

Despre intelligence (II)

Conf. univ. dr. Marian SEBE
Serviciul Român de Informații
e-mail: msebe@dcti.ro

Abstract

Taking into account the evolution and development of intelligence/OSINT realm in the last years the re-conceiving intelligence problem is formulated. In this respect, the role of open system becomes fundamental for such an approach. The intelligence concept is composed by two fundamental attributes: secret and open. These two attributes reshape the main complementary components of the intelligence realm: secret and open intelligence. These two components put forth (manifest) in every organization and we are trying to identify their main role, functions and systemic structures.

Keywords: intelligence/OSINT, open/secret.

Introducere

Într-un articol anterior am inițiat un demers dedicat investigării semnificației intelligence-ului prin care România trebuie să își completeze perspectiva de stat membru NATO aflat în proces de integrare europeană, astfel încât să contribuie într-o manieră identitară la cultura intelligence/OSINT necesară statutului acestui sistem. Baza de cunoaștere necesară pentru un astfel de demers trebuie să îndeplinească anumite condiții ce au fost identificate, documentate, structurate și organizate compatibil cu ciclul de avans al cunoașterii, rând pe rând într-o perioadă de timp compatibilă cu complexitatea problematicii în cauză. Astfel, elementele acestui cadru referențial se pot enumera într-o formă simplificată după cum urmează:

I. Benchmarking pe modelele de intelligence naționale adoptate explicit ori implicit de statele ce compun sistemul.

II. Identificarea evoluțiilor domeniului intelligence prin intermediul factorilor de transformare și a celor de influență (de regulă, primii conduc la schimbări manifeste, ceilalți la transformări latente).

III. Influența factorilor identificați tradițional („știință și tehnologie”) și mai ales a interacției de natură cibernetică între aceștia.

IV. Condițiile, cadrele și manifestările proprii mediului de intelligence și securitate românesc (bineînțeles, în corelație cu punctele corespondente anterioare).

V. Condițiile specifice mediului românesc în privința complexului „știință și tehnologie” (desigur, în contextul punctului corespunzător anterior).

În mod evident, rostul demersului din prezentele pagini nu constă în detalierea precedentelor puncte, care oricum fac parte dintr-un program de anvergură și necesită o precondiție: coeziune conceptuală. Aici construim un demers argumentat privind identificarea dimensiunilor ce trebuie avute în vedere pentru a asigura coeziunea conceptuală a cadrului reprezentat de elementele enumerate mai sus; altfel cuvântul referențial conceptual nu are nicio acoperire, iar a porni la construcția, fie și a unei strategii de securitate, fără o astfel de viziune devine, în esență, un factor de vulnerabilitate cel puțin latentă la adresa culturii intelligence/OSINT.

În acest context, pentru completarea cunoștințelor relevante necesare documentării scurtului algoritm menționat mai sus, consider că este necesar să acoperim și să înțelegem trei repere direcționale, identificate până în prezent, ce intră în componența cadrului referențial, necesare abordării analizei și proiectării unui model de *intelligence românesc*, capabil de *integrare sistemică* într-un *model european* și *euroatlantic*.

Primul reper, trebuie să elucideze care este rolul sistemelor deschise în evoluția și dezvoltarea oricărei organizații, cum au evoluat și se dezvoltă sursele deschise, chiar prin apariția propriului mod de extindere a conceptului de sursă, așa cum domeniul intelligence a făcut-o în ultimul secol, contribuind astfel la redefinirea conceptului de intelligence, prin prisma unei noi paradigme.

Al doilea reper, identificabil prin monitorizarea evoluției domeniului intelligence din ultimele două decenii, permite să distingem două direcții de dezvoltare pe care le putem utiliza în procesul de analiză și proiectare a unui nou model de intelligence. Ambele direcții iau în calcul o viziune și imagine duală a conceptului de intelligence, ce se manifestă pregnant la începutul secolului XXI.

O direcție vizează o dualitate a intelligence-ului prin intermediul a două atribute fundamentale de manifestare funcțională: un atribut al acțiunii și exploatarei informației și cunoașterii cu *circuit închis*, manifestat prin

paradigma secretului, și un atribut al acțiunii și exploatării informației și cunoașterii cu *circuit deschis*, manifestat prin *paradigma deschiderii*.

Cealaltă direcție vizează dualitatea intelligence prin intermediul a două componente de manifestare organizațională: una a informației ori ceea ce serviciile speciale întreprind prin prisma unui intelligence al informației (information intelligence), și una, cea nouă, a cunoașterii ori ceea ce orice entitate organizațională trebuie să întreprindă prin prisma unui intelligence al cunoașterii (knowledge intelligence), proces care nu este derulat astăzi și care trebuie să integreze un ciclu dezintegrat în România ultimelor șase decenii, care să facă conexiunea dintre teorie și practică într-o *societate și economie a cunoașterii*.

Consolidarea activităților de *intelligence al informației* se face numai prin coordonarea eficientă a proceselor de *intelligence al cunoașterii*. Până acum două decenii serviciile și agențiile de intelligence dețineau supremația științifică și tehnologică, situație care în ultimele două decenii s-a modificat dramatic, astfel încât astăzi această supremație o deține sectorul privat, mult mai competitiv și adaptat la nevoile și trendurile pieței globale.

Mai există însă un element hotărâtor. Orice domeniu ori disciplină pentru a fi completă are nevoie de o teorie, strategie, doctrină¹ și tehnologia aferentă necesară atât trecerii de la teorie la acțiune, cât și mai ales dobândirii unui sens suficient de flexibil pentru semnificația cuvântului „practic” asociat acestuia. Dacă unul dintre elemente este omis ori neglijat și se reduce semnificația cuvântului „practică” la elementele rămase, atunci este afectat potențialul de relansare a ciclului de cunoaștere necesar mai ales în intelligence-ul contemporan. Cine nu reușește din diverse motive să își asigure o astfel de viziune, în sensul unei implementări identitare și integrate, se poate considera, dacă nu un învins al viitorului, cu siguranță un perdant al prezentului. Acesta este sensul discursiv pe care noi l-am asociat ideii „knowledge intelligence”.

Al treilea reper se referă la un nou concept menit a reuni și integra procesele de gestiune și administrare a cunoașterii și informației la nivel de organizații, rețele și meta-rețele de intelligence, atât la nivel de stat-națiune, cât și la nivel de coaliții. Este ceea ce numim intelligence sistemic.

¹ În treacăt fie spus, rostul doctrinei este de a asigura coeziunea cu alte cadre teoretice, fapt important dacă se are în vedere rostul coeziunii menționat în primele paragrafe de mai sus.

Fiecare dintre aceste repere direcționale ce compun o parte a cadrului referențial menționat mai înainte au fost analizate în raport cu elementele contextuale I-V. O parte reprezentativă a acestei analize formează intervențiile viitoare reunite sub titlul „Despre intelligence”. Demersul de față se axează pe primul reper, ce vizează rolul sistemelor deschise, ca element dual al domeniului intelligence, și pe o primă parte din al doilea, cu accent pe redefinirea intelligence prin prisma celor două attribute fundamentale: secret și deschis.

Principiul de dualitate și ISD – informația din surse deschise

Una dintre principalele schimbări care au avut loc în era post Război-Rece este determinată de creșterea importanței sistemelor deschise, factorul ce a indus această stare de fapt, și este cel mai lesne de sesizat, fiind preponderența informațiilor din surse deschise. La nivel de proces, dezvoltarea științifică și tehnologică a schimbat în mod radical modul de producere, comunicare și diseminare a informației, modificând optica asupra modulelor ce compun ciclul clasic de intelligence și impunând adoptarea unui similar în domeniul OSINT. De aici rezultând modificarea modelelor și proceselor informaționale, inclusiv a proceselor de intelligence, în orice tip de entitate organizațională, indiferent că acestea îi sunt atribuite responsabilități de securitate ori nu.

Ideea vehiculată de unii analiști precum că modelele de securitate și intelligence s-au modificat urmare a noului spectru de riscuri și amenințări la adresa securității naționale și globale, considerate a fi cauze ale acestor modificări, este dificil de acceptat. Aceasta este o dificultate pentru simplul motiv că nu lasă nicio șansă de a explica nici cum ori de unde au apărut aceste riscuri și amenințări. Mai mult decât atât, cum situațiile catalogate drept riscuri și amenințări presupun nu doar momentul în care sunt considerate ca atare, ci mai ales circumstanțele prin care au evoluat în această stare, impun o abordare explicativă; altfel nu ar avea sens o întregă clasă de noțiuni de bază pentru securitatea oricărui sistem, desemnată în literatura ultimilor decenii prin „early warning”.

La o scară globală ori macro riscurile și amenințările sunt și ele efecte ale unor alți determinanți care le-au cauzat. Există în fapt o înlănțuire indusă printr-o primă inițiere identificabilă în dezvoltarea fără precedent a teoriilor științifice și aplicațiilor tehnologice. Apoi fenomenele clasice corespunzătoare inovării tehnologice conduc inevitabil la difuzia produselor lanțului de inovare care pe un interval suficient de lung diseminează interacții la nivel social.

Așadar, noile teorii științifice și inovarea tehnologică reprezintă cauzele principale – în sensul semnificației expresiei „factori de ordin unu” – ale schimbărilor societale, inclusiv a modificării proceselor de intelligence. Ceea ce discută, în fapt, cei ce susțin respectiva idee, amintită mai sus, se referă nu la un set de factori de influență de tip cauzal, ci la fenomenul adaptării acestor sisteme sociopolitice pe dimensiunea intelligence la noile condiții geostrategice. Acesta este un element important din punct de vedere al orientării care este bine să preceadă analiza.

Ca o consecință directă, în cadrul acestui tip de mecanism al dezvoltării globale și, prin urmare, al relațiilor internaționale s-a produs o mutație dinspre zona geopolitică către cea geoeconomică. Conceptul cheie al acestei mutații este reprezentat de avantajul competitiv, ce acum constă în abilitatea de a gestiona cunoașterea la nivel strategic, în special prin sisteme deschise, în toate sectoarele societății (administrație publică, industrii etc.), pentru crearea de bunăstare economică și socială, privite drept potențial de intelligence necesar garantării securității. Acest mod de a concepe lucrurile provine din gândirea legată de modelarea matematică: acolo în cadrul ciclului de avans al cunoașterii reprezentat de modelare se identifică o înlănțuire de factori cauzali de naturi distincte, se compun în mecanisme furnizându-se nu doar o descriere a fenomenului, ci o funcționare a acestuia. Această funcționare permite cel puțin două construcții esențiale pentru fenomenul decizional: simularea și generarea scenariilor. Simpla descriere ori identificare are un caracter static ori cel mult cinematic și, deși, este absolut necesară, devine total insuficientă după criteriile acțiunii politice în timp real. Problematika sustenabilității avantajului competitiv a impus extinderea și rafinarea precedentului mod de abordare și chiar în acest proces apare necesitatea ca intelligence-ul să migreze către intelligence/OSINT.

Pentru orice organizație, orientată către avantajul competitiv, abilitatea de a gestiona și administra o cultură a deschiderii și de a valorifica rezultatele acesteia a devenit la fel de importantă precum aceea de a gestiona cultura secretului. De găsirea raportului optim între aceste două componente depinde corectitudinea detectării căii către avantajul competitiv sustenabil. Gestionarea corectă a activităților din surse deschise duce de fapt la înțelegerea procesului de intelligence și la concentrarea corectă a resurselor prin întărirea activităților operative, derulate prin surse și metode secrete. Multe comunități de intelligence au întreprins pași decisivi pentru corectarea unora din cele mai sensibile dezechilibre și percepții în utilizarea intelligence-ului din surse deschise.

Dualitatea închis/deschis

Primul fapt relevant ce transpare din scurta discuție introductivă ce deschide prezenta secțiune constă în aceea că o întreagă concepție asupra semnificației cuvântului „securitate” trebuie adaptată cel puțin în raport cu toate cele patru elemente menționate drept precondiții ale unui domeniu complet. Pentru a da un exemplu, domeniile clasice ale geopoliticii ori relațiilor internaționale, azi și cu atât mai mult mâine, nu mai au nicio valoare în forma lor pur clasică – moștenită de la Morgenthau² spre exemplu pe paradigma realistă. Aceasta nu înseamnă, vreun moment, că trebuie omise, însă adaptările pe cele patru componente (cel puțin, teorie, strategie, doctrină, tehnologie) modifică din temelii sensul respectivelor cuvinte. Cum anume s-ar raporta cineva la cadrele actuale ale geopoliticii fără nicio cunoștință privitoare la știința regională a lui Isard³, reconceptualizările geoeconomice ale lui Krugman⁴ ori fără a face apel la reprezentările de tip GIS (Geographic Information System). În mod dual, cum anume s-ar angaja în analiză cineva fără a deține în propriul orizont de cunoștință consistentele contribuții ale lui Morgenthau, Rosenau⁵ etc. ori problemele deschise perene identificate de Alker⁶ în domeniul relațiilor internaționale – este ca în cazul șahului cu portofoliul de partide celebre. Pe scurt, paradigma deschiderii nu conține numai problema de natură informațională, ci și modul în care știm ca națiune să alocăm rolul corect componentei clasice în contextul turbulent al provocărilor viitoare. Iar asta din componenta teoretică, deoarece cuvântul practic de acolo își trage semnificația – cum legăm teoria de acțiune. Din nefericire, mentalul practicat în România în ultimii 60 de ani are foarte puțin de a face cu această concepție, iar acest fapt face și mai dificilă implementarea ei.

² Hans Morgenthau – unul dintre inițiatorii și principalii contributori ai realismului în relațiile internaționale.

³ Walter Isard – unul dintre inițiatorii și principalii contributori ai domeniului “Regional Science”.

⁴ Paul Krugman – unul dintre principalii contributori ai domeniului de interferență între geopolitică, geoeconomie, comerț internațional, ca și continuare a ideilor lui Isard.

⁵ James Rosenau – printre primii contributori în relațiile internaționale care au aplicat teoria complexității pornind de la o analogie cu un fenomen din mecanica fluidelor, turbulența.

⁶ Hayward Alker – unul dintre fondatorii cercetării fundamentale în relațiile internaționale; a identificat problemele deschise transdisciplinare ale domeniului.

Rolul sistemelor deschise

Ascensiunea „deschiderii” în activitatea de intelligence merge dincolo de spectrul informației din surse deschise. În acest context, există comunități naționale de intelligence care încearcă să nu rămână în urma evoluției și dezvoltării tehnologice, unde tonul este dat de proliferarea sistemelor deschise – *mișcarea open source* a început de fapt în domeniul software, lucru ce nu trebuie să mire pe nimeni deoarece pentru a comunica fără frontiere este nevoie de un mijloc ... tehnologic.

Într-o nouă abordare, privind dezvoltarea unei culturi intelligence bazate pe deschidere și noi forme de comunicare, Comunitatea de Intelligence a SUA a anunțat, încă din 2006, dezvoltarea platformei Intellipedia, la cinci ani după apariția Wikipedia, iar recent, în 2009, a făcut publică informația privind dezvoltarea platformei A-Space, proiectată după modelul de succes al site-ului de rețele sociale MySpace, lansat online în 2003. Prin urmare, agențiile FBI, CIA și ale Departamentului Apărării au lansat asemenea platforme ce au la bază software-ul social.

Modul de gestionare a cunoașterii, la nivel organizațional, depinde la ora actuală în mod direct de utilizarea intelligence-ului colaborativ, care nu se mai bazează pe, ci transcede structurile de tip piramidal. În acest sens, în cadrul serviciilor de intelligence procesul de management al cunoașterii nu se mai desfășoară în mod sistematic în spatele ușilor închise. ISD este cunoscută de toți participanții la procesul de intelligence. Inițiativa, lansarea alertei informative, comunicarea și colaborarea în timp real au devenit factori care asigură succesul managementului strategic la nivelul cunoașterii în serviciile de intelligence.

Intelligence-ul din surse secrete este potențat de înțelegerea rolului și locului informației din surse deschise în cadrul ciclului de intelligence și de diseminare a OSINT nu numai în departamentele serviciilor de intelligence, ci, mai ales, atât la nivel național, cât și pentru partenerii externi.

Necesitatea abordării formalizate și extinse a procesului OSINT impune ca spațiul informațional din surse deschise să fie mai întâi înțeles, iar apoi trebuie proiectat, modelat, implementat, administrat și evaluat pentru a asigura suportul informațional al deciziei factorului politic în îndeplinirea obiectivelor strategice ale națiunii.

Pentru a înțelege un domeniu, cum este și cazul OSINT, orice organizație are nevoie de elaborarea unei teorii, a unei strategii și doctrine și, abia apoi, a proiectelor tehnice pentru dezvoltarea și implementarea

tehnologiilor asociate. Tehnologia, în sine, nu poate soluționa problemele organizaționale. În acest sens, Bruce Schneier subliniază în mod concludent faptul că „*If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology*”⁷.

Eșecurile înregistrate la nivel organizațional sunt determinate, de cele mai multe ori, de neînțelegerea dimensiunilor de abordare a unui domeniu. De aceea, reconfigurarea organizațiilor prin intermediul conceptelor reprezintă calea logică de urmat, deoarece nu se are în vedere numai funcționarea ca atare a organizației, ci mai ales capacitățile capitalului uman, începând de la anticipare și terminând cu reziliența.

Înțelegerea și definirea conceptelor dau forma de organizare și regulile de funcționare a entităților ce abordează un domeniu conceput în interdependență cu mediul.

Atributele ISD

ISD este echivalată, în plan social, cu informația publică iar gestionarea resurselor informaționale la nivel național devine o problemă importantă pentru securitatea națională. Pentru a decide dacă ISD se poate echivala în plan intelligence/OSINT cu informația publică este, bineînțeles, nevoie fie să definim informația publică (lucru doar aparent abordabil), fie să definim domeniul intelligence/OSINT. Dacă adoptăm prima variantă riscăm să nu avem nicio legătură cu domeniul intelligence/OSINT; de altfel, până și cei care au practicat această cale, concentrată pe dimensiunea științelor sociale și a abordărilor pur discursive, au ajuns la necesitatea de a introduce perspectiva analitică în problemă. Cel puțin din acest motiv este nevoie de *intelligence analitic* și *academic*. Filosofia proiectului nostru urmează în fapt mecanismul adoptat pentru a da sens cuvântului practică. De aceea, vizează o altă perspectivă axată pe o viziune asupra domeniului intelligence/OSINT, consonantă cugetării academice, dar integrând semnificația respectivului cuvânt, practică – în sensul specificat mai sus – la toate nivelurile construcției. Evident, detaliile asupra acestui punct sunt expuse în alte lucrări și omitem aici orice alte considerații asupra esenței subiectului menționat.

⁷ Bruce Schneier, *Secrets & Lies. Digital Security in a Networked World*, John Wiley & Sons, 2000.

Gestionarea ISD devine o componentă a unei noi funcții de intelligence la nivel național: **intelligence-ul „deschis”** care presupune în primul rând **transfer de cunoaștere** a procesului de intelligence în interiorul și între toate **sectoarele societății**. Acest fapt a determinat lansarea unor inițiative de către guvernele statelor occidentale, precum:

- înființarea unor departamente de intelligence, denumite intelligence competitiv, conduse de un ministru adjunct sau implementarea unui concept de intelligence teritorial, astfel încât toți prefecții să urmeze cursuri de pregătire în domeniu – cazul Franței fiind cel mai ușor de studiat dar relevant pentru statele cu mental societal compatibil cu această cultură;
- dezvoltarea conceptului de intelligence competitiv la nivelul mediului de afaceri – SUA, Marea Britanie, Suedia, Franța, Germania, iar în ultimul deceniu țările BRIC – Brazilia, Rusia, India, China – dar și țări precum Singapore, Africa de Sud etc.

Având în vedere spectrul larg de distribuție la nivel global, abordarea eficientă a ISD va putea fi realizată doar printr-un angajament comun al tuturor actorilor interni ai unui stat – fapt ce prelungește și adaptează conceptul de „intelligence organizațional” lansat în anii '70. De altfel, nicio entitate din această lume (organizație privată sau publică, stat sau organism internațional) nu va putea să acopere ISD decât printr-o organizare de tip rețea. Reușita unui asemenea demers implică identificarea nodurilor importante din rețea, prin intermediul cărora un serviciu de informații se poate conecta la sistemul deschis. Parteneriatele încheiate cu aceste noduri vor conduce la gestionarea eficientă a ISD și la decizii cheie privitoare la participarea în procesele cerute de intelligence-ul alianțelor.

Deoarece ISD este o sursă de informații în cadrul serviciilor de intelligence, abordarea sursei, strategia, intențiile, metodele, procesele și produsele acesteia sunt clasificate. În cazul ISD, însă, pot fi elaborate proceduri prin care, în cadrul unei politici de transparență/opacitate, anumite produse OSINT devin publice. De regulă, produsele devin publice, însă, mai rar metodologiile, foarte rar metodele și tehnicile, și extrem de rar modelele.

În funcție de aria de interes și zonele de responsabilitate în care se poziționează actorii naționali, OSINT se transformă dintr-o sursă de informații a sistemului de surse intelligence într-un domeniu, o resursă, un proces, un produs, o organizație și o capacitate de interes național. În realitate vorbim despre apariția unui nou tip de intelligence ce poate fi derulat la nivelul

oricărei entități organizaționale: *intelligence deschis*. În termeni strict practici, intelligence este un proces de culegere, achiziție și generare a informației și informării, nu cunoașterii. De aceea, părintele intelligence-ului competitiv suedez, Stevan Dedijer afirma faptul că *spionajul este în agonie (pe moarte)*⁸ și numai organizațiile care își vor dezvolta strategii de achiziție a cunoașterii vor supraviețui în viitor, pe o piață din ce în ce mai competitivă și în continuă schimbare. Intelligence nu mai este apanajul exclusiv al serviciilor speciale, deoarece, implicând cunoașterea în problematica intelligence, este imposibil, în actualul stadiu, a nu face aceasta câtă vreme vorbim de avantaj competitiv. Intelligence poate realiza orice organizație orientată spre gestiunea și administrarea eficientă a cunoașterii. Cum însă, în acest context, OSINT nu se reduce nici la surse și cu atât mai puțin la ceea ce a împrumutat inițial de la intelligence, devine un punct cheie înțelegerea semnificației interacției între intelligence *secret* (IS) și intelligence *deschis* (ID), ce are loc în mediul intelligence/OSINT. Aceasta este o altă fațetă a dualității ce a ajuns să se impună natural în reconfigurarea conceptelor secret, securitate etc. iar statele care fie nu au sesizat-o fie au întârziat prea mult repoziționarea în raport cu această viziune plătesc prețul ignoranței celor ce au indus acest retard.

Redefinirea intelligence

Discursul și literatura de specialitate intelligence a anilor '90 scot în evidență o poziționare restrânsă asupra conceptului OSINT, în sensul limitării ariei de concentrare și cuprindere doar la nivelul serviciilor de intelligence.

Analiza evoluției domeniului OSINT în ultimele două decenii subliniază faptul că principalii jucători ai spațiului informațional din surse deschise, serviciile speciale, au început să repoziționeze conceptul OSINT într-o manieră care legitimează apariția de noi instituții și noi tipuri de leadership, precum și noi mecanisme de finanțare ale domeniului care să ducă la eficientizarea activităților în paralel cu creșterea volumelor informaționale, cu necesitatea protejării propriului spațiu informațional, a creșterii capacității și capabilităților de analiză etc. (Fig. 1)⁹.

⁸ Stevan Dedijer, "Doing Business in a Changed World: The Intelligence Revolution and Our Planetary Civilization", *Competitive Intelligence Review*, Vol. 10 (3), John Wiley & Sons, Inc., 1999, pp. 67-78.

⁹ Doug Naquin, „Building OS Enterprise”, *DNI Open Source Conference*, 11-12 September 2008.

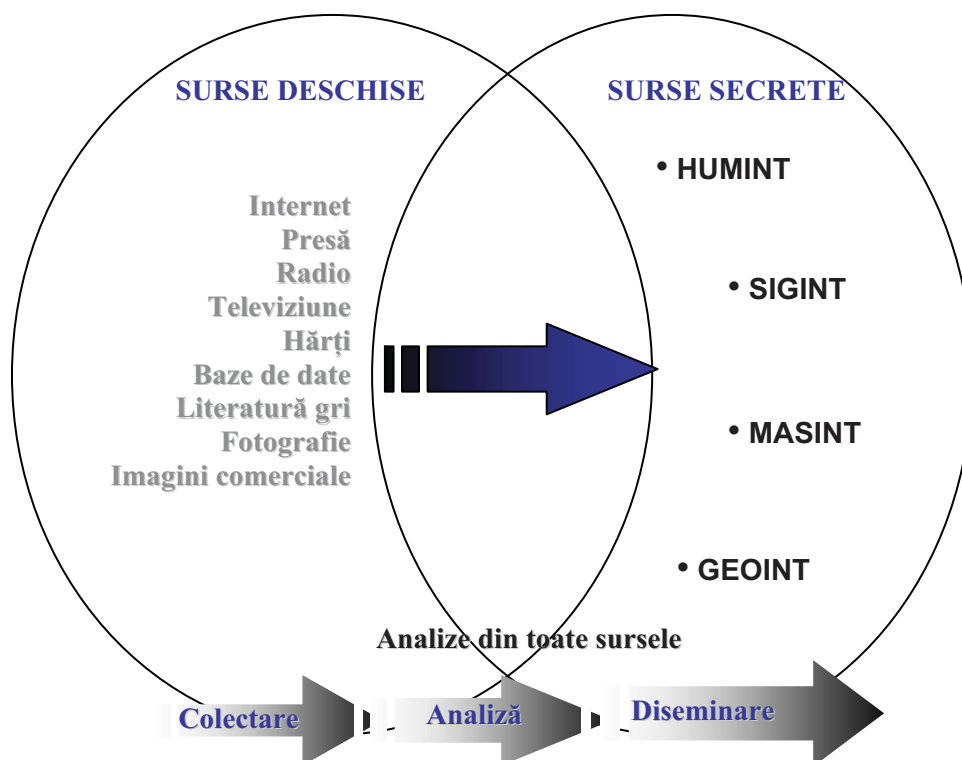


Fig. 1 Exploatarea focalizată a Open Source va conduce la eficientizarea cheltuielilor oricărei Comunități de Intelligence

Intelligence din Surse Deschise (OSINT) este intelligence-ul produs din informațiile disponibile în mod public, care printr-un proces de culegere și exploatare sunt diseminate într-o manieră oportună către o audiență specifică, în scopul soluționării unei cerințe particularizate de intelligence; aceasta este o definiție tradițională și, în acest stadiu al demersului, ne limităm la ea.

Datorită *Revoluției Informaționale*, cantitatea, semnificația și accesibilitatea informației din surse deschise a explodat într-o creștere de tip exponențial în raport cu capacitățile și capabilitățile accepțiunilor clasice de culegere, analiză, configurare decizională și chiar diseminare. Unele servicii de intelligence nu și-au extins, concomitent/imediat, eforturile și sistemele de exploatare și producere a OSINT, ceea ce a avut drept consecință majoră

un potențial redus de adaptare, atât din punct de vedere al indicatorilor obiectivi, cât și mai ales din punct de vedere al capitalului uman. Pe această ultimă dimensiune, majoritatea țărilor ce nu au preparat respectiva adaptare, menținând sisteme rigide când viitorul previzibil cerea sisteme flexibile, au intrat într-o stare de ignoranță relativ la semnificația acestui domeniu. Faptul esențial nesesizat la timp este următorul:

- *Într-o societate a cunoașterii, în care avantajul competitiv asigură sustenabilitatea securității, numai dacă sunt integrate toate componentele noii semnificații, oferită de domeniul intelligence/OSINT se poate dobândi potențial de adaptare.*
- *Cine nu își gestionează propriile stări de ignoranță consonant cu tendințele induse de societatea cunoașterii și stă cu elita economică într-o stare axată numai pe mentalul tangibil întreținut pur cognitiv pe „simplu” și „practic”, iar cu restul națiunii numai în starea de user își afectează perenitatea propriei identități.*

O națiune de useri într-o societate a cunoașterii este echivalentul unei națiuni de consumatori din timpul războiului rece, de tipul blocului sovietic iar în acest caz se cunoasc consecințele – falimentul economic și dispariția unei organizări statale tributară unui mod de gândire ce nu mai putea fi adaptat. Falimentul economic este numai primul pas dintr-un lanț întreg de consecințe ce sunt descrise destul de clar în altă parte. Aici este un punct ce trebuie pus la baza redefinirii intelligence/OSINT orientată către dezideratele enunțate în introducere.

Producția de OSINT a devenit astăzi unul dintre indiciile ce dovedesc prin indicatori specifici existența unei discipline, recte intelligence/OSINT, și valoarea pe care intelligence reușește să o aducă. Modul în care trebuie integrată în ciclul de intelligence, pentru a ne asigura de faptul că orice factor decizional, nu numai cel politic, este pe deplin informat, este cel mai vizibil mod de a îi sesiza utilitatea, însă nu este singurul.

Evoluția OSINT a ultimelor două decenii și schimbarea de paradigmă dinspre o cultură a secretului înspre una a deschiderii configurează o nouă imagine a intelligence-ului pe două componente complementare: *intelligence secret* și *intelligence deschis*.

Dacă este să concentrăm principalele atribute ale modelului de intelligence al secolului XXI, o reprezentare, simplu de definit, ar fi:

- **secretul este invizibil și produce;**
- **deschiderea este vizibilă și dă formă.**

În concluzie, cele două atribute fundamentale ale activității intelligence configurează două componente complementare ale domeniului, intelligence secret și intelligence deschis. Acestea trebuie definite, descrise, structurate prin prisma conceptelor sociale de rețea și organizație, a celor tehnologice de rețele și sisteme, precum și a celor corespondente identității entităților la care sunt atașate.

(Va urma)

Bibliografie

1. Bruce Schneier, *Secrets & Lies. Digital Security in a Networked World*, John Wiley & Sons, 2000.
2. Stevan Dedijer, "Doing Business in a Changed World: The Intelligence Revolution and Our Planetary Civilization", *Competitive Intelligence Review*, Vol. 10 (3), John Wiley & Sons, Inc., 1999.
3. Doug Naquin, „Building OS Enterprise”, *DNI Open Source Conference*, 11-12 September 2008.

Marian SEBE este conferențiar universitar la Academia Națională de Informații „Mihai Viteazul”, doctor în sociologie, titular al disciplinei „Intelligence în secolul XXI”, coordonator al unor programe de cercetare în domeniul intelligence, a publicat articole și studii care valorifică experiența acumulată în domeniul securității și intelligence-ului.