Capabilități ISTAR la nivel Divizie / Brigadă”*.

\*\*\* *SMG/Cc – 2.1, Concepția de construcție, dotare, instruire și întrebuințare a Batalionului ISTAR*, Editura SMG, București, 2005.

\*\*\* *SMG/Cc – 2.2, Manualul pentru luptă al unităților de cercetare*, Editura Tehnică Militară, București, 2005.

\*\*\* *SMG/Cc – 2.3, Manualul pentru pregătirea informativă a câmpului de luptă*, Editura Tehnică Militară, București, 2005.

\*\*\* *AJP – 2.01 A, Joint Intelligence Support to Military Operations*.

\*\*\* *AJP – 2.01.1, Joint Tactics, Techniques, and Procedures for Intelligence Support to Targeting*.

\*\*\* *AJP – 2.01.3, Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace*.

\*\*\* *AJP – 2.03, Joint Tactics, Techniques, and Procedures for Geospatial Information and Services Support to Joint Operation*.

\*\*\* Studiul: *Necesitatea implementării sistemului ISTAR pentru asigurarea unor capacități de informații operaționale și interoperabile cu structuri similare NATO, MApN*, București, 2007.

Duță Mihai, *Considerații privind dezvoltarea sistemului de Informații, Supraveghere și Cercetare în Armata României*, Editura UNAp „Carol I”, București, 2013.