INFORMATION RESOURCES MANAGEMENT COMPONENTS. THE MAIN SOURCES OF INFORMATION

Mr. drd. Ilie PĂUN

ABSTRACT

Information transformation into a major resource of economic growth has resulted in its being a major organizational resource along with the human, material and financial resources. As top companies from developed countries prove, information resources, permenently upgraded, represents the adoption and application of performance strategies. Technically, each element of the strategy is projected and implemented according to the information available to the company. Consequently, the organization's informational potential acts as a cathalist, respectively, as an obstacle to the planned objectives, choices made and established deadlines.

Resursele informaționale în esență, cuprind ansamblul informațiilor şi know-how-ului, indiferent de natura lor – tehnică (brevete, proiecte, etc.) economica (referitoare la piață, preturi, credite, impozite, taxe, etc.), juridica (legile, ordonantele, etc. care privesc firmă), manageriale (privind sistemul informatial, structura organizatorica, adoptarea deciziilor, etc.) etc. – pe care le poseda organizația.

***Sistemele de management al resurselor informaționale (MRI*)** includ resursele informaționale, procesele care au loc pe baza resurselor informaționale, sisteme informaționale, sisteme computerizate, care toate la un loc formează o infosferă globală prin intermediul căreia se asigură informația potrivită, la momentul potrivit şi în locul potrivit. Modalitatea de asigurare a acestei capabilități este prin intermediul unui sistem de management distribuit al resurselor informaționale care formează coloana vertebrală a infrastructurii informaționale a tuturor sistemelor care vor fi dezvoltate în viitor.

Multe capabilități (care în momentul de față nu sunt disponibile) vor deveni parte integrantă a acestui mediu informațional şi vor pune la dispoziția celor aflați în misiuni de luptă mijloace automatizate, adaptabile, robuste de management al resurselor informaționale. Astfel se poate asigura o integrare a planificării misiunii şi a monitorizării executării planului la toate nivelele şi în timp real.

Una dintre problemele care apar ține de menținerea unor costuri realiste mai ales atunci când se vorbeşte de opțiuni pe termen lung sau când se iau în calcul noi capabilități MRI. Dezvoltarea anumitor componente (subsisteme) poate influența o serie de partiționări ale capabilităților, cum se întâmplă mai ales în cazul opțiunilor care implică sisteme multirol de management al resurselor informaționale şi care vor avea efecte secundare asupra altor arii de capabilități. Din motivele expuse mai sus estimarea costurilor trebuie să aibă în vedere toate implicațiile asupra capabilităților de apărare, nu numai costurile directe ale unui anumit subsistem.

Dezvoltarea unui sistem de management al resurselor informaționale implică multe *provocări noi*, provocări enumerate mai jos:

- multitudinea de interese care există în domeniul apărării ca urmare a numărului foarte mare de deținători de interese;
- necesitatea funcționării sistemului în contextul unei coaliții multinaționale;
- necesitatea unor estimări de cost realiste care să includă şi costurilor subsistemelor (elementelor) care încă nu există;
- necesitatea utilizării unor instrumente precum analiza structurii forței şi modele de costuri;
- alinierea sistemului la programul general pune probleme datorită decalajului de timp implicat de componente ale capabilităților cum sunt personal cu pregătire şi echipament IT avansat.

Planificarea însăşi este supusă schimbărilor generate de tehnologie, politica de apărare, ameniță̆ri, resurse informaționale şi managementul organizațional.

Construirea unei capabilități în domeniul managementului resurselor informaționale implică provocări tehnice importante. Respectivele provocări sunt clasificate în funcție de infrastructura mediilor aflate la distanță unul de celălalt, de mecanismele care sprijină managementul serviciilor informaționale şi care se regăsesc în mediile menționate anterior, de capacitatea de desfăşurare în teren a serviciilor de asigurare a resurselor informaționale.

În vederea asigurării mangementului serviciilor informaționale necesare în cadrul mediilor aflate la distanță este nevoie de dezvoltarea de mecanisme de asigurare a managementului tuturor tipurilor de date indiferent de localizarea acestora. Provocările ridicate de acest obiectiv sunt după cum urmează:

1. dezvoltarea de modele de date şi de arhitecturi de stocare şi recuperare a acestor date capabile să asigure utilizarea eficientă a acestora;
2. fuziunea şi sincronizarea datelor dependente sau nu de timp;
3. dezvoltarea de sisteme inteligente capabile să navigheze autonom în cadrul unor baze de date complexe şi care să extragă informațiile necesare unui utilizator;

4. dezvoltarea unui limbaj comun care să vină în sprijinul accesului „intuitiv” la şi a recuperării datelor dint-un sistem de management al bazei de date;
5. utilizarea contextului resurselor informaționale în distribuirea eficientă într-o bandă joasă de comunicații în vederea controlului cantității de informații transmise;
6. asigurarea capabilităților necesare remedierii situațiilor în care are loc doar o transmitere parțială a informațiilor;
7. scalarea tehnicilor de distribuire a informației la sisteme complexe de noduri de comunicare.

În concluzie, un program de dezvoltare a unui sistem de management al resurselor informaționale poate sprijini şi îmbunătăți procesul de luare a deciziilor din MApN. Scopul său este acela de a facilita fluxurile informaționale şi implicit, de a îmbunătți schimbul de informație în condițiile menținerii securității şi relevanței. Condițiile de bază în realizarea unui astfel de program țin de realizarea unui cadru strategic efectiv, de asigurarea interoperabilității, interrelaționaării, disponibilității, securității informațiilor utilizate, precum şi de conformarea sistemelor şi tehnologiilor utilizate la standardele existente.

PRINCIPALELE SURSE ALE INFORMAȚIEI

3.1 Sursele (Input-urile) Informației Pentru Apărare

Input-urile Informației pentru Apărare se referă la varietatea surselor folosite de Serviciul de Informații Militare (SIM) în cadrul activității de culegere a informațiilor. În continuare sunt prezentate principalele surse utilizate de SIM:

3.1.1. OSINT (Open Source INTelligence)

- reprezintă orice informație care poate fi obținută prin metode legale (neacoperit) şi sunt disponibile în mod liber (a nu se înțelege şi gratuit) oricui doreşte să le acceseze. Aceste surse pot îmbrăca forme de genul: ziare, periodice, cărți, publicații guvernamentale şi ştiințifice, radioul sau televiziunea, internetul, servicii comerciale on-line, baze de date electronice cum ar fi cele guvernamentale, universitare sau business.

Din punct de vedere cantitativ, OSINT reprezintă principala sursă de informare. Se estimează că majoritatea serviciilor de informații primesc curent aproximativ 80-85% din totalul de informații din surse deschise. Totuşi folosirea OSINT diferă funcție de mediul de căutare. Astfel nu se pot folosi cu succes sursele deschise în cazul unor operații de targeting, acestea fiind mult mai utile în cazul informațiilor privind evoluția unor tehnologii sau structuri[170].

Existența OSINT nu presupune automat şi accesul direct al serviciului de informații la aceste surse. În cazul IA, 80% din informațiile din surse deschise nu sunt accesibile în România şi nu sunt în limba română. Pentru ca scopul final de

[170] Robert D. Steele, Information peacekeeping, e-print of upcoming publication in Dearth and Campen, 11 March 1998.

obținere de produse de intelligence din surse deschise să fie atins, este necesar un proces extrem de laborios şi nu foarte ieftin.

Acest proces implică descoperirea, diferențierea, filtrarea şi selectarea acelor fragmente de informații care, integrate şi interpretate, să ducă la obținerea unor informații utile.

În ultimii ani, OSINT a devenit în centrul atenției serviciilor de informații grație volumului mare de informații pe care le oferă. Concentrarea specialiştilor în domeniu pe aceste surse a dus la clasificare lor pe două grupe:

- surse deschise accesibile legal şi obținute la un preț convenabil (Jane's, Lloyd, Stratfor);
- surse deschise ce aparțin domeniului proprietății private – acestea pot fi obținute legal dar costurile ce le implică sunt crescute. Un exemplu în acest sens îl constituie achiziția unui sistem de rachetă, în vederea studierii sistemului de ghidare şi a softului de execuție[171].

3.1.2. HUMINT – HUMan INTelligence

- sunt informații obținute prin procedee diverese (de la observare şi ascultare la debriefing sau exploatare în necunoştință de cauză) de personal special pregătit şi antrenat prin exploatarea unor surse umane, în mod oficial, semioficial sau neoficial (clandestin), prin intermediul informatorilor, colaboratorilor sau agenților.

Potrivit Doctrinei NATO de intelligence, *"orice persoană – amic, inamic sau neutră –poate fi o potențială sursă umană*". Ofițerul de caz sau agentul utilizat pentru culegerea de informații HUMINT folosesc o multitudine de metode şi procedee, pasive sau active, legale şi ilegale, în scopul obținerii de date şi informații care să satisfacă nevoia de produse de intelligence.

Activitățile desfăşurate în spectrul HUMINT pot fi şi neacoperite. Astfel, este utilizat termenul surse umane deschise cum ar fi contacte cu academicieni, ziarişti, diplomați, manageri sau servicii partenere[172]. Totuşi, există o specificitate a activității în sensul că accesul la aceste surse nu este liber oricui. Aici intervin două elemente care trebuie să conveargă: sprijinul serviciului de informații şi abilitățile ofițerului de caz.

În literatura de specialitate s-au dezvoltat două tipuri de HUMINT funcție de nivelul de adresare a informației şi de modalitatea de obținere a acesteia:

- funcție de nivelul de adresare a informației: HUMINT strategic (pe termen lung, surse de nivel mare) şi HUMINT tactic (informație perisabilă, surse de nivel mic, accent pe protecția forțelor);
- funcție de modalitatea de obținere a informației – HUMINT obținut prin interogare (sub presiune) de la surse care nu doresc să coopereze (prizonieri de război, persoane reținute), HUMINT obținut prin debriefing de la surse ce doresc să coopereze (dezertori, refugiați, trupe proprii) şi HUMINT obținut prin exploatare în necunoştință de cauză de la persoane care nu realizează că

[171] Steele, Open Source Intelligence, 1996, chapter 2, section 2004
[172] Steele, Open Source Intelligence, 1996, chapter 2, section 2013

fac obiectul unei activități de informații (contacte diferite ale ofițerului de caz sau ale agentului acestuia).

În cazul IA, *sursele HUMINT* includ în principal[173]:

- *Prizonieri de război, dezertori, deținuți civili.* Aceştia pot furniza informații despre capabilitățile adversarului, date de identificare a unităților, date despre locații de interes, despre lideri militari şi alte personalități, elemente de natură logistică etc. Informațiile culese de la acest gen de surse umane pot fi extrem de valoroase şi trebuie utilizate imediat. Totuşi, se impune multă prudență, ca şi o minimă verificare a acestor date provenite de la o singură sursă, pentru a evita dezinformarea.
- *Agenții* sunt indivizi care acceptă conştient să coopereze cu serviciul de informații, furnizând informații conform nevoilor acestora. Agentul primeşte sarcini de la ofițerul de caz care îl conduce şi este recompensat pentru activitatea sa.
- *Trădătorii* sunt persoane din tabăra adversă care, în mod voluntar, repudiază regimul țării căreia îi aparțin, furnizând, astfel, benevol servicii sau informații adversarului. Ca şi în cazul altor surse umane, aceştia trebuie atent controlați şi manipulați de un personal calificat.
- *Civili locali, persoane dislocate şi refugiați.* Acest gen de surse umane sunt specifice activităților din teatrele de operații, la îndemâna serviciilor de informații ale statelor care participă cu trupe la operații de impunere sau menținere a păcii. Ei pot fi utili în obținerea de date relevante despre câmpul de luptă, despre unitățile luptătoare angajate în conflict, rețelele de insurgenți, terorişti sau alte structuri politico-militare ale adversarului. Folosind orice oportunitate, structurile de *HUMINT* identifică persoanele locale din aria de responsabilitate care sunt dispuse să divulge informații de interes.
- *Persoane aparținând forțelor proprii sau aliate* (friendly forces). Militarii nespecializați în domeniul intelligence din cadrul forțelor proprii sau aliate au multe oportunități de a interacționa cu populația locală, pe timpul îndeplinirii misiunilor pe timp de război sau în cursul operațiunilor militare de alt tip decât războiul. Unele dintre aceste forțe, precum patrulele de recunoaştere, pot primi sarcini de culegere a informațiilor, fiind apoi debrifate de personalul specializat. Alte potențiale surse valoroase pot fi comandanții sau persoanele din statele majore de diferite niveluri care au legături cu populația şi autoritățile locale, precum şi membrii structurilor CIMIC, medicale, de geniu care intră în contact cu populația locală. Deoarece aceştia nu au pregătire de intelligence, ei trebuie debrifați de echipele de specialişti *HUMINT*, pentru a se obține maximum de informații relevante.
- *Documentele* obținute de la surse *HUMINT* pot, de asemenea, furniza informații valoroase, care pot fi exploatate operațional sau utilizate pentru a obține noi informații de la aceste surse.

[173] Snyder, "With a little bit of heart and soul analyzing the role of HUMINT in the post cold war area," Woodrow Wilson School Policy Conference 401a, 6 January 1997

3.1.3. SIGINT – SIGnal INTelligence

- sunt informații obținute din surse care acționează în spectrul electromagnetic şi constau din patru subdomenii[174]:

COMINT (COMmunication INTelligence) – informații obținute prin interceptarea comunicațiilor şi a transmisiilor de date de către entități specializate şi care nu sunt destinatarii acestor informații. *COMINT* implică interceptarea şi procesarea comunicațiilor externe transmise prin radio sau alte mijloace electromagnetice şi procesarea comunicațiilor externe criptate, indiferent de modul de transmitere. Interceptarea presupune cercetare, capturare, identificarea operatorului, analiza semnalelor, analiza de trafic, analiza criptografică, decriptare, studiu de text, fuzionarea acestor procese şi înaintarea rezultatelor.

Sunt excluse din această definiție interceptarea şi procesarea comunicațiilor scrise necriptate, emisiunile de propagandă şi presa.

ELINT (ELectronic INTeligence) sunt informații obținute prin intermediul transmisiilor electromagnetice care nu aparțin comunicațiilor. *ELINT* presupune culegerea (observarea şi înregistrarea) şi procesarea în scop informativ a informațiilor obținute din surse nonverbale, prin radiații electromagnetice emanând din alte surse decât cele radioactive sau de detonare nucleară.

3.1.4. IMINT[175] (IMagery INTelligence)

- sunt informații provenite din surse specializate în prelucrarea imaginilor; culegerea, întocmirea de hărți şi prelucrarea imaginilor dobândite prin intermediul senzorilor video-fotografici.

IMINT este prin excelență o activitate care permite comandanților să "vadă" câmpul de luptă în timp real.

Prin *IMINT* se dobândesc informații cu ajutorul senzorilor care pot avea baza la sol, pe mare sau purtate de platforme aeriene/spațiale. O mare parte din *IMINT* provin din surse cum ar fi sateliți, avioane cu pilot şi UAV.

Există o mare varietate de senzori *IMINT*. Unii dintre ei furnizează imagini în timp real, alții achiziționează imagini care sunt apoi procesate. Iată câteva exemple de senzori *IMINT*: camere optice, care pot produce imagini alb-negru sau color; dispozitive de vedere pe timp de noapte, utilizând tehnologie în infraroşu sau de identificare termică; radare pentru identificarea aparatelor aeriene, de identificare a țintelor, radare Doppler; aparatură video şi de televiziune pe timp de noapte; laseri de detecție; aparatură de analiză video multispectrală.

Platformele uzuale folosite pentru senzorii de *IMINT* sunt: avioanele fără pilot echipate cu camere video şi alți senzori electronooptici, avioane sau elicoptere de recunoaştere, vehicule (blindate, uşor blindate sau neblindate) special echipate pentru cercetare terestră, precum şi roboți echipați cu senzori *IMINT*.

---

[174] Richelson & Ball, The ties that bind, 1985, 101, 175-178

[175] www.fas.org/irp/doddir/army/tacimlp.htm.

3.1.5.MASINT (Measurement and Signatures INTelligence)

- sunt informații provenite din analiza calitativă şi cantitativă a datelor obținute cu ajutorul senzorilor specifici. Această categorie conține, de obicei, informații acustice, informații obținute prin radar, detectare a radiației nucleare, informații obținute prin infraroşu, informații electro-optice, frecvență radio, radiații întâmplătoare, luarea de probe din diverse materiale, ape reziduale şi surse spectral-radiometrice şi electro-optice (altele decât cele ce fac obiectul domeniilor *SIGINT* şi *IMINT*). *MASINT* se referă, de asemenea, la informații obținute din surse care acționează în spectrul electromagnetic sau de informații provenite din surse specializate în prelucrarea imaginilor ce necesită procesare specializată. Ca produs finit, *MASINT* vine, în primul rând, în sprijinul comandanților militari. Există două subdomenii *MASINT*: *ACINT(Accoustic Intelligence)* şi *RADINT (Radiation Intelligence)*:

• *ACINT* sunt informații provenite din culegerea şi procesarea fenomenelor acustice. Acestea sunt informații transformate din sunet (de ex.: hidrolocatoare, sonare, Sistemele integrate de supraveghere submarină – IUSS şi Sistemele de cercetare de artilerie prin mijloace acustice). Din cauza originii sunetului, *ACINT* vizează, în primul rând, mişcarea şi informațiile care pot fi extrase din detectarea ei. *ACINT* în domeniul maritim implică detectarea, urmărirea şi identificarea contactelor submarinelor prin sonar activ sau pasiv de diferite tipuri.

• *RADINT* sunt informații obținute prin utilizarea radarului ca instrument de detectare (de ex.: identificarea unei nave sau aeronave), care poate fi recunoscut sau nu, pe o anumită direcție şi la o anumită distanță de radar sau simpla detectare a mişcării unei ținte la un anumit punct pe sol. Acest aspect este diferit de exploatarea datelor radar de *IMINT*.

TELINT (TELemetric INTelligence) sunt informații obținute prin telemetrie.

Din cele prezentate anterior cred că rezultă cu argumente că resursa informațională este una dintre cele mai importante din cele ale apărarii iar în multe momente ale pregătiri desfăşurării războiului şi perioadei post conflict devine cea mai importantă. Ne permitem o personală formulare care nu se vrea maximă sau aforism potrivit căreia: o resursă informațională bogată şi veridică dar nefolosită oportun cu măestrie de comandanți poate să se sfârsească în eşecul luptei, dar, cu certitudine, lipsa, puținătatea şi alterarea resursei informaționale conduc la un eşec anunțat.

Bibliografie

- Robert D. Steele, Information peacekeeping, e-print of upcoming publication in Dearth and Campen, 11 March 1998.
- Steele, Open Source Intelligence, 1996,
- Snyder, "With a little bit of heart and soul analyzing the role of HUMINT in the post cold war area," Woodrow Wilson School Policy Conference 401a, 6 January 1997
- Richelson & Ball, The ties that bind, 1985, 101, 175-178
- Allied Joint Publications AJP 2-1
- Documentul AJP-2 - Doctrina integrată de informații, contrainformații şi securitate a NATO;
- Doctrina pentru sprijinul cu informații al operațiilor întrunite, Bucureşti 2003
- Legislații ale serviciilor de informații şi securitate din statele membre ale Uniunii Europene