

Intelligence și globalizare

Neag, Mihai Marcel; Simion, Eduard; Kis, Alexandru

Veröffentlichungsversion / Published Version

Monographie / monograph

Empfohlene Zitierung / Suggested Citation:

Neag, M. M., Simion, E., & Kis, A. (2015). *Intelligence și globalizare*. Sibiu: Editura Techno Media. <https://nbn-resolving.org/urn:nbn:de:0168-ssoar-73540-7>

Nutzungsbedingungen:

Dieser Text wird unter der CC0 1.0 Universell Lizenz (Public Domain Dedication) zur Verfügung gestellt. Nähere Auskunft zu dieser CC-Lizenz finden Sie hier: <https://creativecommons.org/publicdomain/zero/1.0/deed.de>

Terms of use:

This document is made available under the CC0 1.0 Universal Licence (Public Domain Dedication). For more information see: <https://creativecommons.org/publicdomain/zero/1.0/deed.en>

Mihai Marcel Neag

Eduard SIMION

Alexandru KIS

~ INTELLIGENCE ȘI GLOBALIZARE ~



EDITURA TECHNO MEDIA
Sibiu, 2015

Biblioteca Națională a României

Descrierea CIP a Bibliotecii Naționale a României

ISBN 978-606-616-189-3

Coperta: Alin KIS ©

CUPRINS

CAPITOLUL 1. INTELLIGENCE ÎN ERA GLOBALIZĂRII. COMUNITĂȚILE DE INTELLIGENCE ÎN SOCIETATEA GLOBALĂ	...4
CAPITOLUL 2. CAPABILITATEA INTELLIGENCE ÎN NATO	...27
CAPITOLUL 3. INTELLIGENCE SOCIO-CULTURAL	...40
CAPITOLUL 4. INTELLIGENCE DIN SURSE UMANE. ÎNTRE SPIONAJ ȘI CULEGEREA DE INFORMAȚII DIN SURSE UMANE LA NIVEL OPERAȚIONAL ȘI TACTIC	...57
CAPITOLUL 5. OSINT ÎN ACTIVITATEA DE INTELLIGENCE	...68
CAPITOLUL 6. ELEMENTE CHEIE ALE ANALIZEI INFORMAȚIILOR ÎN CONTEXTUL GLOBALIZĂRII	...87
CAPITOLUL 7. INTELLIGENCE PRIVAT – DE LA SECURITATE LA COMPETITIVITATE PRIN INTELLIGENCE	...99
CAPITOLUL 8. CONTRAINFORMAȚIILE ȘI SPECTRUL AMENINȚĂRILOR LA ADRESA SECURITĂȚII	...113
CAPITOLUL 9. SITUAȚIILE DE CRIZĂ ȘI EȘUAREA STATALĂ – O PROVOCARE PENTRU ANALIZA DE INTELLIGENCE	...124
CAPITOLUL 10. CENTRUL DE EXCELENȚĂ NATO ÎN DOMENIUL HUMINT DIN ORADEA – UN MODEL INSTITUȚIONAL DE DEZVOLTARE A UNEI CAPABILITĂȚI DIN SPECTRUL INTELLIGENCE	...144
CAPITOLUL 11. INTELLIGENCE ȘI AMENINȚĂRILE DIN MEDIUL CIBERNETIC	...159

CAPITOLUL 1. INTELLIGENCE ÎN ERA GLOBALIZĂRII. COMUNITĂȚILE DE INTELLIGENCE ÎN SOCIETATEA GLOBALĂ

Introducere

Lucrarea de față urmărește să contribuie la dezvoltarea culturii de securitate a publicului larg prin dezvoltarea unor aspecte generale legate de domeniul Intelligence, în special în condițiile actuale ale evoluției mediului de securitate, marcat decisiv de procesul de globalizare.

În cadrul temelor subscrise acestui demers, voi recurge la identificarea principalelor aspecte care marchează transformarea cerințelor de securitate, care determină adaptarea comunităților de Intelligence în materie de structură, dotare, funcționare și operare în efortul lor de a furniza produse specifice în sprijinul procesului decizional, la orice nivel de referință.

Securitatea în contextul globalizării

Globalizarea este un proces cu efecte multiple în toate domeniile existențiale, efecte a căror înțelegere este necesară deoarece schimbă fundamentele analitice cu care ne-am obișnuit, modificând percepții, comportamente și atitudini într-o largă varietate de opțiuni și cauzalități, ce pot fi traduse în beneficii sau dezavantaje. Modalitățile de cuantificare ale acestora diferă, la rândul lor, în funcție de interesele, obiectivele și cultura organizațională a instituțiilor care le abordează.

Globalizarea întrunește poziții opuse ale suporterilor - care o văd ca factor pozitiv de presiune în favoarea politicilor democratice și a economiei de piață, cu rezultate directe în ce privește o populație globală cu standarde de viață superioare - și ale criticilor - care consideră că globalizarea servește doar interesele corporațiilor transnaționale, subminează democrația, accelerează degradarea mediului înconjurător, impune omogenitatea culturală și duce la escaladarea stărilor de conflict. (Frost, 2002, 35)

În plan filozofic, perspectiva realistă asupra globalizării apreciază că modalitatea în care aceasta influențează aspectele sociale, economice, culturale etc. nu este de natură să modifice în mod critic sistemul internațional actual, în care statele sunt principalii actori în competiția pentru putere și influență, în timp ce curentul idealist privește acest proces ca fază superioară a evoluției sistemului internațional, în care actorii non-statali intră în competiție cu statele.

La nivel global, asimetriile generatoare de dezechilibre se regăsesc în multiple domenii de activitate. În economie, concentrarea progresului tehnic și tehnologic în țările dezvoltate, ca sursă principală a creșterii lor economice, vulnerabilitatea macroeconomică ridicată a țărilor în curs de dezvoltare la șocurile externe, precum și contrastul dintre gradul înalt de mobilitate a capitalului și mobilitatea internațională a muncii, în special forța de muncă necalificată, pot constitui surse de instabilitate (criză economică și socială) și produc situații de risc la adresa securității. Gestionarea economicului este puternic subordonată factorului politic, reverberațiile dezechilibrelor de natură economică găsindu-și o puternică reprezentare în stabilitatea și coeziunea comunităților.

Totodată, globalizarea reduce capacitatea statelor de a menține monopolul asupra informației și puterii, accentuează permeabilitatea granițelor și permite actorilor nonstatali să acumuleze capital. Organizațiile societății civile se dezvoltă și încep să acționeze global, fără intermedierea guvernelor naționale pe care le concurează ca reprezentate legitime în promovarea intereselor comunităților, mai puțin interesate de expresia politică, cât de acțiuni concrete care să le sprijine dezvoltarea și bunăstarea.

Pentru a contracara această influență, sistemele politice naționale trebuie să dea dovadă de flexibilitate și să își dezvolte capacități de acțiune coordonată/ integrată, să redevină exponente ale intereselor maselor largi (promovând o formă avansată, modernă, a modelului statului social) și să evite alienarea funcțională (înțelegând prin aceasta aservirea și subordonarea energiei politice unor scopuri pur clientelare).

Din definiția globalizării nu trebuie eliminată dimensiunea militară, care, în ultimii ani, s-a manifestat în special prin lupta împotriva terorismului și fenomenelor de insurgență, mai mult sau mai puțin asociate acestuia. În contextul globalizării, această interconectare și „afiliere” este un argument necesar și suficient pentru a putea afirma că securitatea unei zone date este inseparabilă de securitatea globală. Cu toate că formele tradiționale de luptă împotriva pericolelor și amenințărilor la adresa securității internaționale - alianțele militare - sunt încă necesare eliminării factorilor și surselor de insecuritate ce se globalizează, simpla proiecție a puterii militare a statelor nu mai este suficientă. Conflictul, de orice natură, capătă noi caracteristici, suferind dezvoltări cărora statele și instituțiile internaționale nu sunt pe deplin pregătite să le facă față, dar la care reacționează printr-un proces adaptativ ad-hoc.

Putem afirma că, prin dimensiunile sale de manifestare, globalizarea crează germenii unor presiuni ce influențează mediul internațional de securitate, dar și modul în care percepția securității se reflectă la nivelul experiențelor de securitate fizică și spirituală ale fiecărui individ¹. În ansamblu, globalizarea conduce la o nouă structură internațională, divizată între acele țări care sunt integrate în economia globală și cele care fie sunt lăsate în urmă, fie se opun normelor unei noi ordini globale.

Peisajul securității la nivel politico-militar este completat de trendurile globale privind creșterea populației, inegalitățile în dezvoltarea economică, urbanizarea, pandemiile, dezvoltările în domeniul biotehnologiei, aspectele ecologice și încălzirea globală, scaritatea resurselor, etc.

În acest context, principala provocare a perioadei post-război rece este, cu certitudine, reaşezarea coordonatelor echilibrului de putere (în sens multidimensional) la nivel global. Perioada „unipolarității” (SUA ca principal agent de putere la nivel global) a constituit doar segmentul de tranziție care a reliefat nevoia de reformă în înțelegerea noilor repere ale interdependențelor dintre actorii arenei internaționale. Noua arhitectură de securitate se manifestă ca un teren competițional în care se redefinesc sisteme de referință, repere relaționale și niveluri de ambiție, în virtutea unor seturi de valori și interese mai mult sau mai puțin diferite, dar care poziționează statele în raport cu principalele entități - ”subiecte” și ”obiecte” ale scenei relațiilor internaționale.

Statele se definesc, din această perspectivă, ca puteri² (tradiționale/ emergente) – atribut dat de potențialul politic, economic, militar¹ al acestora – în antiteză cu statele

¹ ***, Department of Social and Cultural Anthropology, *Constructing Human Security in a Globalizing World*, (2007), în <http://www.fsw.vu.nl/en/research/research-programmes/social-and-cultural-anthropology/index.asp>

² Conceptul de putere capătă o înțelegere nuanțată. Dacă Joseph Nye o lega exclusiv de atingerea obiectivelor și scopurilor propuse (în virtutea unui program predefinit) (Nye Jr., 1990, 177), dicționarele definesc puterea: ca abilitate de a face anumite lucruri în parametri doriți și capacitate de exercita control/ autoritate/ influență (Oxford Mini Dictionary&Thesaurus); ca statut de forță și capacitate de proiectare a acesteia (The American Heritage Dictionary of the English Language); ca entitate politică ce se bucură de soliditate politică, industrială sau militară și ca potențial militar (Collins English Dictionary). P. Duțu și C. Bogzeanu detaliază principalele criterii de putere ale statului (definitorii pentru statutul său internațional și rolurile asumate pe scena globală):

problemă (ce experimentează diferite stadii și variabilități ale crizei). În concertul relațiilor dintre acestea intervin organizațiile internaționale guvernamentale și o întreagă pleiadă de actori non-statali (organizații ale societății civile, rețele teroriste, firme transnaționale, etc).

Din punct de vedere al solidității și maturității conceptuale, nivelul de referință fundamental îl constituie securitatea națională, pornind de la premiza atenției pe care statele o acordă balanței puterii și concurenței cu competitorii direcți (în cursa pentru resurse, influență, prezervarea valorilor, promovarea intereselor, etc).

La acest nivel, factorii generatori de crize politico-militare sunt bine conturați și se raportează la vulnerabilități și amenințări interne sau externe la adresa structurii și funcționalității sistemului statal (Oprea, 2013, 53), manifestate pașnic (Gene, 2012) sau prin recurgere la violență. Făcând o comparație între perioada războiului rece și etapa actuală distingem o dezvoltare și diversificare semnificativă a acestora – în special în contextul globalizării, fapt ce antrenează nevoia de adaptare a instrumentelor de cunoaștere, a proceselor decizionale și a elementelor de suport (incluzând aici și spectrul *intelligence*).

Statul își prezervă statutul de principal reper ca sistem de securitate la care se raportează ființa umană atunci când își evaluează existența și perspectivele. Prin mecanismele complexe dezvoltate în timp, statul – într-o formulă a sa ideală – este garantul securității fizice și demnității cetățenilor, promovând premisele bunăstării și asigurând libertatea individuală de exprimare și opțiune. Strategia de securitate națională a României (SSNR, 2006, 4) își definește scopul ca vizând ”*atât prevenirea și contracararea pericolelor generate de mediul internațional, cât și garantarea stării de securitate internă, în ansamblul său, a siguranței personale și securității comunităților*”, cerințe raportate la aspecte privind: securitatea individuală, securitatea energetică și alimentară, securitatea transporturilor și a infrastructurii, securitatea sănătății publice, sanitară, ecologică și culturală, securitatea financiară, informatică și informațională.

Pe de altă parte, în condițiile în care resortul principal al globalizării rezidă în dezvoltarea economică, aspecte ca: accesul la resurse, securitatea căilor de transport, dezvoltarea capacităților de producție, asigurarea forței de muncă adecvate (nivel de calificare în balanță cu costul acesteia), găsirea și prezervarea de noi piețe de desfacere, transferul de bunăstare, pierderea exclusivităților, accesul la informație, duc la reconsiderarea distribuției rolurilor ierarhice ale statelor în sistemul relațiilor internaționale.

Faptul că majoritatea manifestărilor violente pornesc de la motivații de natură etnico-religioasă (Dinu, 2005), teritorială și/sau ideologică, iar o relativă reducere a violenței militare este asociată cu creșterea violenței politice, economice și tehnologice (Vasilescu, 2009), reprezintă un argument în plus că toate aceste aspecte trebuie avute în vedere în cadrul analizelor stării de securitate.

Procesul re poziționării statelor pe scena relațiilor politice internaționale are o puternică semnificație în plan intern. Dobândirea unor avantaje economice strategice, asigurarea unui nivel decisiv de influență în evoluția unor procese vitale, controlul procesualităților sistemice, prezervarea securității naționale (și reflectarea propriei securități la nivel regional și global), ca obiective ale politicilor internaționale, toate se reflectă în politica internă.

populația, diaspora, forța militară, autonomia strategică, capacitatea de proiecție, puterea nucleară, sistemele de alianțe, protecția asigurată propriilor cetățeni, economia, cultura, educația, modelul, coeziunea socială, funcționarea instituțiilor, asumarea voluntară, activă și responsabilă de roluri diferite, ca natură și durată, pe scena mondială (Duțu și Bogzeanu, 2010, 36-40). O analiză asupra puterii din perspectiva securității umane este disponibilă în Kis, 2012, 66-68.

¹capacitatea de apărare națională prin mijloace militare autonome este centrală pentru concepția modernă de stat suveran, însă acesteia i se adaugă potențialul generat de emergența aspectelor legate de capitalul multidimensional de resurse

Proiectarea acestor interese nu se poate rezuma însă strict la teritoriul național, situație în care echilibrul obținut ar fi unul precar, supus contagiunii vecinătăților și conexiunilor insecurizante. Securitatea fiecărei națiuni trebuie concepută în context mult mai larg, care acceptă anumite ierarhii și dinamici multidimensionale, dar nu și compromisuri care să alieneze spiritul "contractului social" pe care apartenența la o formă de organizare statală o presupune. Alianțele și aliații sunt esențiali în a gestiona aspectele de securitate ale globalizării, atât din perspectiva resurselor, cât și a succesului acestei întreprinderi.

În acest sens, dorim să subliniem predilecția pe care abordarea analitică a problemelor de securitate o are privind sistemele teritoriale regionale, în care abordarea individuală a problemelor de securitate ale unei națiuni ar fi lipsită de realism fără corelarea cu aspectele similare ale vecinătăților. Barry Buzan denuște aceste sistem teritorial "*complex de securitate*" (Buzan, 2000, 196), în care interacțiunile militare, politice, economice, socio-culturale transcend – facilitate de realități geopolitice – legăturile funcționale cu alte state, sub "cupola" globalizării.

Dezvoltarea, la nivel global, a unui mare număr de organizații și agenții internaționale indică o atenție crescută a statelor cu privire la viața economică și socială a popoarelor. Sprijinul pe care statele și-l acordă bilateral sau multilateral capătă o importanță aparte, securitatea socială depășind tot mai mult barierele naționale, cunoscând succesiuni graduale ale dezvoltării către limite teritoriale regionale.

Pe de altă parte, disfuncțiile interne sau cele de relaționare externă ale statelor se traduc în tensiuni care pot evolua în stări de criză sau chiar conflicte armate. Aceste distorsiuni ale stării de normalitate reclamă intervenția sistemelor de securitate configurate tocmai în vederea diminuării riscurilor identificate – de aici reieșind rolul pe care organizațiile internaționale interguvernamentale îl au în domeniul securității.

Organismele internaționale au un rol aparte în procesul de evaluare continuă a situației de securitate la nivel regional și global¹, prin analiza și reconsiderarea permanentă a priorităților de securitate regională și globală și adaptarea conceptelor de securitate în raport cu noile evoluții din toate domeniile de referință.

În NATO, din perspectiva interesului pentru domeniul intelligence, sunt recunoscuți o serie de factori cheie ce își pun amprenta asupra dezvoltării acestei capabilități ca necesitate pentru asigurarea superiorității decizionale în caz de risc de securitate în oricare dintre domeniile amintite: terorismul, statele ostile (în mod direct sau prin intermediari), statele fragile (sau în colaps), amenințările hibride², globalizarea (prin nucleele de instabilitate pe care le provoacă și caracterul transnațional al amenințărilor), fenomenele de mediu (dezastre naturale asociate cu urgențe umanitare și instabilitate) și proliferarea rachetelor balistice, a armamentului nuclear și a altor arme de distrugere în masă.

De la dihotomia securitate națională - securitate internațională la securitatea umană. Către un nou cadru de referință în câmpul informațional

Specific evoluției adaptării abordărilor în domeniul securității dictate de schimbările induse de procesul de globalizare, conceptul de securitate umană a fost lansat în anul 1994, în cadrul Programului Națiunilor Unite pentru Dezvoltare (UNDP), prin "Raportul anual asupra

¹Modelul liberal al securității internaționale se bazează pe utilizarea a patru instrumente: dreptul internațional (substituie rezolvarea diferendelor prin conflict armat), organizațiile internaționale, integrarea politică și democratizarea. Organizațiile internaționale sunt folosite de către comunitatea internațională în scopul întăririi dreptului internațional și a prevenirii sau stopării agresiunii.

²Amenințările hibride constă în combinarea adaptată și sistematică (Aaronson și alții, 2011) a amenințărilor convenționale, neregulate și asimetrice în același timp și în același spațiu, folosite de adversari în vederea atingerii unor obiective (IMSM-0292-2010). P. Duțu diferențiază caracterul hibrid al amenințărilor prin raportarea la cadrul organizațional și metodele și mijloacele folosite de beligeranți (Duțu, 2013, 46).

dezvoltării umane”¹, fiind dezvoltat ulterior în cadrul a două curente (școli) distincte – absența fricii (*freedom from fear*) și absența nevoilor (*freedom from wants*) (UNDP, 1994, 24). Concret, *absența fricii* se referă la protejarea indivizilor de conflicte violente, asociate cu sărăcia, lipsa capacităților statale de suport și a altor forme de inechitate (promovând ca soluții: asistența de urgență, prevenirea și rezoluția conflictelor, construcția păcii), pe când *absența nevoilor* reprezintă o abordare holistică a rezolvării necesităților umane legate de: foamete, boli, dezastre naturale, care afectează mult mai mulți oameni decât conflictele violente (și vede ca rezolvare a acestor surse de insecuritate focalizarea pe dezvoltare). Raportul Secretarului General al ONU - "*In Larger Freedom: Towards Development Security and Freedom for All*" (2005) - a formulat o a treia dimensiune a conceptului de securitate umană: "*libertatea de a trăi în demnitate*"², dimensiune ce militează pentru necesitatea promovării regulii de drept și a democrației.

Școala "absenței fricii" a căutat să impună ca subiect esențial primatul protecției indivizilor în fața conflictelor violente³ (de aici decurgând asigurarea condiției minimale pentru drepturile și libertățile recunoscute), abordare considerată ca asigurând dimensiuni realiste și gestionabile demersurilor analitice, operând cu termeni ca "asistența în caz de urgență" (*emergency assistance*), "prevenirea și încheierea conflictelor" (*conflict prevention and resolution*), "construcția păcii" (*peace-building*), dar și cu o componență cheie a agendei sale, care a determinat o adevărată revoluție în modalitatea de interpretare a ideii de suveranitate statală – conceptul "responsabilității de a proteja"⁴.

Curentul absenței nevoilor ca și condiție primordială a securității umane (conceptul "extins" al securității umane) pornește de la premiza că foametea, bolile și dezastrele naturaleucid de departe mult mai mulți oameni decât războaiele, genocidul și terorismul la un loc, fiind necesară asocierea acestora celorlaltor amenințări la adresa securității umane. Eliberarea de nevoi, dincolo de asocierea cu violența în diferitele ei forme de manifestare, promovează necesitatea analizei tuturor aspectelor care aduc atingere a ceea ce este acceptat ca definind securitatea individului, punând accentul pe obiective de dezvoltare multidimensională.

Libertatea de a trăi în demnitate corespunde beneficiului accesului la drepturi civile și politice ca: dreptul inerent la viață, nesupunerea la tortură sau acte de cruzime, la arest sau detenție ilegală, dreptul la prezumția de nevinovăție, la un proces rapid și corect, dreptul la liber sufragiu, la intimitate, la libertatea de expresie, asociere și întrunire. Această libertate cuprinde și drepturile economice, sociale și culturale – dreptul la hrană, sănătate, educație și protecție socială, dreptul la muncă, dreptul de a participa la viața culturală a comunității și a se bucura de beneficiile progresului științific și a aplicațiilor sale. Demnitatea, ca dimensiune a trăirii, presupune absența oricărei forme de deprivare, ca: foametea, ignoranța, incapacitatea, dizabilitatea și boala. Oamenii trebuie să fie în măsură să se protejeze de orice formă de

¹<http://hdr.undp.org/en/reports/global/hdr1994/chapters/>; documentul raportează nevoile umane la referințe de securitate economică, alimentară, a sănătății, a mediului, siguranță personală și a comunității și securitate politică

²Raportul Secretarului General al ONU, (2005), "*In Larger Freedom: Towards Development Security and Freedom for All*", în <http://www.un.org/largerfreedom/contents.htm>

³ Human Security Centre, *Mini Atlas of Human Security*, în http://www.miniatlasofhumansecurity.info/en/files/miniAtlas_human_security.pdf

⁴Principiile de bază ale *responsabilității de a proteja*, ca recurs la acțiune în condiții specificate de risc la adresa securității umane, au fost conturate în 2001, în cadrul sesiunii Comisiei Internaționale privind Intervenția și Suveranitatea Statelor (ICISS) (Raport ICISS, *The Responsibility to Protect*, International Development Research Council, Ottawa, 2001, în <http://www.iciss.ca/report2-en.asp>). Acestea vizează prezervarea siguranței, bunăstării individuale și a demnității umane inclusiv prin eludarea autorității de stat, în condițiile în care aceasta devine ea însăși amenințare la adresa securității propriilor cetățeni. De aici rezultă că recunoașterea internațională a suveranității unui stat implică o responsabilitate subsidiară în ce privește protecția comunității statului respectiv (Galia Glume, *Responsabilité de protéger*, Centre d'études des crises et des conflits internationaux, Université catholique de Louvain, în http://operationspaix.net/Responsabilite-de-proteger?var_mode=calcul

discriminare, insecuritate, abuz sau nedreptate. Mai mult decât atât, ei trebuie să fie în măsură să participe activ și consistent la procesele democratice care le vor afecta viețile și viitorul ca indivizi sau ca persoane.

În acest context intră în discuție problematica intervenției cu scop umanitar¹, care se referă la interferența armată² a unui stat (grup de state) pe teritoriul suveran al altui stat, cu obiectivul declarat de a pune capăt sau a reduce suferințele populației acestuia, rezultate ca urmare a unui conflict armat intern, a crizei umanitare sau a crimelor la care sunt supuși de către aparatul propriului stat, obiectiv care nu poate fi asociat cu scopuri anexioniste sau atingeri aduse integrității teritoriale³ a statului țintă. Actualmente, această logică este limitată de către ONU la cazuri de genocid, purificare etnică și crime împotriva umanității⁴, situații în națiunile se declară pregătite ca – prin rezoluție a Consiliului de Securitate – să intervină militar, în caz de epuizare a mijloacelor pacifiste menite să amelioreze situația.

Un exemplu în acest sens îl constituie fundamentarea intervenției NATO în Libia, în baza unor criterii specifice dezideratelor de securitate umană. La polul opus, criza din Siria a antrenat interese politice diferite la nivelul statelor cu statut de membri permanenți ai Consiliului de Securitate al ONU, fapt ce a determinat o evoluție diferită a situației de securitate în zonă. În mod evident, domeniul intelligence este solicitat să contribuie cu produse specifice în cadrul unor astfel de operații – de unde reiese importanța conștientizării de către personalul acestor servicii a specificului a ceea ce R. Smith denumea ”războiul printre oameni” (Smith, 2005)⁵.

Recunoașterea la nivelul NATO a aspectelor socio-culturale ca sursă de intelligence este o consecință firească a evoluțiilor mediului operațional. Cu toate că nu există o doctrină a Alianței care să stabilească liniile directoare ale culegerii și prelucrării de date și informații de natură socio-culturală, mai multe inițiative în acest sens promit conturarea reperelor și principiilor care să o fundamenteze.

În primul rând, națiunile se constituie în promotori ai experienței acumulate în acest domeniu. Armate cu tradiție în câmpul operațional modern au dezvoltat doctrine și sisteme complexe de abordare a aspectelor umane în sprijinul procesului decizional.

Armata SUA are o îndelungată și probată tradiție în ceea ce denumește ”Human Terrain System” – Sistemul Terenului Uman, o abordare științificată a mediului uman din teatrul de operații, care are ca scop dezvoltarea, antrenarea și integrarea produselor de

¹Bernard Kouchner este considerat părintele intervenționismului modern, care promovează responsabilitatea democrațiilor liberale de a interveni în caz de dezastru umanitar (a se vedea Mario Bettati, Bernard Kouchner, *Le devior d'ingerence. Peut-on les laisser mourir?*, Denoel, Paris, 1987); o analiză a fațetei umanitare a intervenției militare este prezentată în Kis, 2008

²După Kofi Annan, intervenția nu trebuie înțeleasă ca un recurs exclusiv la forță, existând multe alte posibilități de asistență (Kofi A. Annan, *Two concepts of sovereignty*, în ”*The Economist*”, 18.09.1999, apud <http://www.un.org/News/press/docs/1999/9909/990918.html>).

³Așa cum s-a întâmplat în cele din urmă cu Serbia, căreia i s-au oferit garanții privind integritatea sa teritorială, ulterior nesocotite

⁴Genocidul, purificarea etnică și crimele împotriva umanității sunt în egală măsură amenințări atât din perspectiva securității umane, cât și la adresa securității și păcii internaționale.

⁵R. Smith identifică un număr de șase evoluții fundamentale ce contribuie la conturarea noii paradigme a confruntărilor militare:

- finalitatea conflictului se transferă de la îndeplinirea unor obiective strategice ce fundamentează decizia politică la stabilirea condițiilor în care o rezoluție politică poate avea loc;
- lupta se dă în cadrul comunităților și nu pe câmpul de luptă;
- conflictele tind să devină tot mai extinse în timp, chiar fără perspective de finalizare;
- implicarea în conflict se focalizează pe prezervarea forței în detrimentul asumării cerințelor critice de atingere a obiectivelor;
- mijloacele războiului industrial sunt reciclate și utilizate constant;
- părțile implicate în conflict cuprind entități non-statale.

cercetare și analiză bazate pe metodele științelor sociale în procesul decizional la nivel operațional, contribuind totodată la dezvoltarea fundamentului cunoașterii și facilitând înțelegerea din perspectivă socioculturală a mediului operațional¹.

În armata britanică, documentul doctrinar JDN 3/11 – *Luarea deciziei și rezolvarea problemelor: factorii umani și organizaționali*, analizează modalitatea în care abordările individuale, de grup sau societale influențează rezolvarea unor probleme complexe specifice mediului operațional, contribuind la înțelegerea de către factorii decizionali a implicațiilor pe care acestea le presupun, atât ca problemă cât și ca soluție.

La nivelul unor organizații ce cuprin națiuni NATO și parteneri există preocupări similare, materializate în determinarea relevanței pentru mediul operațional a analizei bazate pe metodologia Terenului Uman (ABCA²) sau dezvoltarea capacității de înțelegere a aspectelor culturale (Finabel³).

Centrul de Excelență NATO pentru Cooperare Civili-Militari (CIMIC COE), prin natura activității sale, este direct interesat de dezvoltarea și utilizarea unor modele adecvate de interacțiune cu multiplii actori ai mediului civil, în cadrul spectrului larg de activități pentru care această capacitate este responsabilă. Specialiștii din cadrul CIMIC COE au fundamentat conceptul de *Advanced Cultural Competence (Competență Culturală Avansată)*, model care servește înțelegerea și facilitează relaționarea cu partenerii civili pe baze științifice.⁴

Domeniul Intelligence – cu precădere informațiile din surse umane (HUMINT) – este direct interesat de aspectele sociale complexe ale mediului operațional, pornind de la percepțiile și atitudinile individuale până la fenomene sociale ample. Proiectul „Aspectele umane ale mediului operațional”, derulat în cadrul Centrului de Excelență NATO în domeniul HUMINT, vine să formuleze o serie de propuneri concrete în vederea îmbunătățirii modalității în care factorii de decizie militari își dezvoltă capacitatea epistemologică și abilitățile de integrare a aspectelor socio-culturale în procesul decizional și de planificare a operațiilor (HCOE, 2013).

Toate aceste inițiative se constituie în elemente de referință pentru o viitoare doctrină NATO privind aspectele socio-culturale în cadrul operațiilor militare, document ce va trebui să cuprindă o parte consistentă dedicată modului în care datele și informațiile din acest spectru parcurg întreg ciclul Intelligence.

Intelligence – delimitări conceptuale

În acest context, se impune definirea clară a termenilor de lucru, pornind de la constatarea unor evidente confuzii conceptuale în ce privește definirea parametrilor și caracteristicilor unor noțiuni ca „apărarea națională” și „securitatea națională”, dar și în ce privește accepțiunea conceptului *intelligence*.

Doctrina pentru Intelligence a Armatei SUA definește *intelligence* ca reprezentând produsul rezultat din colectarea, procesarea, integrarea, evaluarea, analiza și interpretarea informațiilor disponibile cu privire la națiuni străine, forțe sau elemente ostile sau potențial ostile, sau zone de operații actuale sau potențiale. (JP-2.0, 2013, I-1)

NATO definește *intelligence* în mod similar, ca produs rezultat din procesarea informațiilor cu privire la națiuni străine, forțe sau elemente ostile sau potențial ostile, sau

¹<http://humanterrainsystem.army.mil/>

² Reunește armate ale unor state NATO și parteneri cu tradiție în materie de cooperare militară (SUA, Marea Britanie, Canada, Australia și Noua Zeelandă) <http://www.abca-armies.org/>

³ Finabel este o organizație europeană creată pentru a promova interoperabilitatea și cooperarea între armatele naționale ale statelor membre UE, sub controlul șefilor de stat major ale acestora. România este parte a acestei organizații începând cu 2008. (http://espace-finabel.eu/public/images/stories/Finabel/Finabel_UK-midres.pdf)

⁴<http://www.cimic-coe.org/content/scope/acc.php>

zone de operații actuale sau potențiale. Definiția este extinsă și asupra activității ce are ca rezultat produsul de *intelligence* și a organizațiilor implicate în această activitate (AAP-6, 2013, 2-1-8). În cadrul activităților de dezvoltare doctrinară din NATO, propunerea făcută în forumurile responsabile ale Alianței pentru reformularea definiției (*"Intelligence ca produs rezultat din colectarea direcționată și procesarea informațiilor cu privire la mediul acțional și capabilitățile și intențiile actorilor, cu scopul de a identifica amenințări și a oferi oportunități pentru exploatarea lor de către factorii de decizie"*¹) urmărește o înțelegere corectă a *intelligence* exclusiv ca produs, rezultat al unui proces bine definit și orientat către noul mediu operațional, deschis diversității actorilor lumii globalizate.

În plan național, există dificultăți în a determina un reper conceptual comun în cadrul comunității de interes; dacă la nivelul dezbaterilor academice împrumuturile conceptuale și lexicale gen *"Intelligence"* sunt tolerabile, la nivel formal, instituțional, rezultă nevoia clarificării și standardizării tuturor elementelor de taxonomie care poziționează și definesc domeniul de referință.

Doctrina națională a informațiilor pentru securitate realizează o clasificare comprehensivă a categoriilor de informații, pe baza mai multor criterii (DNIS, 2004, Anexa 2):

- izvoarele acestora,
- stadiile proceselor la care se referă,
- stadiul prelucrării,
- sfera tematică de cuprindere,
- autenticitatea,
- veridicitatea sursei/ informației,
- modul de obținere,
- sursa/originea și/sau mijloacele de obținere,
- tehnica de înregistrare sau forma de exprimare,
- modul de reglementare,
- procedura de descriere,
- scop/utilitate,
- deciziile și acțiunile la care servesc,
- direcția și sensul de vehiculare (circuitul fluxului informațional),
- legătura dintre producătorul informației și mediu,
- preponderența elementelor componente,
- nivelurile de analiză,
- regimul juridic,
- criteriile de analiză,
- domeniile de activitate socială la care se referă (politic, economic, tehnic, științific, militar etc.) și/sau domeniile de realizare a siguranței naționale (ordine constituțională, antiterorism, siguranță economică etc.).

Totodată, *Doctrina națională a informațiilor pentru securitate* asimilează *"intelligence"* cu *informația prelucrată* și o definește ca *produs analitic rezultat din procesarea datelor (informațiilor brute)*, precizând că termenul se aplică și pentru activitatea ce generează informații prelucrate și ca titlu generic pentru cele care finalizează procese ce conduc la realizarea acestora. (DNIS, 2004, Anexa 3)

În aceeași idee, S. Petrescu arată că *"informațiile primare brute (information) reprezintă un material neevoluat, care poate proveni din surse deschise sau secrete. Numai după ce acestea sunt analizate, combinate, coroborate cu alte informații, sintetizate etc., vor*

¹Propunere adoptată în cadrul Joint Intelligence Working Group în cursul anului 2013, urmând a fi supusă acceptării de către națiuni și inclusă în viitoarea ediție a Glosarului NATO pentru termeni și definiții, AAP-6

avea însemnătate și conținut operativ în măsură să servească factorului de decizie (produse de tip *intelligence*)” (Petrescu, 2007, 32).

În dicționarele românești, *informația* este definită ca ”fiecare dintre elementele noi, în raport cu cunoștințele prealabile, cuprinse în semnificația unui simbol sau a unui grup de simboluri (text scris, mesaj vorbit, imagini plastice, indicație a unui instrument etc.)” (DELR, ediția a II-a, 1998), sau ”totalitatea materialului de informare și de documentare” (Marele dicționar de neologisme, 2000)¹.

Oxford Dictionary definește *intelligence* ca ”informație, în special cu valoare militară” (Hombly, 1999, 620), însă considerăm această explicație doar parțial satisfăcătoare ca relevanță în ceea ce privește marcarea diferenței dintre informația brută, neprelucrată (date inițiale) și informația rezultată în urma procesului denumit, în limbaj de specialitate, ”*ciclul Intelligence*” (figura 1.1). În schimb, această definiție ar servi ca argument al traducerii în limba română a termenului englezesc ”*intelligence*” ca ”*informații militare*”, în condițiile în care traducerea sa ca ”*informație*” este relativ suficientă, iar ca ”*inteligentă*”, nerelevantă și producătoare de confuzii².

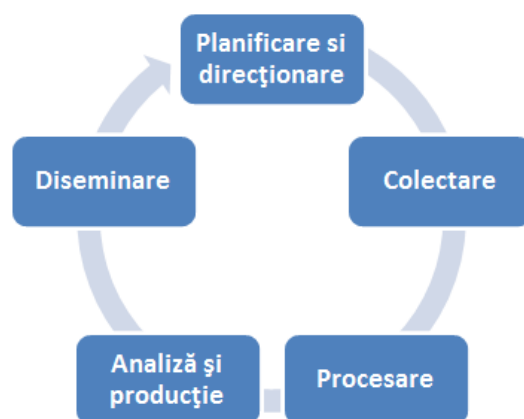


Figura 1.1: Ciclul Intelligence³

Doctrina pentru Intelligence a Armatei SUA subliniază două diferențe fundamentale între *informație* și *intelligence*, în sensul că aceasta din urmă permite anticiparea/ predicția unor situații și circumstanțe viitoare și sprijină procesul decizional prin determinarea diferențelor între cursurile de acțiune avute în vedere la nivelul factorilor de decizie. (JP-2.0, 2013, I-1)

Dincolo de valoarea anticipativă a produsului de Intelligence, un alt curent de opinie subliniază importanța acestuia ca fiind predilectă prin raportarea efectivă la obiectivul culegerii de informații/ ținta operației. În 2003, în cartea sa ”Analiza de Intelligence: o abordare centrată pe țintă”⁴ (Clark, 2003), Robert M. Clark oferea o metodologie de lucru diferită de cea clasică, raportată la ciclul Intelligence, promovând algoritmul de lucru al proceselor specifice acestui ciclu într-o formulă bazată pe relaționarea de tip rețea, în care palierele umane (operatorii implicați în culegerea de informații, analiștii și beneficiarii produselor de Intelligence conlucrează în mod integrat, permițând transferul de informație pe

¹ după <http://dexonline.ro/definitie/informa%C8%9Bie>

² Cu toate acestea, termenul nu este strict caracteristic domeniului militar, el fiind întâlnit și în domeniul afacerilor (”*business intelligence*”, ”*competitive intelligence*”) (Măzăreanu, 2006, 361) – cu rezerve față de traducerea termenului *intelligence* ca *inteligentă* în acest context

³ după <https://www.cia.gov/>

⁴ ”Intelligence Analysis: A Target-Centric Approach”

canale directe, în funcție de cerințe și limitările dictate de relevanța acestora în timp și spațiu (figura 1.2).

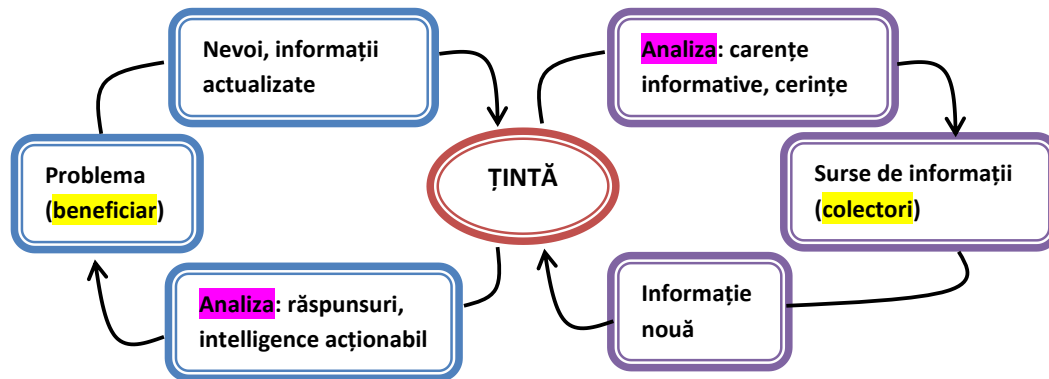


Figura 1.2: Procesul Intelligence din perspectiva orientării spre țintă (Clark, 2003)

Această abordare a fost elocvent ilustrată în 2010 de generalul maior (USA) Flynn în articolul "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan" (Flynn, Pottinger și Batchelor, 2010), la acea dată adjunctul pentru Intelligence al șefului de stat major în misiunea ISAF. Acesta făcea apel la întărirea parteneriatului între palierul analitic, beneficiarii produselor de *intelligence* și colectori, promovând fluiditatea informației între toate nivelurile de referință.

În aceeași idee, doctrina actuală pentru Intelligence a forțelor armate SUA promovează o abordare a activității de *intelligence* dintr-o perspectivă procesuală (figura 1.3), evidențiind șase categorii ale operațiilor de *intelligence*: planificarea și direcționarea, colectarea, procesarea și exploatarea, analiza și producția, diseminarea și integrarea, evaluarea și conexiunea inversă (feed-back), argumentând că – în multe situații – operațiile de intelligence evoluează aproape simultan sau unele pot fi eludate. (JP-2.0, 2013, I-5)

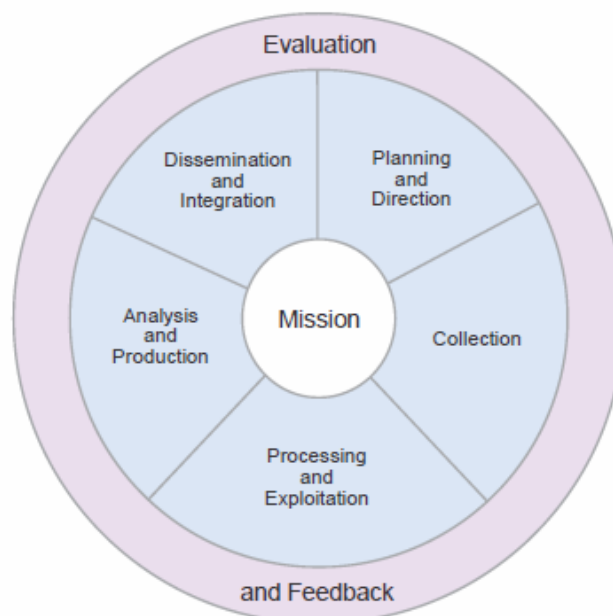


Figura 1.3: Procesul Intelligence conform Doctrinei pentru Intelligence a forțelor armate ale SUA (JP-2.0, 2013, I-6)

Doctrina britanică arată că, în condițiile în care mediul operațional complex oferă o multitudine de date și informații asupra factorilor de analiză specifici, produsul de *intelligence* reflectă ansamblul condițiilor, circumstanțelor și influențelor transpuse în estimarea predictivă a situației, precum și a capacităților și intențiilor adversarului, care afectează folosirea propriilor capacități în baza deciziei elementelor de comandă. (JP-2.0, 2013)

După I. Tulică, conceptul *intelligence* definește în sens general, ansamblul de activități ce țin de domeniul informațiilor, contrainformațiilor și protecției intereselor fundamentale ale statului ori a sistemelor de valori naționale. (Tulică, 2009, 3-4)

La nivelul Academiei Naționale de Informații (ANI), termenul *intelligence* a fost adoptat ca atare, regăsindu-se în atât în produsele activității de cercetare ale Academiei, cât și în denumirea *Institutului Național de Studii de Intelligence* din cadrul acesteia.¹ Acest împrumut lexical și conceptual este un compromis determinat de necesitatea de a opera o distincție - anume că *intelligence* nu înseamnă doar informație (în conformitate cu aspectele teoretice anterior prezentate). Cu toate acestea, termenul de "informații" se regăsește cu sensul "Intelligence" în denumirea atât a ANI, a Serviciului Român de Informații (SRI) sau a Comunității Naționale de Informații, pentru a menționa doar câteva din instituțiile/organizațiile de referință în domeniu – fapt ce alimentează lipsa de consistență și absența unui reper conceptual clar definit și adoptat în cadrul comunității de interes din România.

Alte variațiuni (traduceri/ interpretări) ale termenului Intelligence, în absența unor abordări naționale de standardizare clare, sunt reprezentate de concepte ca "**Informații pentru securitate națională**" - produs analitic, rezultat al activității specializate de căutare, identificare, obținere, prelucrare/procesare a datelor referitoare la disfuncții, vulnerabilități, factori de risc, amenințări, stări de pericol la adresa principiilor și normelor politico-sociale statornicite prin Constituție (Marinică și Ivan, 2009, 38), "**Informații pentru apărare**" - disciplina ce vizează obținerea de intelligence, în baza cerințelor specifice, prin analizarea/exploatarea datelor și informațiilor colectate prin diferite mijloace și de la diferite surse, în sprijinul procesului decizional, sau "**Informații militare**", termen regăsit în titulatura Direcției pentru Informații Militare sau al Brigăzii pentru Informații Militare.

Din cele prezentate putem observa dificultatea evidentă a găsirii unui termen echivalent în limba română, care să reflecteze cu acuratețe sensul noțiunii de *intelligence*. Cu toate acestea, ne raliem opiniei prof. Duvac, optând pentru folosirea ca atare a termenului în forma sa originală, în limba engleză (Duvac, 2007), în contextele în care se face referire la intelligence ca produs al ciclului informațional în domeniul larg al securității. Acest fapt asigură compatibilitatea de terminologie și un numitor comun în abordările comparative în cadrul comunităților de intelligence, dar nu exclude folosirea în paralel a altor noțiuni consacrate în literatura de specialitate națională, însoțite de explicațiile aferente.

Sursele de colectare a datelor și informațiilor primare sunt multiple, disciplinele de culegere (și prelucrare) a acestora grupându-se, în funcție de senzor și domeniul de colectare, în: HUMINT (Human Intelligence – intelligence derivat din informații colectate sau furnizate de către surse umane/ AAP-6), GEOINT (Geospatial Intelligence – date și informații geospațiale înregistrate prin intermediul sateliților, fotogrametriei aeriene², hărților și datelor despre teren), MASINT (Measurement and Signature Intelligence – date rezultate în urma analizei rezultatelor măsurătorilor și a semnelor electronice), OSINT (Open Source Intelligence – informații rezultate din analiza surselor deschise, publice - reviste, ziare, cărți, emisiuni TV, websiteuri, cursuri/ evenimente academice, observații și conversații personale), SIGINT (Signals Intelligence – în baza datelor culese prin interceptarea semnalelor radio și

¹<http://www.animv.ro/ro/index.php?ccs=30>

²aceste două surse acoperă denumirea de IMINT / Imagery Intelligence (informații rezultate din analiza imaginilor satelitare și a fotografiilor aeriene)

electronice), TECHINT (Technical Intelligence – informații rezultate din analiza armamentului și echipamentelor folosite de către forțele armate ale altor națiuni), FININT (Financial Intelligence – informații rezultate din analiza tranzacțiilor financiare, etc.) și altele.

Noțiunea de *Intelligence* se regăsește la nivel strategic, operațional și tactic, parcurgând algoritmi bine definiți în cadrul structurilor ierarhice politice și militare.

NATO definește *Intelligence la nivel strategic* ca *Intelligence necesar stabilirii politicilor, planificării militare și fundamentării indicatorilor și avertizărilor, la nivel național și/ sau internațional* (AAP-6). Acesta privește capacități, vulnerabilități și cursuri de acțiune probabile ale altor națiuni - în contextul globalizării, tot mai mult și a actorilor non-statali relevanți (Rolington, 2013) - în baza unor factori de analiză care acoperă domeniile economic, politic, militar, social, etc. La nivel strategic, domeniul de colectare îl reprezintă mediul de securitate global sau regional, zonele de criză și aspectele sectoriale de risc cu implicații la acest nivel.

Capabilitatea de *Intelligence operațional* este necesară planificării și conducerii campaniilor la nivel operațional (AAP-6). Managementul activității de Intelligence în cadrul structurilor/ operațiilor militare sunt responsabilități ale structurilor de comandă la toate eșaloanele; rezultatul acestei activități duce la folosirea optimă a forțelor în vederea atingerii obiectivelor.

La nivel tactic, rezultatele ciclului *Intelligence* sprijină deciziile necesare operațiilor tactice, fiind focalizate pe mediul acțional și amenințările specifice¹, pemițând comandanților să ia decizii pentru acțiuni și sarcini în cadrul misiunilor de mică amploare.

Fiecare dintre specialitățile de culegere și procesare a informațiilor pe care le-am amintit se poate regăsi, într-o măsură mai mică sau mai mare, în ipostaza de a furniza date și informații la oricare dintre nivelurile strategic, operațional sau tactic. Ponderea acestora este dictată de o multitudine de factori, amintind aici doar câțiva dintre aceștia: disponibilitatea mijloacelor tehnice adecvate, instruirea corespunzătoare, existența surselor și accesul la date și informații de interes, capacități de procesare și diseminare, etc.

Capabilitatea Intelligence în societatea informațională

Începutul secolului XXI este dedicat eforturilor de a dezvolta forme de cooperare și politici de securitate care să răspundă globalizării insecurității, conștientizând, totodată, că globalizarea nu elimină preocupările geopolitice tradiționale. Pozițiile divergente, dar și nevoia atingerii unei arii de consens, sunt puternic vizibile în cadrul forumurilor și summiturilor unde se întrunesc lideri-cheie ai planetei; aceștia sunt provocați să depășească sfera intereselor strict naționale (presiunile politice și sociale interne) și să adopte un limbaj politic global (o soluție de compromis), în care să încadreze propriile priorități. În acest sens, este evident că o capacitate adecvată de control și gestiune a securității presupune previziune, anticipare; orice politică de acțiune trebuie să se bazeze pe predicții logice, coerente, plauzibile.

Doctrina britanică evaluează o serie de factori care afectează capabilitatea intelligence în mediul operațional contemporan. O primă particularitate o reprezintă faptul că **palierele tactic, operațional și strategic sunt permeabile** în ce privește accesul la informație și relevanța acesteia. Operatorii care își desfășoară activitatea la nivel tactic pot oricând obține informații de importanță strategică. Pe de altă parte, elementele de sprijin și coordonare din afara teatrului de operații (**reach-back**) permit forțelor dislocate accesarea de expertiză și servicii suplimentare din centre sau organizații aflate la depărtare (Intelligence strategic).

¹<http://www.fas.org/irp/doddir/army/miotc/ttbaxx01.htm>

Capacitatea de a influența mediul operațional, tradusă în abilitatea de păstra inițiativa și controlul, permite atingerea **efectelor** dorite prin diferite mijloace de putere, ”soft” sau ”hard” (figura 1.4), iar produsele de intelligence fundamentează opțiunile factorilor de decizie.

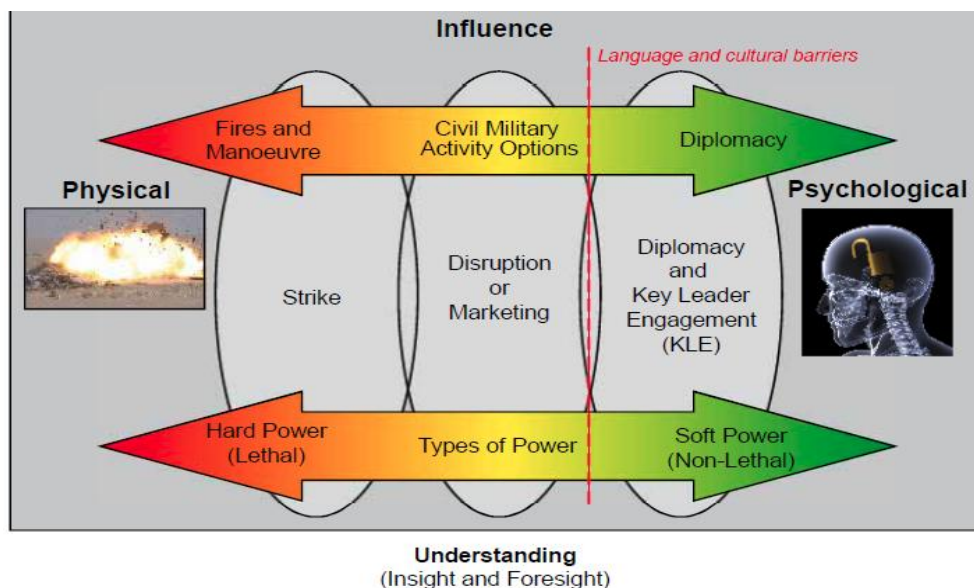


Figura 1.4 Spectrul de influență în cadrul operației, raportat la capacitatea de înțelegere - după doctrina britanică (JDP 2-00, 2011, fig. 1.4)

Comunitățile de Intelligence au cunoscut, la rândul lor, dezvoltări calitative și cantitative menite să asigure nevoia de informații pentru factorii decizionali, în toate mediile și la toate nivelurile, atât în ce privește strategiile și politicile, cât și metodele și procedurile de acțiune. Absența unei guvernante globale viabile face loc eforturilor statelor cu interese regionale și pan-regionale, care – recurgând la capabilități de resortul politic sau militar (toate tributare nevoii de informații), intră în competiție sau colaborează în vederea atingerii propriilor obiective – în acest caz, apelul la etica acțională rămânând o problemă de actualitate.

Dezvoltarea **cadrelor colaborative** (figura 1.5), pe plan național sau internațional, între serviciile și agențiile din spectrul intelligence (dar și cu o gamă variată de parteneri.), în diferite forme, a devenit critic - atât din perspectiva nevoii de acoperire a unui spectru larg de cereri de informații și multitudinea de surse disponibile, dar și din rațiuni de pragmatism funcțional, în special în contextul dictat de criza economică. Contracurarea optimă a amenințărilor actuale la adresa securității impune cooperarea în cadrul formal al unor comunități naționale de informații¹, completate cu ramificațiile și legăturile externe de cooperare și conlucrare ale acestora în vederea determinării eficiente a riscurilor și amenințărilor de securitate la nivel național, regional și internațional.

¹ Soluția revoluționară propusă de cercetătorul american W. Lahneman constă în promovarea unui nou concept al procesului de intelligence, în care între „informația secretă” și „informația deschisă” este plasată „informația de încredere” (trusted information), care circulă într-o „rețea a încrederii” (trusted network) (Lahneman, 2010). Sistemul ar fi utilizat în mod responsabil, contributorii urmând să alimenteze, după niște reguli prestabilite, numai informații validate. Printre membri pot fi agenții guvernamentale, companii private, ONG-uri, comunități de interese și chiar indivizi în mod particular. În fond, regula de bază ar fi încrederea mutuală între membri,

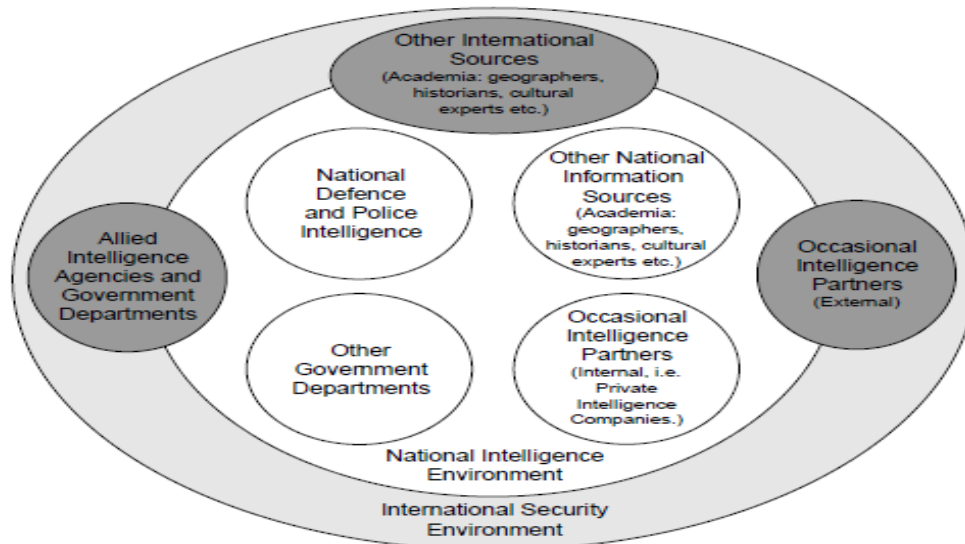


Figura 1.5 Cadrul general de relaționare în domeniul securității și al Intelligence (JDP 2-00, fig. 1.3)

Într-o abordare originală a mediului informațional într-o societate deschisă (poate chiar utopică), R. Steele vede un spectru valid al cooperării dependent de o definiție a Intelligence (și abordarea aspectelor legate de Intelligence, în general) prin prisma scopului, și nu a procesului în sine. Astfel, el pune în plan secund ”intrările” (input) în sistem: cerințele, sursele, procesarea, analiza, producția, procedurile (acțiunile sub acoperire), în antiteză cu importanța ”ieșirilor” (output): oferirea de răspunsuri la anumite probleme, evaluarea situațiilor specifice, anticiparea evoluției unor factori specifici într-un context dat, etc., identificând opt medii (”tribes”) (figura 1.6) menite să contribuie în comun la satisfacerea acestor nevoi informaționale, într-o abordare transparentă a capacității Intelligence (Steele, 2013)

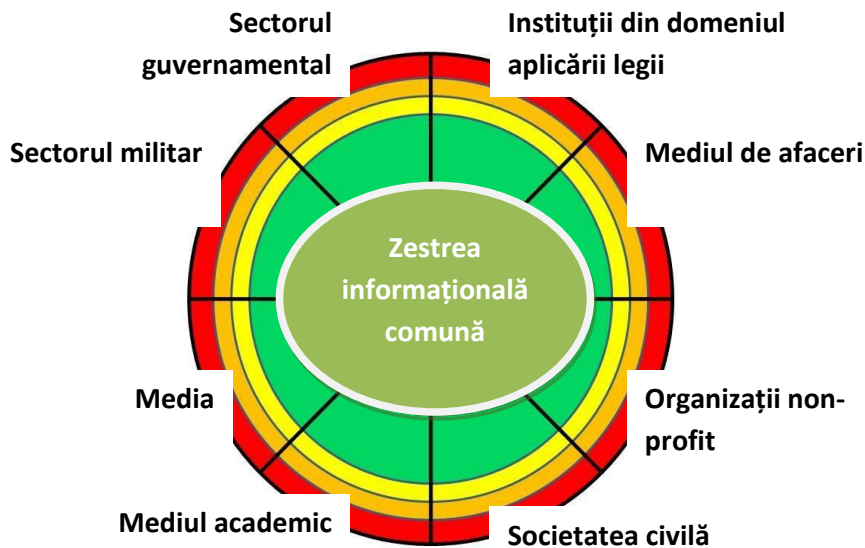


Figura 1.6 Cele opt medii ce contribuie la zestrea informațională comună (Steele, 2013)

Conceptul „Intelligence” este, în mod general, abordat din trei perspective – ca proces, organizație și produs. Procesul „Intelligence” este înțeles ca serie de activități care are ca

rezultat produsul de "Intelligence" (figura 1.7), aspectele calitative și cantitative ale acestuia fiind direct condiționate de structurile și procesele aferente.

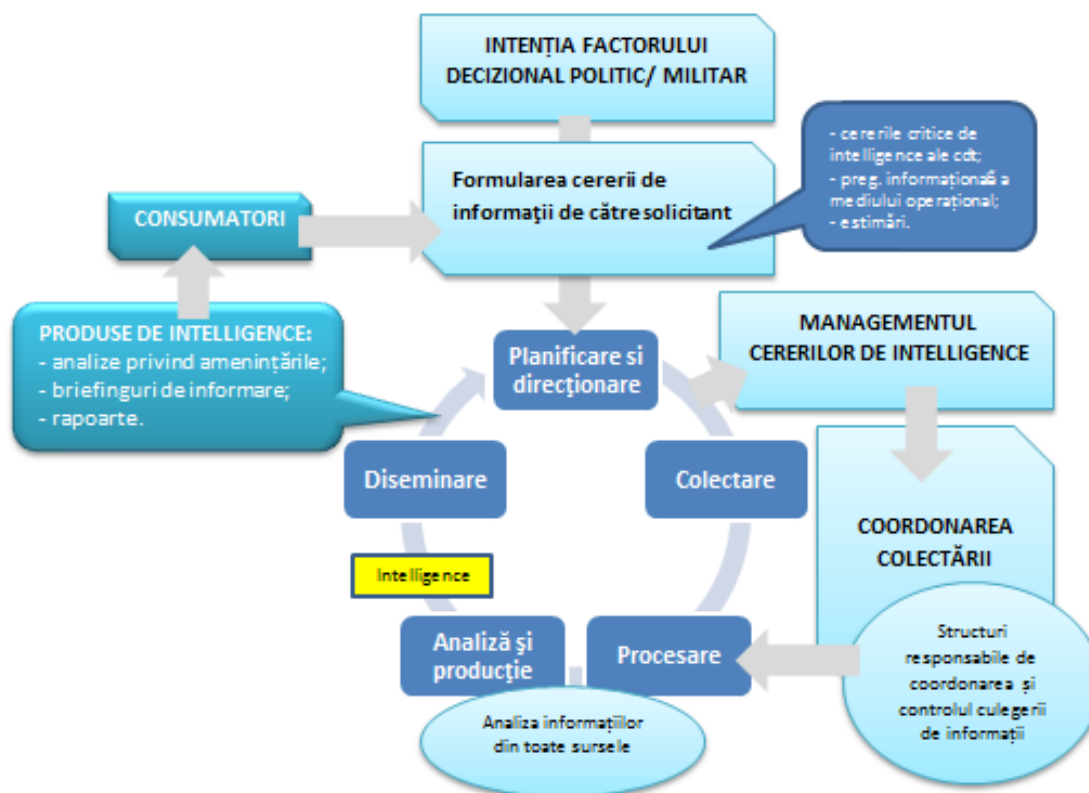


Figura 1.7 Structuri și activități în ciclul Intelligence

Mecanismele de angajare în domeniul culegerii de informații depășesc referința paradigmei clasice a securității, în virtutea căreia serviciile de intelligence, în efortul lor de a promova interesele naționale, urmăreau exclusiv penetrarea până la cel mai înalt nivel a instituțiilor străine în vederea determinării intențiilor și capabilităților acestora. În plan global s-a produs o mutație a intereselor dinspre zona geopolitică spre cea geoeconomică, abilitatea statului constând acum în gestionarea cunoașterii la nivel strategic pentru consolidarea sectorului administrației publice, al economiei, al educației, al cercetării și al bunăstării sociale. Bineînțeles, acest fapt nu exclude importanța sectorului de securitate și apărare, însă abordarea acestor aspecte suferă o mutație. Reducerea resurselor în acest sector în favoarea celor emergente se poate baza pe cooperare și punerea în comun a resurselor (a se vedea inițiativele "smart defence" în NATO sau "sharing and pooling" în UE).

Colectarea și diseminarea informațiilor, raportat la conceptul extins al securității naționale (figura 1.8), ia în considerare nivelul de percepție a amenințărilor și răspunsul politic la acestea (folosirea forței militare sau a amenințării cu forța, agresiune asimetrică, etc.) pentru impunerea voinței sau apărarea intereselor naționale. Poziționarea politică a statului în acest spectru dictează modalitatea în care serviciile specializate vor aborda aspectele legate de culegerea de date și informații, precum și politicile de diseminare a acestora.

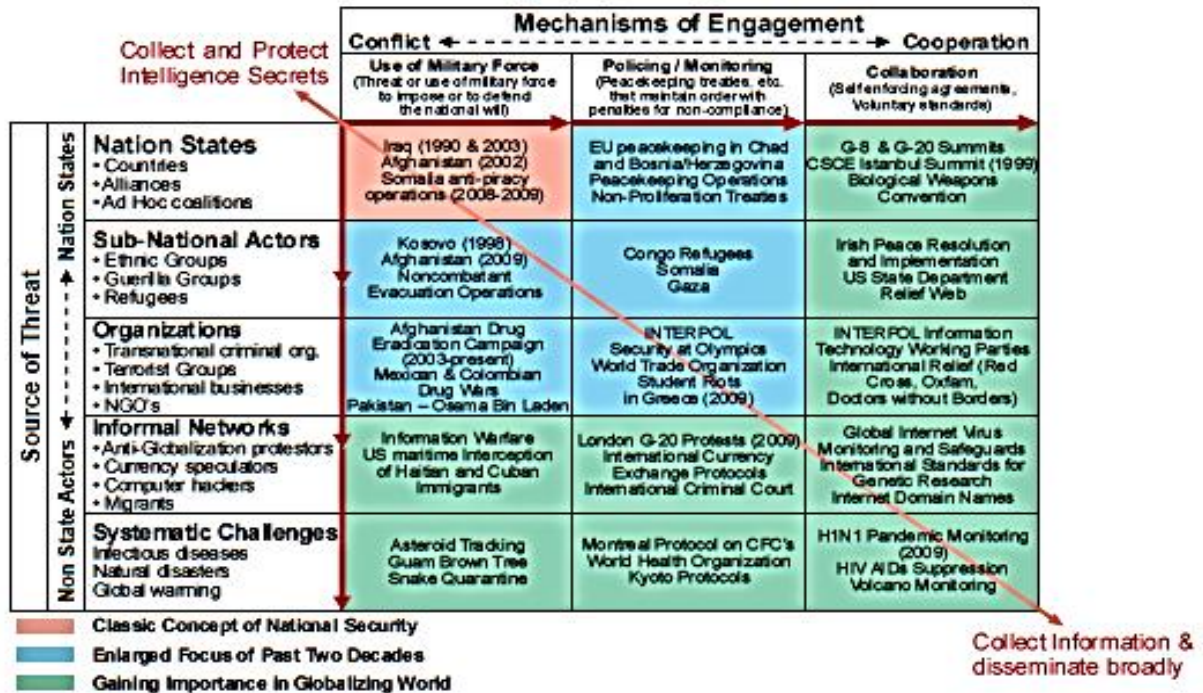


Figura 1.8 Colectarea și diseminarea informațiilor raportat la conceptul extins al securității naționale. Tipuri de amenințări și mecanisme de angajare (Pherson, 2009, 15)

În ce privește direcționarea activității de culegere de date și informații, putem evidenția o serie de elemente care influențează calitatea și utilitatea produsului final în atingerea obiectivelor propuse :

- în plan strategic, corecta identificare a riscurilor și amenințărilor de securitate, precum și conștientizarea propriilor vulnerabilități;
- la nivel operațional, identificarea, integrarea și managementul elementelor de risc determinate de intenția și capacitățile adversarului, precum și de către celelalte elemente ale mediului operațional;
- dimensiunea controlului spațial - spațiul confruntărilor (de aici și spațiul informațional de interes) este, de multe ori, un sistem teritorial necontrolat de state sau de comunitatea internațională (Raufer, 2007);
- implementarea unei strategii coerente de prevenire și gestionare a situațiilor de risc;
- intenția factorilor decizionali, completată de strategia de acțiune și finalitățile operaționale urmărite; cererile critice de intelligence ale factorilor de decizie politici sau militari trebuie să acopere toate aspectele necesare fundamentării măsurilor luate, orientate spre efectele urmărite;
- utilizarea adecvată a capacităților de culegere a informațiilor la dispoziție;
- opțiunile de cooperare și conlucrare.

Culegerea de date și informații în mediul actual, caracterizat de unii analiști ca ”societate informațională” sau ”societate bazată pe cunoaștere” este fundamentată de creșterea masivă a volumului de date și informații¹ și diseminarea acestora, facilitată de inovațiile din domeniul tehnologiei informațiilor (Vallima și Hoffman, 2008), care permite inter-conectivitatea în combinații practic nelimitate a rețelilor de cunoaștere.

¹ realitate care, în absența controlului asupra provenienței și dificultățile ridicate de discriminarea și validarea acestora, este caracterizată ca ”anarhie informațională” de către doctrina britanică

În aceste condiții, **managementul și exploatarea informației** devine decisivă în ce privește maximizarea potențialului fluxului de informații, în baza unor principii solide și eficiente ale sistemului de diseminare.

Alte probleme identificate în efortul de colectare țin atât de factorii calitativi (credibilitatea sursei și veridicitatea informației, pregătirea și experiența personalului, nivelul de actualizare a tehnologiilor, proceduri, managementul informației, etc.), cât și de cei cantitativi (acoperirea efectivă în timp și spațiu a domeniului informațional, capacități de culegere, rețele de colaborare, etc.).

În acest cadru, consolidarea culturii de securitate în rândul populației devine o necesitate. Aceasta duce la conștientizarea riscurilor și responsabilizarea actorilor societății civile, cu ecou în acțiunea civică, dar și în ce privește asigurarea cadrului interdisciplinar și pan-regional al schimbului de informații, în condițiile în care societate civilă, mediul academic, mediul de afaceri au dobândit o importanță tot mai mare în filtrarea/ analiza informațiilor și semnalarea amenințărilor emergente.

O posibilă soluție este folosirea *crowdsourcing*-ul - opțiune pe care serviciile de intelligence trebuie să o ia în calcul în construirea unui model de cooperare pentru un portofoliu determinat de problematici, în care indivizii și diferitele organizații folosesc informații obținute etic și legal pentru beneficiul comun (Albu, 2013) - abordare ce marchează trecerea de la Intelligence ca "rezolvare a puzzle-ului" (în mediu secretizat) la Intelligence ca "interpretare adaptativă" (bazat pe deschidere) (Lahneman, 2010).

O observație finală în ce privește viitorul în materie de culegere de informații îl reprezintă importanța tot mai crescută a OSINT – în special la nivel strategic – și a HUMINT, la nivel operațional-tactic.

În ce privește analiza în cadrul ciclului Intelligence, putem delimita câteva aspecte care marchează această activitate în condițiile specifice ale mediului informațional al lumii globalizate:

- refocalizarea efortului analitic dinspre amenințările de securitate la dimensiune inter-statală către cele la scară mică, diversificate, în rețea, dispersate, disimulate și dinamice;
- înțelegerea fenomenelor la scară globală și interpretarea lor la nivel regional/ local (intelligence contextual), fapt ce presupune schimbul de informații/ cunoaștere în cadrul unor rețele colaborative (intra și între comunitățile de Intelligence și sectorul privat) pe criterii geografice și de interdisciplinaritate;
- cunoașterea și înțelegerea fenomenelor securitare reclamă capacitatea culturală - abilitatea de a înțelege cultura și de a aplica aceste cunoștințe pentru angajarea eficientă în diferite medii; aprofundarea proceselor psihice și a elementelor de relaționare condiționate de cultură – prezrvând, totodată, importanța geografiei și istoriei, care fundamentează contextul în care produsele de intelligence sunt plasate, în timp și spațiu, permițând activități ca: identificarea, vizualizarea, integrarea și fuziunea elementelor oferite de cele două științe, în scopul identificării de obișnuințe, trenduri, percepții și interrelaționări;
- analiza integrată (fuziunea tuturor senzorilor disponibili/ adecvați);
- analiza de intelligence privat/ independent (în concurență cu serviciile guvernamentale). Pe măsură ce securitatea își lărgeste aria de referință, tot mai multe organizații (think-tankuri, mediul academic, societăți private cu obiect de activitate în domeniul securității, organizații ale societății civile, etc.) vin să contribuie cu expertiza proprie la conturarea unui tablou complex al mediului de securitate și, implicit, la transformarea domeniului *intelligence*.
- dreptul de proprietate asupra produsului de intelligence;
- focalizare pe anticipare și prevenirea riscurilor de securitate;

- lupta se dă în contratimp, entitățile agresoare fiind, de regulă, în avans temporal față de state (Raufer, 2007); de aici, și efortul analitic este presat de nevoia de a furniza în timp oportun produse de intelligence factorilor de decizie, în vederea asigurării unei reacții oportune;
- controlul calității informației (structurile informaționale trebuie să pună în practică proceduri de control a calității informației, în vederea evitării manipulării și dezinformării într-un mediu în care exaltarea anonimității este tot mai prezentă);
- automatizarea procesului de analiză (progresul tehnologic se va regăsi și la nivelul demersurilor analitice; dincolo de avantajul oferit de creșterea vitezei de procesare, automatizarea nu poate înlocui atributele analistului cum ar fi judecata logică, intuiția sau empatia).

Din această perspectivă, W. J. Lahneman sesizează germenii unei schimbări de paradigmă în ce privește construcția și funcționarea structurilor de Intelligence, pornind de la dificultățile de adaptare ale acestora privind gestionarea amenințărilor transnaționale, specifice lumii globalizate. După acesta, principalele tare ale sistemului actual rezidă în predilecția pentru secretizarea produselor specifice, fapt ce conduce la afectarea schimbului oportun și eficace de informații, afectând și capacitatea de a elabora produse analitice complexe, care să integreze peisajul larg al mediului de securitate actual (Lahneman, 2010).

În demersurile sale, analiza de intelligence se bazează atât pe instrumente și proceduri dezvoltate și perfecționate în timp, cât și pe calitatea personalului implicat – capacitatea epistemologică a acestuia, experiența acumulată, interesul pentru cunoaștere continuă și perfecționare, inteligența emoțională și trăsături ca imaginația sau intuiția. Abilitatea de a acoperi multitudinea de problematice care fac obiectul analizei și de a realiza conexiunile adecvate este o adevărată provocare.

Diseminarea produselor de intelligence este facilitată de suportul tehnologic existent, capabil să asigure distribuția sau accesul la acestea în baza unor politici agreeate privind managementul informației, pornind de la echilibrul adecvat dintre principiile *nevoii de a cunoaște* ("need to know") și cel al *nevoii de a împărtăși* ("need to share") informația.

Politicile de diseminare capătă o rezonanță aparte în mediile de cooperare, unde trebuie să se pună accent pe fluidizarea schimbului de informații, intra și inter-servicii. Tendințele de supra-clasificare a produselor de intelligence conduc la accesul limitat la acestea (cu posibile consecințe negative în anumite situații), pe când presiunile de diminuare a nivelului de clasificare pot să afecteze tocmai protecția elementelor din sistem.

În completarea celor două categorii de informații în mod comun acceptate – clasificate sau neclasificate – Lahneman promovează conceptul de "*trusted information*" (informație de încredere), atribuită "rețelelor de încredere" ale comunităților de interes, în care membrii pun în comun informații validate, valoarea adăugată a acestora fiind dată de pan-regionalism și interdisciplinaritate (Lahneman, 2010, 216-217).

În orice circumstanță, protecția și securitatea informațiilor rămâne o temă de actualitate. Securitatea este esențială în asigurarea protecției persoanelor, organizațiilor și surselor din mediul intelligence.

În plus, proiectarea unei relații active cu beneficiarii, în sensul transformării *feed-back*-ului într-un instrument de îmbunătățire a performanței, trebuie să se constituie într-un element suplimentar al ciclului intelligence, cu efecte la nivelul tuturor palierelor acestuia.

Comunitatea de Intelligence în România

Sub imperiul globalizării, înțelegerea profundă a tendințelor majore și a nuanțelor regionale de evoluție ale securității internaționale, precum și a oportunităților de afirmare națională în acest context, constituie o condiție esențială a progresului și prosperității.

Asociată cu înțelegerea și evaluarea corectă a proceselor interne, securitatea fiecărei țări, ca și securitatea comunității internaționale, se bazează nu numai pe capacitatea de adaptare și reacție la noile realități sau provocări ci, mai ales, pe capacitatea de anticipare (unde disciplina Intelligence joacă un rol esențial) și de acțiune pro-activă.

Strategiile naționale de securitate urmăresc integrarea într-un concept unitar și coerent a activităților de politică externă, diplomatică și de colaborare internațională cu organizarea și funcționarea instituției militare și a forțelor de ordine publică, activitatea structurilor de informații, precum și pe cea a altor agenții guvernamentale cu responsabilități în domeniu. Apartenența la NATO și la Uniunea Europeană dictează integrarea și armonizarea acestor eforturi dincolo de cadrul național, în dinamica relațiilor din spațiul comun de securitate și apărare european, precum și în spațiul euroatlantic. (SSNR, 2006, 4)

În acest sens, reformarea structurilor de intelligence în sensul optimizării activității acestora se aliază tendințelor globale, în linie cu politicile generale ale structurilor supra-naționale la care statul este parte, și se regăsește în toate aspectele definiției ale capacității, precum și în ce privește toate capacitățile angrenate în ciclul intelligence.

În România, *Doctrina națională a informațiilor pentru securitate*, având ca bază doctrinele corespunzătoare NATO, furnizează elementele cadrului conceptual al activității sistemului securității naționale¹ și oferă baza conceptuală a colaborării sistematice cu serviciile de securitate națională ale statelor membre pentru a conveni, de comun acord, asupra informațiilor, valorilor și resurselor care necesită protecție, precum și a standardelor comune de apărare (DNIS, 2004). Obiectivele DNIS sunt legate de:

- 1) perceperea și înțelegerea corectă a activității de informații – ca element al culturii de securitate;
- 2) asigurarea suportului teoretic al politicilor, strategiilor și legislației privind activitatea de informații, contrainformații și de securitate;
- 3) statuarea principiilor coordonării efortului informativ național în vederea elaborării produselor analitice și luării deciziilor privind securitatea națională;
- 4) instituirea mecanismelor de cooperare, conlucrare, colaborare între structurile de informații ale sistemului securității naționale, precum și cu cele ale aliaților, pentru cunoașterea, prevenirea și contracararea, potrivit domeniilor de competență, a amenințărilor specifice și comune;
- 5) instituirea terminologiei unitare care să asigure compatibilitatea structurilor de informații naționale cu cele ale aliaților;
- 6) perfecționarea cadrului organizațional-funcțional;
- 7) asigurarea, în domeniul securității și al activității serviciilor de informații pentru securitate, a supremației legii, protejarea statului de drept și a respectului drepturilor și libertăților fundamentale ale omului;
- 8) dezvoltarea și consolidarea participării la cooperarea internațională și la schimbul de informații privind amenințările la adresa securității naționale și a aliaților României.

Serviciile de informații și celelalte structuri care, potrivit legii, au atribuții în acest domeniu reprezintă o componentă esențială a sistemului securității naționale, fiind dezvoltate la nivelul principalelor instituții ale României: Serviciul Român de Informații (SRI), pentru informațiile din interiorul țării, Serviciul de Protecție și Pază (SPP), pentru protecția demnitarilor români și străini pe timpul prezenței lor în România, a sediilor de lucru și a reședințelor acestora², Serviciul de Informații Externe (SIE) - specializat în obținerea de

¹din sfera legislativului, executivului, sistemului național de securitate, autorităților și instituțiilor publice, organizațiilor de drept privat, celor neguvernamentale și altor forme asociative ale societății civile

²<http://www.spp.ro/>

informații din străinătate¹, Ministerul Apărării Naționale- prin Direcția Generală de Informații pentru Apărare², Ministerul Administrației și Internelor - prin Direcția Generală pentru Informații și Protecție Internă (DGPII)³, Ministerul Justiției și Serviciul de Telecomunicații Speciale (STS)⁴.

Conform Strategiei de Securitate Națională a României, activitatea lor are ca scop principal avertizarea oportună a autorităților competente cu privire la riscurile și amenințările care creează sau pot genera pericole la adresa valorilor și intereselor fundamentale ale României, prevenirea acestora, precum și protecția adecvată împotriva unor astfel de pericole. Informațiile asigură evitarea surprinderii strategice, fundamentarea corectă a deciziilor și viteza adecvată de reacție, precum și capacitatea de acțiune pro-activă, în scopul îndeplinirii noilor tipuri de misiuni.

Atribuțiile de planificarea strategică, coordonare și control a acestor autorități sunt exercitate de către Președintele României, Parlament, Consiliul Suprem de Apărare a Țării (CSAT) și Guvern. Politica de securitate este un element de o deosebită importanță la nivelul statelor, guvernele fiind structurile direct implicate în coordonarea agențiilor responsabile. Parlamentul, prin sarcinile de examinare și monitorizare a activității aparatului executiv, asigură și controlul în domeniul securității, în baza cadrului legislativ existent. În ciuda limitărilor inerente presupuse de nivelul de confidențialitate și complexitatea acestui sector, acest tip de control democratic este decisiv pentru prevenirea regimurilor autocratice, monitorizarea modului de folosire a resurselor bugetare, crearea cadrului legal pentru chestiuni de securitate și asigurarea unei punți de legătură cu publicul. (Fluri, Johnsson și Born, 2003)

În plan funcțional, activitatea autorităților din domeniul securității și al informațiilor este planificată la nivel strategic de către Comunitatea Națională de Informații, care funcționează sub coordonarea CSAT și care reprezintă „rețeaua funcțională a autorităților informative din sistemul securității naționale” (Duțu și Bogzeanu, 2010, 59), un parteneriat instituționalizat a serviciilor de informații, contrainformații și securitate, care își păstrează atribuțiile și misiunile specifice, concomitent cu o mai bună coordonare a activității la nivelul strategic.

Prin aceasta, se asigură posibilitatea realizării de programe naționale comune pentru creșterea eficienței activității de culegere, procesare și utilizare în comun a informațiilor (îmbunătățirea tuturor etapelor ciclului Intelligence), conform exigențelor statului democratic de drept și cerințelor de securitate actuale.

Concluzii

Globalizarea fundamentează parametrii funcționali ai societății umane, devenind o referință indispensabilă pentru orice demers analitic al lumii contemporane sau prospect al

¹ SIE este instituția de stat specializată în domeniul informațiilor externe privind siguranța națională, apărarea României și a intereselor sale (<http://www.sie.ro/index.html>)

² structura specializată responsabilă pentru colectarea, procesarea și verificarea informațiilor privind factorii de risc interni și externi, militari și nonmilitari, coordonarea măsurilor contrainformative și cooperarea cu serviciile/structurile departamentale naționale de informații, cât și cu cele ale statelor membre ale alianțelor, coalițiilor și organizațiilor internaționale la care România este parte și asigură securitatea informațiilor clasificate naționale, NATO și UE la nivelul Ministerului Apărării Naționale (Duțu și Bogzeanu, 2010, 58-59)

³ structura specializată a Ministerului Afacerilor Interne care desfășoară activități de informații și protecție internă, în vederea asigurării ordinii publice, prevenirii și combaterii amenințărilor la adresa siguranței naționale privind misiunile, personalul și informațiile clasificate în cadrul ministerului (<http://www.dgipi.ro/>)

⁴ organul central de specialitate, cu personalitate juridică, ce organizează și coordonează activitățile în domeniul telecomunicațiilor speciale pentru autoritățile publice din România și alți utilizatori prevăzuți de lege (<http://www.stsnet.ro/>)

viitorului. Influența pe care procesele asociate globalizării o au asupra capacității Intelligence sunt multiple și, după cum am arătat în cadrul cursului, se regăsesc în toate etapele ciclului Intelligence – planificare și direcționare, colectare, procesare, analiză și producție, diseminare.

Caracteristicile mediului de securitate actual, amenințările asimetrice și cele hibride reclamă un răspuns pe măsură. Capacitățile de reacție trebuie să prevadă întreg spectrul de funcțiuni menite să contracareze orice posibilă amenințare; în acest sens, pregătirea forțelor trebuie diferențiată și diversificată, pentru măsuri clasice și neconvenționale, prin care să se realizeze obiectivele referitoare la misiunile antiteroriste, contra proliferării armelor de nimicire în masă, contra insurgenței, etc.

În sprijinul factorilor decidenți și a forțelor de răspuns, comunitățile de informații caută să se adapteze din punct de vedere funcțional și operațional la realitățile societății informaționale. În acest sens, dezvoltarea coordonării între serviciile și agențiile din domeniul intelligence dă naștere unor comunități de interes naționale și supra-naționale, a căror colaborare cu o rețea extensivă de actori ai societății civile ne oferă imaginea de ansamblu a eforturilor făcute în sensul asigurării securității. În cadrul colaborativ dezvoltat, comunitățile de interes în domeniul intelligence trebuie să depășească palierul strict al cunoașterii (prin schimbul de informații), concentrându-se inclusiv asupra transmiterii operative a informațiilor culese către decidenți (Duțu, 2013, 55), astfel încât să permită luarea măsurilor corespunzătoare, în timp oportun.

Mai mult, strategiile de securitate moderne privesc serviciile specializate ca parte a unui efort național care implică nu doar instituțiile guvernamentale și civile, ci merg până la responsabilizarea individuală a cetățeanului și la promovarea unei culturi de securitate¹ care să răspundă cerințelor actuale de cunoaștere.

Bibliografie

1. AARONSON, Michael, DIESEN, Sverre, KERMABON, Yves de, LONG, Mary Beth, and MIKLAUCIC, Michael (2011) *NATO Countering the Hybrid Threat*, în PRISM, Vol. 2, no. 4, 09/2011, The Center for Complex Operations, National Defense University Press, Washington
2. ALBU, Alina (2013) *Crowdsourcing în activitatea de Intelligence*, în volumul Sesiunii de Comunicări Științifice cu participare națională *Tehnologiile mileniului al III – lea și viitorul activității de informații* Ediția a III—a, 27 Noiembrie, București
3. ANNAN, Kofi A. (1999) *Two concepts of sovereignty*, în "The Economist", apud <http://www.un.org/News/Press/docs/2000/00012000012001.asp?OpenID=12001>
4. BĂDESCU, Ilie (2013) *Semnele vremurilor și geopolitica "turbulențelor"*, în revista Infosfera, anul V, nr. 3, pp. 39-51, București
5. BETTATI, Mario, KOUCHNER, Bernard (1987) *Le devior d'ingérance. Peut-on les laisser mourir?*, Denoel, Paris
6. BUZAN, Barry (2000) *Popoarele, statele și teama. O agendă pentru studii de securitate internațională în epoca de după Războiul Rece*, Ed. Cartier, Chișinău
7. CLARK, Robert M. (2003), *Intelligence Analysis: A Target-Centric Approach*, CQ Press
8. DINU, Mihai-Ștefan (2005) *Componenta etnico-religioasă a conflictelor*, Editura Universității Naționale de Apărare „Carol I”, București
9. DUȚU, Petre (2013) *Amenințări asimetrice sau amenințări hibride: delimitări conceptuale pentru fundamentarea securității și apărării naționale*, Editura Universității Naționale de Apărare „Carol I” București, http://cssas.unap.ro/ro/pdf_studii/amenintari_asimetrice_sau_amenintari_hibride.pdf
10. DUȚU, Petre, BOGZEANU, Cristina (2010) *Interesele naționale și folosirea instrumentelor de putere națională pentru promovarea și apărarea acestora. Cazul României*, Editura Universității Naționale de Apărare „Carol I”, București
11. DUVAC, Ion (2007) *Suport de curs Intelligence – aplicații*, Facultatea de Sociologie și Asistență Socială, Universitatea din București, București

¹ o abordare proactivă a acestui aspect impune colaborarea reprezentanților comunității de intelligențe cu membrii societății civile și academice, în cadrul unor evenimente academice cu deschidere către publicul larg

12. FLYNN, Michael T., POTTINGER, Matt, BATCHELOR, Paul D. (2010) *Fixing Intel – A blueprint for Making Intelligence Relevant in Afghanistan*, Kabul
13. FLURI, Philipp, JOHNSON, Anders B. (redactori-șefi), BORN, Hans (redactor și autor principal) (2003) *Controlul parlamentar al sectorului de securitate. Principii, mecanisme și practici*, publicat de Uniunea Interparlamentară, Centrul pentru Controlul Democratic al Forțelor Armate, traducere certificată de Centrul de Studii Regionale, Editura ZIUA, București
14. FROST, Ellen L. (2002) *Globalization and National Security: A Strategic Agenda*, in Richard L. Kugler, Ellen L. Frost (editori), *The Global Century. Globalization and National Security*, vol. 1, Institute for National Strategic Studies, National Defense University, University Press of the Pacific, Honolulu, Hawaii
15. GLUME, Galia, *Responsabilité de protéger*, Centre d'études des crises et des conflits internationaux, Université catholique de Louvain, în http://operationspaix.net/Responsabilite-de-proteger?var_mode=calcul
16. HOMBY, A.S., (1999), *Oxford Advanced Learner's Dictionary of Current English*, Fifth Edition, Oxford University Press
17. KIS, Alexandru (2008) *The Afghanistan War as Humanitarian Intervention – a view over the implications of Military through the process of ensuring Human Security in Zabul Province*, The 14th KBO International Conference, "Nicolae Bălcescu" Land Forces Academy Publishing House, Sibiu
18. KIS, Alexandru (2012) *NATO și securitatea umană*, Editura Universității din Oradea
19. LAHNEMAN, William J. (2010) *The Need for a New Intelligence Paradigm*, International Journal of Intelligence and CounterIntelligence, 23:2, 201-225
20. MARINICĂ, Mariana, IVAN, Ion (2009) *De ce Intelligence?*, în Revista Română de Studii de Intelligence, Nr. 1-2
21. MĂZĂREANU, Valentin (2005) "Inteligență" în business intelligence, Analele Științifice ale Universității „Alexandru Ioan Cuza” din Iași, Tomul LII/LIII Științe Economice 2005/2006, în [http://anale.feaa.uaic.ro/anale/resurse/54_Mazareanu_V_-_"Inteligenta"_in_Business_Intelligence.pdf](http://anale.feaa.uaic.ro/anale/resurse/54_Mazareanu_V_-_)
22. NYE, Joseph S. Jr. (1990) *Bound To Lead: The Changing Nature of American Power*, Publisher: Basic Books
23. OPREA, Gabriel-Marian (2013) *Noi tipuri de manifestare a crizelor politico-militare contemporane*, în revista Infosfera, anul V, nr. 3, pp. 52-58, București
24. PETRESCU, Stan (2007) *Despre Intelligence. Spionaj-contraspionaj*, Editura Militară, București
25. PHERSON, Randolph H. (2009) *Rethinking National Security in a Globalizing World: A New Ecology*, în Revista Română de Studii de Intelligence, Nr. 1-2
26. RAUFER, Xavier (2007) *Menaces terroristes, criminelles, hybrides, la perspective large*, Conférence prononcée dans le cadre du colloque organisé par l'Université de Sherbrooke, "Le terrorisme : une perspective canadienne". Longueuil, les 29-30 mai 2007, http://classiques.uqac.ca/contemporains/raufer_xavier/menaces_terroristes/menaces_terroristes_texte.html#Anchor-Xavier-49575
27. SEBE, Marius (2009) *Despre intelligence (I)*, în Revista Română de Studii de Intelligence, Nr. 1-2
28. SHARP, Gene (2012) *From Dictatorship to Democracy*, Serpent's Tail, London
29. SMITH, Rupert (2006) *The utility of Force. The Art of War in the Modern World*, Penguin Books, London
30. STEELE, Robert David (2013) *2013 Intelligence Future – The Third Era of Local to Global Intelligence Overview & Workshop 2.8 Adds 2 Memos to CINCEUR & CINCSOC*, în <http://www.phibetaiota.net/2013/04/2013-robert-steele-keynote-workshop/>
31. TULICĂ, Ioan (2009) *Note de curs: Intelligence și securitate*, Iași
32. VALLIMA, J., HOFFMAN, D. (2008) *Knowledge society discourse and higher education*, în *Higher Education*, 56(3), 265-285.

33. ***, Department of Social and Cultural Anthropology, *Constructing Human Security in a Globalizing World* (2007) în <http://www.fsw.vu.nl/en/research/research-programmes/social-and-cultural-anthropology/index.asp>
34. ***, *Doctrina națională a informațiilor pentru securitate* (2004) Editura S.R.I., București, în <http://www.sri.ro/doctrina-nationala-a-informatiilor-pentru-securitate.html>
35. Bi-Strategic Command (2011) *Knowledge Development - Pre-Doctrinal Handbook*, http://www.cicde.defense.gouv.fr/IMG/pdf/20110209_np_otan_bi-sc-knowledge-development.pdf
36. Dicționar online termeni militari SUA - http://www.dtic.mil/doctrine/dod_dictionary/index.html?zoom_query=intelligence&zoom_sort=0&zoom_per_page=10&zoom_and=1
37. Dicționarul Explicativ al Limbii Române (DELR), ediția a II-a, 1998
38. Human Security Centre, *Mini Atlas of Human Security*, în http://www.miniatlasofhumansecurity.info/en/files/miniAtlas_human_security.pdf
39. Joint Publication 2-0 Joint Intelligence, 22 October 2013, http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf
40. Marele dicționar de neologisme (2000) <http://dexonline.ro/definitie/informa%C8%9Bie>
41. NATO Bi-SC, IMSM-0292-2010, *Hybrid threats description and context*

42. NATO HUMINT Centre of Excellence (HCOE) (2013), *Human aspects of the operational environment - Final Report*, Project developed under the framework of NATO's Defence against Terrorism Programme of Work with the support of Emerging Security Challenges Division/ NATO HQ, CNI Coresi SA, Oradea
43. NATO Standardization Agency (2013) *AAP-6, NATO Glossary of terms and definitions (English and French)*
44. Președinția României (2006) *Strategia de securitate națională a României*, București, <http://www.presidency.ro/static/ordine/SSNR/SSNR.pdf>
45. Raport ICISS (2001) *The Responsibility to Protect*, International Development Research Council, Ottawa, în <http://www.iciss.ca/report2-en.asp>.
46. Raportul Secretarului General al ONU (2005) "*In Larger Freedom: Towards Development Security and Freedom for All*", în <http://www.un.org/largerfreedom/contents.htm>
47. The American Heritage Dictionary of the English Language
48. The Development, Concepts and Doctrine Centre, UK Ministry of Defence, Joint Doctrine Publication 2-00 (JDP 2-00) *Understanding and Intelligence support to Joint Operations* (3rd Edition) (2011) Shrivenham Swindon, Wiltshire, UK
49. The Development, Concepts and Doctrine Centre, UK Ministry of Defence, Joint Doctrine Note 3/11 (JDN 3/11) *Decision-Making and Problem Solving: Human and Organisational Factors* (2011) Shrivenham Swindon, Wiltshire, UK
50. The Development, Concepts and Doctrine Centre, UK Ministry of Defence, Joint Doctrine Publication 04 (JDP 04) (2010) *Understanding*, Shrivenham Swindon, Wiltshire, UK
51. UNDP (1994) *Human Development Report 1994*, în http://hdr.undp.org/en/media/hdr_1994_en_chap2.pdf

52. <http://dexonline.ro/definitie/informa%C8%9Bie>
53. http://espace-finabel.eu/public/images/stories/Finabel/Finabel_UK-midres.pdf
54. <http://hdr.undp.org/en/reports/global/hdr1994/chapters/>
55. <http://humanterrainsystem.army.mil/>
56. <http://www.abca-armies.org/>
57. <http://www.animv.ro/ro/index.php?ccs=30>
58. <http://www.cimic-coe.org/content/scope/acc.php>
59. <http://www.dgipi.ro/>
60. <http://www.fas.org/irp/doddir/army/miotc/ttbaxx01.htm>
61. <http://www.sie.ro/index.html>
62. <http://www.spp.ro/>
63. <http://www.stsnet.ro/>
64. <https://www.cia.gov/>

CAPITOLUL 2 CAPABILITATEA INTELLIGENCE ÎN NATO

Transformarea Alianței Nord-Atlantice și mediul Intelligence

Viziunea de ansamblu asupra adaptării NATO la mediul de securitate actual și la provocările viitoare sunt exprimate în Conceptul Strategic și politicile menite să guverneze modalitatea efectivă de realizare a obiectivelor Alianței. Evaluările și estimările care stau la baza fundamentelor conceptuale ale procesului de transformare în NATO, dincolo de voința politică a națiunilor, decurg din experiența acumulată, lecțiile învățate, abordarea analitică a amenințărilor și riscurilor la adresa securității, toate acestea contribuind la modelarea a diferite cursuri de acțiune cărora Alianța trebuie să le facă față.

Un exemplu elocvent îl constituie Proiectul Scenariilor Multiple ale Viitorului (Multiple Futures Project – MFP, figura 2.1), inițiativă concepută să permită modelarea unor medii plauzibile ale viitorului cu care Alianța se va confrunta, cu un orizont de acțiune până în 2030, în scopul identificării amenințărilor relevante și implicațiilor militare și de securitate ale acestora. În contextul evoluției lumii globalizate, experții participanți la proiect au identificat un set complex de provocări, determinate de o largă paletă de factori cauzali:

- Puterea (multidimensională) a altor entități (statale sau non-statale);
- Fragilitatea altor entități (incluzând instabilitatea cauzată de statele eșuate);
- Natura (dezastre naturale, resurse energetice, asigurarea apei și hranei, etc.);
- Schimbări societale sistemice (care antrenează transformarea organizațiilor militare în cadrul societăților aflate în schimbare);
- Mediul operațional complex.

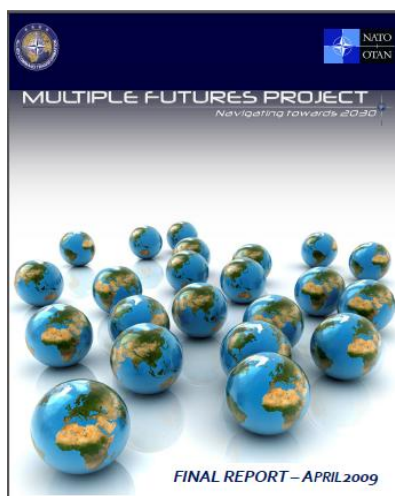


Figura 2.1 Raportul final al MFP

Studierea algoritmilor MFP privind evoluția stării de securitate a viitorului, sugestiv denumiți: ”Latura întunecată a exclusivității” (statele slabe și eșuate generează instabilitate în ariile de interes, iar statele lumii globalizate se confruntă cu opțiunile strategice ce decurg din această realitate), ”Stabilitatea înșelătoare” (statele dezvoltate preocupate de schimbările societale și problemele demografice în detrimentul riscurilor geopolitice), ”Contradicțiile modernității”(societățile avansate, raționale, bazate pe rețele, cu fragilități inerente, sunt supuse provocărilor unor regimuri externe autoritariste) și ”Politicile noilor puteri” (un număr crescând de puteri majore, competiția și proliferarea subminează valoarea organizațiilor internaționale) (MFP-Final Report, 2009, 5-6), sunt de interes deosebit pentru comunitățile de Intelligence. Abordarea particularizată a acestor modele, coroborată cu interesele naționale și

obiectivele pragmatice de dezvoltare ale statelor, reprezintă un element de reper în activitatea de analiză și estimare.

La nivelul NATO, MFP prefigurează cadrul și premisele a patru direcții fundamentale ale transformării Alianței, sintetizate în:

- reasigurarea determinării de a acționa împotriva unui atac armat, în conformitate cu prevederile art. 5;
- flexibilizarea în ce privește tipurile de atac ce se încadrează în categoria non-art. 5 – provocări netradiționale sau dezastre umanitare ce reclamă contribuția cu forțe militare;

- responsabilitatea împărțită a tuturor membrilor în ce privește contribuția la gestionarea crizelor în condițiile în care Consiliul Nord-Atlantic agreează o astfel de misiune;
- reafirmarea angajamentelor cu partenerii și alte națiuni din afara teritoriului Alianței în vederea asigurării premiselor diplomației defensive, a cooperării militare, construcției și întăririi capacităților de parteneriat. (Binnendijk și Hoon,2010,1)

Conceptul Strategic NATO din 2010 preia și prefigurează prioritățile strategice pentru următoarea decadă, furnizând cerințele și asigurând cadrul de dezvoltare a capacităților – actualizat prin deciziile luate la summitul NATO de la Chicago (în mai 2012) și puse în operă în cadrul procesului de planificare a apărării, la nivelul disciplinelor aferente, în vederea îndeplinirii angajamentele asumate pentru apărarea colectivă, gestionarea situațiilor de criză și asigurarea securității prin cooperare.

Recent, în al 30-lea Atelier de Lucru Internațional privind Securitatea Globală (Paris, 24 iunie 2013), locțiitorul Secretarului General al NATO, dl. ambasador Alexander Vershbow, făcea o radiografie a provocărilor pe care NATO și comunitatea transatlantică le are de înfruntat în perioada post 2014, punct de inflexiune al transformării Alianței (determinat de nevoia de re-focalizare post-ISAF, cu accent pe operaționalizarea forțelor și interoperabilitate)¹.

Nimeni nu anticipa la acea dată evoluțiile dramatice ale situației de securitate în estul Europei, având Rusia în prim planul afirmării intereselor sale strategice în detrimentul integrității teritoriale a Ucrainei și prin conturarea unui profil agresiv la adresa Alianței Nord-Atlantice. Demonstrația de forță a Rusiei a luat prin surprindere NATO, fapt evidențiat ca deficiență majoră în special în ce privește capacitățile de avertizare timpurie și, implicit, întreg spectrul ISR – Intelligence, Supraveghere, Recunoașteri al Alianței.

Contextul crizei economice, ce profila ca provocare majoră ajustarea contribuției țărilor europene în cadrul NATO în balanță cu SUA, în condițiile în care capacitățile actuale ale Alianței trebuie menținute și dezvoltate² - concurent logicii inițiativei Smart Defence³, regăsită în diferite proiecte și programe de dezvoltare a capacităților (armonizate cu inițiativele Agenției Europene de Apărare), dar și în aranjamente de cooperare regionale în domeniul securității (Tratatul Franco-Britanic de la Lancaster, grupul Vișegrad, grupul Weimar, grupul Nordic de Cooperare în domeniul Apărării/ NORDEFECO, etc.) – suferă reconsiderări majore, dictate de noile realități geopolitice din flancul estic al Alianței.

Summitul NATO din Wales, 4-5 septembrie 2014, dincolo de reafirmarea sarcinilor cheie prevăzute în Conceptul Strategic, ia act de criza declanșată de agresiunea Rusiei împotriva Ucrainei și prevede instituirea unui plan de acțiune în măsură să determine o mai bună capacitate de pregătire și răspuns a Alianței în situații de natură să amenințe securitatea statelor membre. Declarația Summitului⁴ prevede inclusiv îmbunătățirea capacităților de

¹ http://www.nato.int/cps/en/natolive/opinions_101606.htm

² în special pentru capacități ce necesită costuri ridicate de mentenanță și operare – drone, avioane de alimentare în zbor, avioane pentru transport strategic, mijloace de război electronic, etc.

³ Inițiativa Forțelor Conectate (Connected Forces Initiative - CFI) completează programul Smart Defence prin oportunitățile de instruire în baza standardelor NATO, ambele contribuind la obiectivul "Forțele NATO 2020" stabilit la Summitul de la Chicago (http://www.nato.int/cps/en/natolive/official_texts_87594.htm). Cadrul de dezvoltare al CFI presupune educație și instruire intensificată, un număr crescut de exerciții și îmbunătățirea performanțelor în folosirea tehnologiei (http://www.nato.int/cps/en/natolive/topics_98527.htm); în acest cadru, capacitatea Intelligence trebuie să fie proactiv promovată, atât din perspectiva spectrului întrunit al Intelligence, Supravegherii și Recunoașterilor (Joint Intelligence, Surveillance and Reconnaissance – JISR), cât și la nivelul disciplinelor de culegere a datelor/ informațiilor.

⁴ <https://www.gov.uk/government/publications/nato-summit-2014-wales-summit-declaration/the-wales-declaration-on-the-transatlantic-bond>

Intelligence și avertizare strategică, urmând ca acestea să fie modernizate și dezvoltate atât la nivelul structurilor de comandă și control de nivel strategic și operațional, cât și în cadrul noilor structuri de forță (Very High Readiness Joint Task Force - VJTF) ce vor fi dislocate în flancul estic al Alianței, ca parte a Forței de Răspuns NATO. Aceste capacități vor fi concepute să răspundă atât provocărilor ridicate de conflicte clasice, cât și celor specifice războiului hibrid; pe lângă acestea, amenințări ca proliferarea rachetelor balistice sau cele din domeniul cibernetic, combaterea terorismului și a pirateriei etc. reclamă, la rândul lor, capacități adecvate de răspuns.

În vederea adresării adecvate a acestor obiective, unul dintre scopurile transformării este reprezentat de obținerea superiorității, tradusă în obiective reprezentate de superioritatea informațională și capacitățile pe bază de rețea¹. Într-o primă fază, efortul de implementare a mijloacelor ISR aferente noului concept NATO JISR se va concentra asupra capacității operaționale a operațiilor curente ale NATO, precum și a Forței de Răspuns NATO – începând cu rotația 2016.

Atingerea acestor deziderate se realizează prin efortul coordonat al structurilor responsabile și al rețelelor lucrative pe care statele aliate le-au realizat în timp, în cadrul acțiunilor presupuse de dezvoltarea și experimentarea conceptelor, actualizarea doctrinelor și procedurilor, derularea unor proiecte de cercetare științifică și tehnologică, planificarea apărării, educarea și instruirea personalului – ca domenii funcționale ale transformării.

Nivelul conceptual al transformării – inclusiv pentru domeniul Intelligence – este exploatat și își găsește aplicabilitatea practică în spectrul definit de acronimul DOTMLFPI (*Doctrine, Organisation, Training, Material, Leadership, Personnel, Facilities, Interoperability*/ Doctrină, Organizare, Instruire, Materiale, Conducere, Personal, Infrastructură, Interoperabilitate).

Ca urmare a profilării Rusiei ca amenințare la adresa securității în estul Europei, structura de comandă a NATO, recent reformată (figura 2.2), va fi dezvoltată prin adăugarea unor noi structuri de comandă și control de nivel operativ-tactic, pre-poziționate în statele din flancul estic al Alianței (între care și România²).

Eforturile de transformare se reflectă, în mod concret, la nivelul statelor NATO, implicând nemijlocit structurile de decizie politică și militară. Acestea sunt cele care trebuie să realizeze/ asigure capacitățile specificate în obiectivele forței la nivelul structurilor cu care contribuie în cadrul Alianței.

Dincolo de exprimarea voinței politice și asigurarea resurselor bugetare, de aici decurg responsabilități privind asigurarea interoperabilității, dislocabilității, achizițiilor de echipamente, modernizarea procesului de educare și instruire, adecvarea sistemului legislativ și reglementărilor specifice, dezvoltarea și participarea la forme instituționalizate ale sprijinului acordat procesului de dezvoltare în NATO, asumarea de responsabilități și participarea în diferite forme de cooperare.

¹ Abilitatea cognitivă și tehnică a Alianței de a conjuga diferite componente ale mediului operațional prin intermediul rețelelor informatice și a infrastructurii de informații (concretizată în Capabilitatea bazată pe rețea a NATO - NNEC) ilustrează crezul cooperării („a împărți [*informație* – n.a.] pentru a învinge”) ca trăsătură de cultură organizațională, conducând către o mai bună avertizare situațională și sprijinind procesele decizionale ce duc, în ultimă instanță, la interoperabilitate și eficiență acțională, optimizarea consumului de resurse, salvarea de vieți omenești, etc. Urmărind asigurarea coerenței și integrării eficiente a sistemelor deja existente, NNEC urmărește obiective specifice la nivel de personal/ operatori, arhitectura proceselor și tehnologia de suport, cu implicații la nivelurile strategic, operativ și tactic. (http://www.nato.int/cps/en/natolive/topics_54644.htm)

² <http://www.hotnews.ro/stiri-esential-18042680-live-text-traian-basescu-face-declaratii-doua-summit-ului-nato.htm>

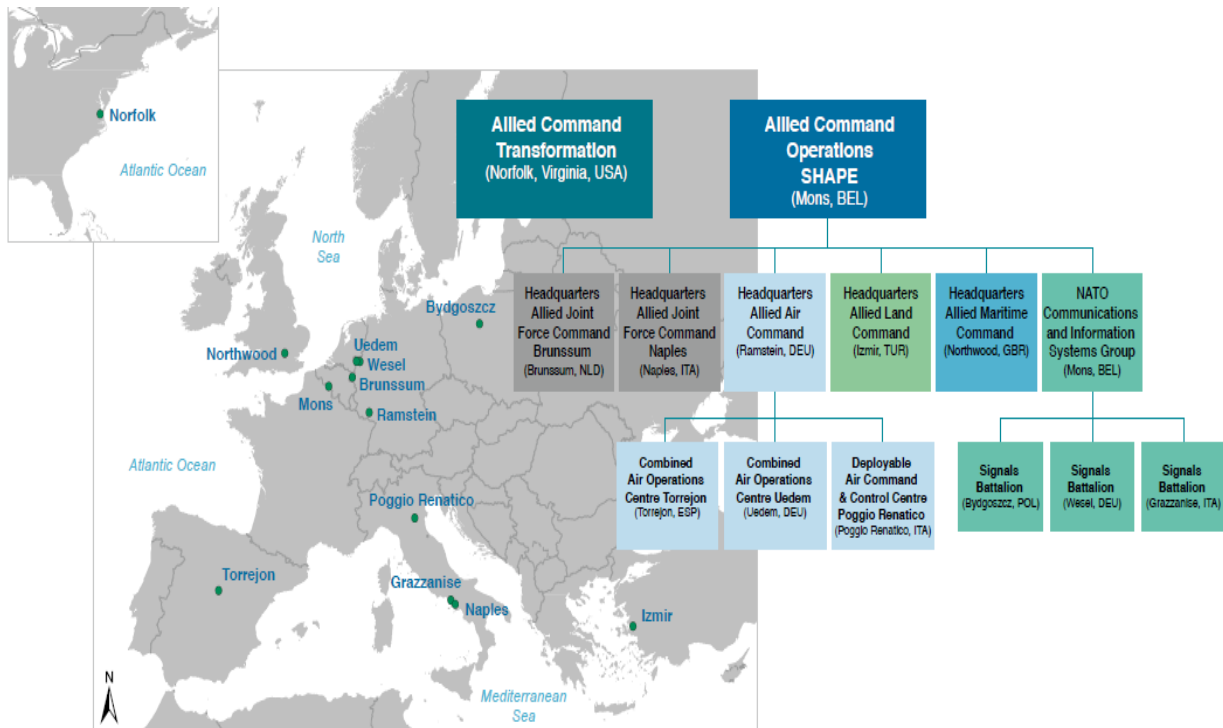


Figura 2.2: Structura actuală de comandă a NATO
 (Sursa: NATO Public Diplomacy Division, *The Secretary General's Annual Report 2012*, 16)

Intelligence în NATO – aspecte doctrinare

Doctrina NATO pentru Intelligence (AJP 2.0A) reiterează caracteristicile mediului de securitate actual și observă necesitatea – dincolo de cunoașterea aspectelor strict legate de determinarea forței și capacităților militare ale adversarului – de a aprofunda și înțelege cultura, motivațiile, perspectivele și obiectivele acestuia, corelate cu cele ale populației din teatrul de operații.

Revizuirea recentă a doctrinei și procedurilor pentru Intelligence în NATO a marcat, pe lângă diminuarea nivelului de clasificare, și re-focalizarea acestora de la cerințele specifice războiului clasic, interstatal, la intervenții limitate ca scară și la operații de tip contrainsurgență, într-un mediu operațional complex.

Factorii care influențează capacitatea Intelligence atât din perspectiva culegerii de informații din diferite surse, cât și în plan analitic, țin de complexitatea operațiilor și natura adversarului, supra-saturarea cu informații și capacitatea lor de a transcede limite de relevanță tradiționale.

Abordarea comprehensivă vine ca soluție de instituționare a relației dintre structurile militare și actorii non-militari ai mediului operațional întrunit, tot mai prezenți în zonele de criză sau conflict. Cooperarea și coordonarea optimă cu aceștia, în baza principiilor abordării comprehensive, impune și capacității Intelligence adaptarea la domenii de specialitate diverse, astfel încât să asigure căile de comunicare optime cu partenerii din mediul civil.

Doctrina NATO pentru Intelligence oferă o serie de îndrumări pentru modul în care structurile de intelligence contemporane trebuie să se adapteze la mediul actual, cum ar fi:

- focalizarea atât pe adversar, cât și pe mediul operațional;
- structurile/ mijloacele de colectare trebuie să fie pregătite să preia date și informații cu relevanță la toate nivelurile – tactic, operativ, strategic;

- asigurarea preciziei și acurateții necesare identificării adversarului disimulat în cadrul societății;
- păstrarea unei legături puternice și permanente a comandanților cu structurile Intelligence subordonate;
- asigurarea fluxurilor de informații pe orizontală și verticală în cadrul structurii de comandă;
- dezvoltarea complexului de informații legat de potențialele ținte, pentru a exploata oportunitățile oferite prin înțelegerea tuturor aspectelor asociate acestora.

După cum reiese din seria documentelor de standardizare în domeniul Intelligence în NATO (figura 2.3), nu toate disciplinele de culegere a informațiilor beneficiază de normare în acest cadru; la nivelul Alianței se fac eforturi în vederea dezvoltării de standarde¹ care să acopere întreg spectrul acestora.

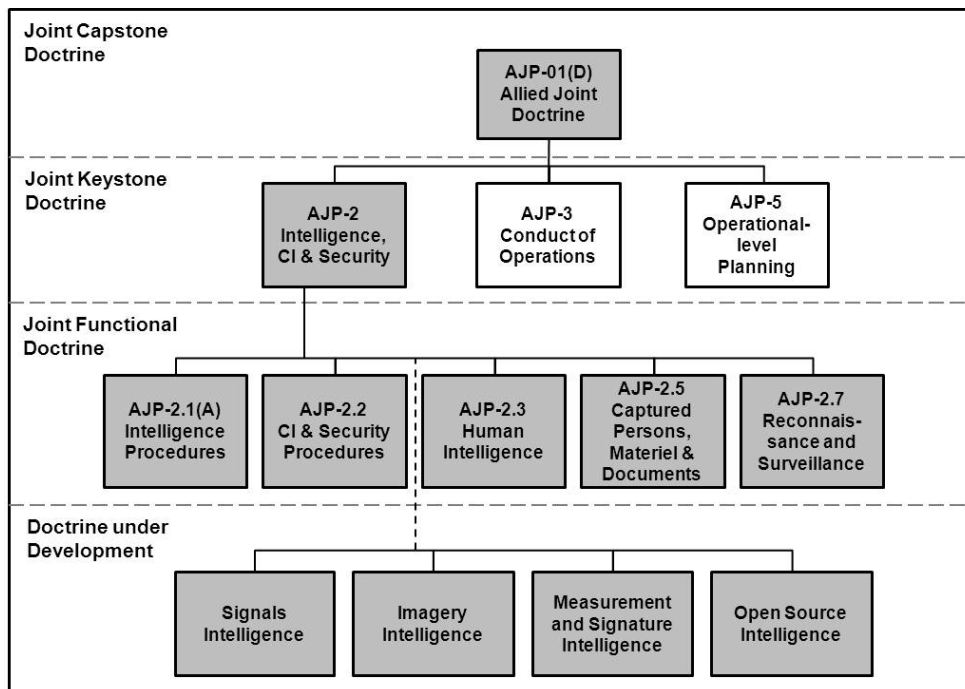


Figura 2.3 Arhitectura doctrinelor întrunite pentru Intelligence în NATO

În general, taxonomia categoriilor din spectrul Intelligence se raportează la tipul de senzor (receptorul) – incluzând modalitatea de colectare – și sursa datelor și informațiilor. În funcție de aceste elemente, distingem²:

- Intelligence Acoustic (ACINT), derivat din date legate de sunet, interceptat prin diferite dispozitive speciale: hidrofoane, geofone, sonare, sisteme integrate de supraveghere subacvatică, etc.; în general, acest tip de informații este relevant pentru detectarea mișcării și determinarea traiectoriilor;
- Intelligence din surse umane (HUMINT), provenind din date colectate de operatori umani de la surse umane (incluzând documente și materiale ale acestora); caracteristic acestui tip de intelligence este accesul la informații legate de aspecte psihologice

¹SIGINT (Olanda), IMINT (Canada), MASINT (Canada), OSINT (Canada), Biometria în sprijinul operațiilor militare (Olanda)

²Descrierea sub-diviziunilor Intelligence este făcută în baza definițiilor NATO cuprinse în catalogul AAP-6

- (intenția, starea moralului) sau sociale (relații dintre indivizi sau organizații) ale adversarului;
- Intelligence imagistic (IMINT), obținut în baza imaginilor/ capturilor video, realizate de pe platforme terestre, maritime sau aeriene/ spațiale;
 - Intelligence din măsuri și semnături (MASINT), obținut din analiza cantitativă și calitativă a datelor obținute de diferite instrumente de măsură, având ca scop principal identificarea echipamentului sau sursei generatoare de emisii;
 - Intelligence din surse deschise (OSINT), derivat din informațiile disponibile în mod public (la radio, TV, Internet, în diferite publicații) sau cu distribuție/ acces public limitat, însă fără a fi clasificate; OSINT oferă date de interes în absolut toate domeniile (Intelligence de bază) și este puternic facilitat de evoluția tehnologică în domeniul informațiilor;
 - Intelligence din semnale/ emisii (SIGINT), derivat din colectarea și exploatarea semnalelor sau emisiilor electromagnetice, poate fi separat în două surse distincte:
 - Intelligence provenit din interceptarea semnalelor electromagnetice specifice comunicațiilor (COMINT) – mesaje radio, comunicații între corespondenți, etc.;
 - Intelligence derivat evaluarea tehnică a transmisiunilor electromagnetice, altele decât comunicarea (ELINT) – cum sunt cele produse de radare, sistemele de ghidare a rachetelor, instrumente laser și în spectrul infraroșu, sau emisii în spectrul electromagnetic.

Intelligence, Supraveghere și Recunoașteri Întrunite în NATO

În NATO, disciplina Intelligence este privită ca parte a unui set de capacități integrate – Intelligence, Supraveghere și Recunoașteri Întrunite/ Joint Intelligence, Reconnaissance, Surveillance (JISR) – spectru ce întrunește elementele de planificare și operare ale tuturor mijloacelor de colectare a informațiilor cu procesarea, exploatarea, și diseminarea informației rezultate în sprijinul direct al planificării, pregătirii și execuției operațiilor¹.

Bineînțeles, nivelul de integrare a capacităților ISR naționale la nivelul Alianței este unul perfectibil², însă pașii făcuți în acest sens sunt mai mult decât promițători.

În primul rând, națiunilor NATO întrunite în cadrul proiectului MAJIIC (Multi-sensor Aerospace-ground Joint ISR Interoperability Coalition)³ trebuie să li se recunoască rolul jucat în dezvoltarea noului concept JISR în NATO, în baza tehnologiei și procedurilor comune exersate în cadrul exercițiilor ce au întrunit entități reprezentante ale națiunilor parte (MAJEX⁴), inițial limitate la disciplinele tehnice de colectare a datelor și informațiilor, acestea căpătând noi dimensiuni odată cu inițierea, planificarea și derularea seriei de exerciții-test (*trial*) Unified Vision.

¹Inițiativa JISR în NATO a luat naștere la summitul de la Chicago, în 2012

² parte din problemele identificate ținând de disponibilitatea sistemelor la nivelul națiunilor, armonizarea eforturilor de colectare sau păstrarea exclusivă a controlului asupra informațiilor și datelor colectate (Seffers, 2011)

³<http://www.nato.int/docu/update/2007/pdf/majic.pdf>

⁴<http://www.ncia.nato.int/news/Pages/20122112-MAJEX12-%E2%80%93NATO-Agency-hosted-exercise-puts-NATO%E2%80%99s-Joint-ISR-Smart-Defence-initiative-into-practice.aspx>

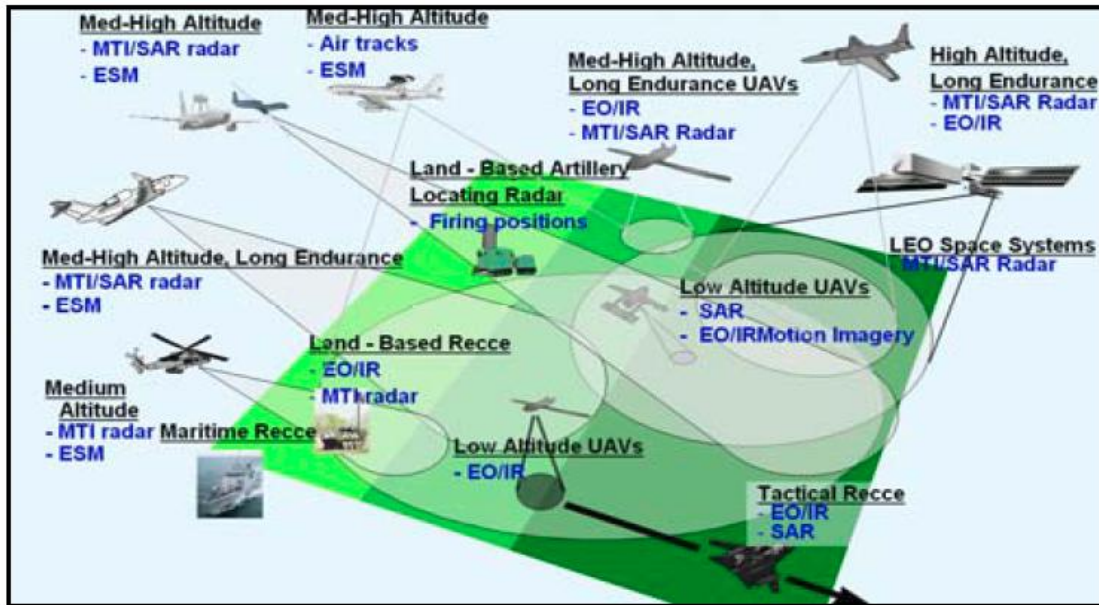


Figura 2.4 Schema senzoriilor ISR din MAJIC (2006), axată exclusiv pe colectoriile tehnici (<http://www.nato.int/docu/update/2007/pdf/majic.pdf>)

Exercițiul-test Unified Vision, ediția 2014 (figura 2.5), a avut în vedere nu doar interconectarea capacităților JISR, ci și integrarea operațională, comanda și controlul, și folosirea la nivel tactic a mijloacelor ISR. Interoperabilitatea bazată pe complianța națiunilor cu Înțelegerile de standardizare (Standard Agreements - STANAG) în domeniu necesită un mediu propice validării acestor cerințe și practicării ISR integrat în mediul operațional (Martin, 2014), iar Unified Vision reprezintă cadrul optim de antrenare, testare și ajustare a referințelor doctrinare și procedurale.



Figura 2.5 Colaj foto cu aspecte din cadrul exercițiului. Sigla exercițiului-test Unified Vision, ediția 2014 (*nemo solus sapis satis = nimeni nu este suficient de înțelept de unul singur*)¹

¹ http://www.nato.int/cps/en/natolive/photos_110396.htm

Planul de dezvoltare a capacității JISR în NATO este reprezentat în figura 2.6, cuprinzând principalele etape ce vor permite realizarea cerințelor specifice până la finalul anului 2014.

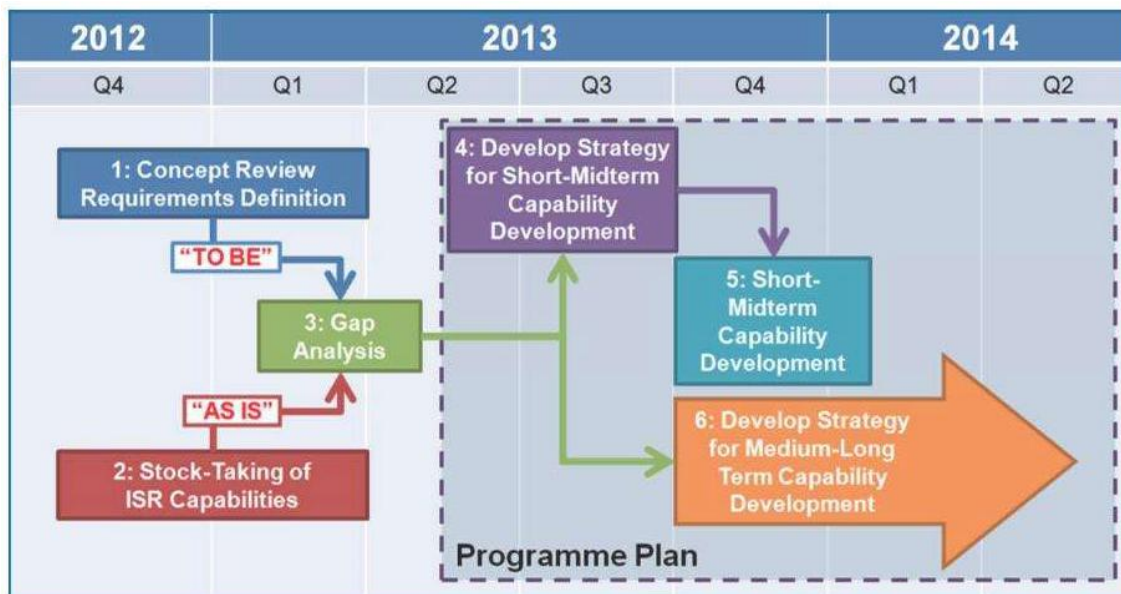


Figura 2.6 Planul de dezvoltare a capacității JISR în NATO (<http://www.aofs.org/wp-content/uploads/2013/10/131010.03-NIAG-SG177-Munday.pdf>)

Dezvoltarea capacității JISR cuprinde și o componentă esențială în asigurarea mijloacelor proprii de supraveghere ale NATO – sistemul Alliance Ground Surveillance (AGS) (Sistemul Aliat pentru Supraveghere Terestră)¹, format din cinci vehicule aeriene fără pilot Global Hawk (foto 1), precum și elementele de sprijin, comandă și control la sol.



Foto 1 Northrop Grumman RQ-4 Global Hawk (<http://www.af.mil/shared/media/photodb/photos/070301-F-9126Z-229.jpg>)

¹http://www.nato.int/cps/en/natolive/topics_48892.htm

Sistemul AGS va fi achiziționat de un grup de 14 națiuni NATO (Bulgaria, Cehia, Danemarca, Estonia, Germania, Italia, Letonia, Lituania, Luxemburg, Norvegia, România, Slovacia, Slovenia și SUA) și se preconizează că va fi operațional în 2017¹ (dată la care Franța și Marea Britanie vor evalua propria contribuție la sistem).

Acesta va permite Alianței să asigure supravegherea zonelor de interes și a obiectivelor statice sau în mișcare de la mare altitudine, folosind senzorii performanți cu care Global Hawk este echipat, în sprijinul unui larg spectru de misiuni – operații de răspuns în caz de criză/ managementul crizelor, securitatea maritimă, contraterorism, asistența umanitară, asistența în caz de dezastre naturale, etc.

Structurile de comandă NATO vor fi astfel în măsură să beneficieze de o imagine clară și în timp real a mediului de interes informațional, să identifice amenințări – sprijinind avertizarea situațională timpurie, să identifice ținte, etc., în condiții de maximă siguranță.

Dezvoltarea cunoașterii vs. Intelligence în NATO

Dezvoltarea cunoașterii (Knowledge Development - KD) – concept care la nivelul NATO semnifică procesul proactiv ce acoperă colectarea, analiza, stocarea și distribuția informației, cu scopul de a contribui la înțelegerea comună și împărtășită a mediului operațional – reprezintă modalitatea prin care produsele informative din ciclul Intelligence (focalizate pe riscuri și amenințări) se îmbogățesc ca substanță prin înțelegerea mai bună a interacțiunilor și efectelor posibile în domeniul militar, politic, economic, social, infrastructură și mediu informațional (subscris acronimului PMESII, folosit în activitatea de analiză) în diferite faze ale gestionării situației de criză.

Îndrumarul pre-doctrinal NATO privind KD evidențiază două diferențe semnificative între KD și Intelligence (Bi-SC – KD, 2011, VI):

- dacă domeniul Intelligence se concentrează asupra adversarilor actuali și potențiali, KD, submisă abordării comprehensive, observă capacitățile, interacțiunile și influențele între toți actorii principali în cadrul mediului operațional complex;
- KD cuprinde folosirea deliberată a surselor nemilitare dincolo de scopul activităților de tip Intelligence al structurilor militare, incluzând colectarea de informații și cunoaștere de la organizații internaționale guvernamentale și neguvernamentale, agenții, organizații comerciale, etc.

Capabilitatea KD este necesară activităților de avertizare situațională, planificare, execuție și evaluare a operațiilor în cadrul abordării comprehensive. Imaginea cuprinzătoare a cadrului operațional este realizată prin fuzionarea produselor KD și Intelligence într-un format analitic integrat, submis nevoii de dezvoltare a cunoașterii și înțelegerii fenomenelor securitare specifice unei zone de interes informațional.

Figura 2.7 ilustrează modalitatea în care managementul informației și al cunoașterii contribuie la dezvoltarea cunoașterii, deziderat în care capabilitatea Intelligence reprezintă un pilon esențial.

¹ Conform Declarației Summitului NATO din Wales, septembrie 2014 (<https://www.gov.uk/government/publications/nato-summit-2014-wales-summit-declaration/the-wales-declaration-on-the-transatlantic-bond>)

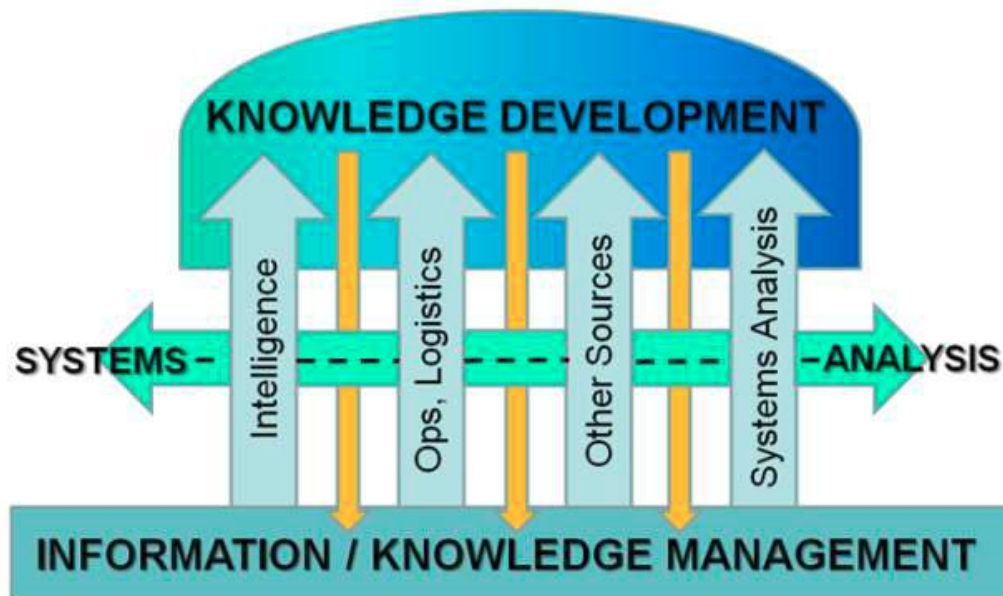


Figura 2.7 Relația dintre dezvoltarea cunoașterii și managementul informației/ cunoașterii
(Bi-SC – KD, 2011, 5-1)

Conceptul comun al Comandamentelor Strategice privind Dezvoltarea Cunoașterii descrie KD ca integrare a datelor izolate într-un bloc informațional și relațional utilizabil¹, însă – pornind de la metodologia de implementare a KD și funcțiunile specifice asumate în procesul de colectare a datelor (declarat dincolo de scopul activităților din spectrul Intelligence) – identificăm aspecte care reclamă o delimitare clară a responsabilităților celor două discipline complementare. Doar practica operațională va contribui la acest proces de consolidare identitară a KD.

Biometria în cadrul capacității Intelligence a NATO

Anonimitatea fizică, pe lângă cea din spațiul virtual, a intrat în atenția structurilor de informații și contrainformații ale forțelor militare odată cu tranziția spectrului de amenințări către cele asimetrice, neconvenționale, în care individul sau rețelele umane devin vectorul purtător al riscului de securitate. În acest caz, puterea militară și capacitățile de care aceasta dispune nu pot fi utilizate în mod corespunzător, reclamând adaptarea ”senzorilor” ISR, a capacităților de înțelegere a mediului operațional și de identificare a amenințărilor, la noile realități.

În situația în care datele/ documentele biografice pot fi prea comune pentru a permite identificarea exactă, eronat înregistrate sau traduse, falsificate sau greșit interpretate, datele biometrice, colectate cu privire la detalii fizice: topometria facială (distanța între oasele feței), a degetelor sau palmelor (amprente), forma urechii, structura irisului, structura venoasă a brațelor, structura ADN, sau de comportament: dinamica scrisului, a vocii, tastării la calculator ori ținuta mersului, devin elemente de identificare de mare precizie. Folosirea sistemelor automatizate pentru compararea și recunoașterea persoanelor este cea care asigură eficiența ansamblului, contribuind decisiv la calitatea produselor specifice diseminate.

Recunoscând necesitatea instituirii unei capacități biometrice în cadrul NATO, fapt demonstrat de realitatea mediului operațional și experiența dobândită de anumite națiuni cu bogată practică operațională și implicare activă în cercetare și dezvoltarea de soluții tehnice

¹ Bi-SC Knowledge Development Concept, 12 August 2008

necesare, statele membre NATO au adoptat, în unanimitate, Conceptul cadru al biometriei în sprijinul operațiilor NATO, MCM 0050-2012, urmat de promulgarea unui standard tehnic (STANAG 4715¹) în măsură să asigure cerințele de interoperabilitate ale sistemelor biometrice naționale.

Partea de fundamentare doctrinară a modalității de folosire a acestei capacități este în plin proces de dezvoltare, proiectul inițial al publicației aliate întrunite denumite ”Countering Threat Anonymity: Biometrics in support of NATO Operations”, a cărei custode este Olanda, fiind lansat spre dezbateri în cadrul Grupului de Lucru NATO pentru Intelligence Întrunit.

Chiar dacă anumite state NATO au folosit mijloace de înregistrare și baze de date biometrice în misiuni externe precum ISAF (foto 2), acest fapt s-a bazat în primul rând pe prevederile legislative naționale și permisivitatea procedurilor standard de operare ale misiunii. Operația NATO în Kosovo – KFOR – este prima misiune a Alianței în care se urmărește implementarea unui set de capacități biometrice care să deservească anumite sectoare de activitate în cadrul multinațional oferit de KFOR.



Foto 2 Militar SUA înregistrând date biometrice ale unui localnic în Afganistan. Dispozitivul folosit se numește Secure Electronic Enrollment Kit and Multimodal Identification Platform — construit de Cross Match Technologies, fiind același cu dispozitivul folosit pentru identificarea lui Osama bin Laden de către trupele Navy SEAL participante la operația de eliminare a acestuia²

Efortul de standardizare a capacității biometrice este unul care depășește cadrul strict al culegerii, prelucrării și schimbului de informații la nivelul structurilor militare; formațiunile specializate în asigurarea securității și aplicarea legii (figura 2.8), cu experiență acumulată în domeniu, sunt parteneri absolut necesari în demersul de identificare și neutralizare a amenințărilor reprezentate de indivizi în condițiile specifice ale lumii globalizate.

¹STANAG4715, Biometric Data Interchange, Watch listing and Reporting Standard, octombrie 2013

²<http://kitup.military.com/2013/08/marines-soldiers-biometrics-tool.html>

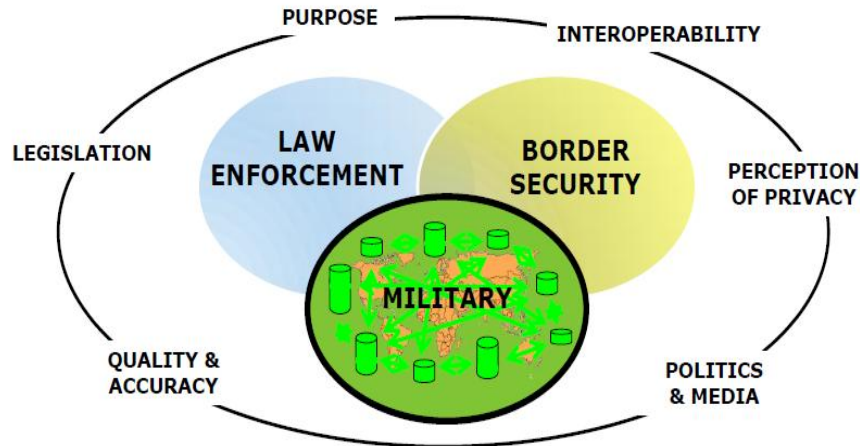


Figura 2.8 Maximizarea eficienței capabilității biometrice; limitări și oportunități de colaborare (Wulfse, 2013)

La nivel operațional și tactic, aplicațiile militare ale biometriei sunt relevante în mod deosebit în operațiuni sau acțiuni centrate pe mediul uman, și amintim aici contracararea amenințărilor reprezentate de dispozitivele explozive improvizate, protecția forței, controlul căilor de acces și a culoarelor de mobilitate, contrainsurgența, operațiile împotriva terorismului, acțiunile antipiraterie, sprijinul umanitar sau evacuarea și recuperarea personalului. Dincolo de detectarea indivizilor ce se constituie în amenințări la adresa propriilor forțe, datele biometrice se pot dovedi utile în identificarea unor persoane de interes informativ, coordonarea activității de culegere de informații din surse umane, aplicații de autentificare, etc.

În Intelligence, analiza datelor biometrice și a datelor contextuale realizează conexiunea dintre indivizi și locuri, timp, relații, activități, etc., care, coroborată cu date și informații culese prin alte mijloace specifice, pot oferi tabloul complet al unor evenimente, determina rețele umane implicate în activități ostile, detecta diferite acoperiri folosite, anticipa amenințări ș.a.m.d.

Cu toată utilitatea lor, implementarea sistemelor biometrice ridică o serie de problematici, pornind de la cele legislative și continuând cu costurile legate de achiziționarea și operarea tehnicii, standardizare și interoperabilitate, instruirea personalului, securitatea operațiilor, gestionarea bazelor de date și protecția datelor personale, schimbul de informații, automatizarea asistată de personal calificat, etc.

În funcție de soluțiile găsite pentru aceste aspecte, valorificarea expertizei naționale, găsirea de soluții comune, dezvoltarea bazei doctrinare, putem vorbi de o viitoare capabilitate solidă a NATO în acest domeniu.

Bibliografie

1. ***, *Multiple Futures Project – navigating towards 2030* (Final Report – 2009)
2. ***, *Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales from 4 to 5 September 2014*, în <https://www.gov.uk/government/publications/nato-summit-2014-wales-summit-declaration/the-wales-declaration-on-the-transatlantic-bond>
3. BINNENDIJK, Hans, HOON, Geoffrey (coord.) (2010) *Affordable Defense Capabilities for Future NATO Missions*, Special Report of Center for Technology and National Security Policy, National Defense University, USA
4. Bi-SC, *Knowledge Development Concept*, 12 August 2008

5. MARTIN, Matthew J. (2014) *Unifying Our Vision. Joint ISR Coordination and the NATO Joint ISR Initiative*, JFQ 72, 1st Quarter – Special Feature / Joint ISR Coordination and the NATO Initiative, http://www.ndu.edu/press/lib/pdf/jfq/jfq-72/jfq-72_54-60_Martin.pdf
6. NATO Public Diplomacy Division, *The Secretary General's Annual Report 2012*, in http://www.nato.int/nato_static/assets/pdf/stock_publications/20130131_Annual_Report_2012_en.pdf
7. SEFFERS, George I. (2011) *NATO Works MAJIC Again*, in SIGNAL Magazine, October 2011, <http://www.afcea.org/content/?q=node/2743>
8. *STANAG4715*, Biometric Data Interchange, Watch listing and Reporting Standard, octombrie 2013
9. WULFSE, Bernard (2013) *Biometrics in support of NATO Operations*, Netherlands Joint Task Force C-IED, presentation at 2013 Biometric Consortium Conference, <http://biometrics.org/bc2013/presentations/wulfse.pdf>
10. <http://kitup.military.com/2013/08/marines-soldiers-biometrics-tool.html>
11. <http://www.af.mil/shared/media/photodb/photos/070301-F-9126Z-229.jpg>
12. <http://www.aofs.org/wp-content/uploads/2013/10/131010.03-NIAG-SG177-Munday.pdf>
13. <http://www.hotnews.ro/stiri-esential-18042680-live-text-traian-basescu-face-declaratii-doua-summit-ului-nato.htm>
14. http://www.nato.int/cps/en/natolive/official_texts_87594.htm
15. http://www.nato.int/cps/en/natolive/opinions_101606.htm
16. http://www.nato.int/cps/en/natolive/photos_110396.htm
17. http://www.nato.int/cps/en/natolive/topics_48892.htm
18. http://www.nato.int/cps/en/natolive/topics_54644.htm
19. http://www.nato.int/cps/en/natolive/topics_98527.htm
20. <http://www.nato.int/docu/update/2007/pdf/majic.pdf>
21. <http://www.ncia.nato.int/news/Pages/20122112-MAJEX12-%E2%80%93-NATO-Agency-hosted-exercise-puts-NATO%E2%80%99s-Joint-ISR-Smart-Defence-initiative-into-practice.aspx>

CAPITOLUL 3 INTELLIGENCE SOCIO-CULTURAL

Emergența factorului socio-cultural în ecuația mediului de securitate

În lumea aflată într-o continuă transformare, caracterizată de ritmul tot mai rapid al schimbării, de incertitudine și un grad sporit de complexitate, capacitatea de adaptare devine critică. Din perspectivă organizațională adaptabilitatea poate fi ca “abilitatea de a schimba ceva sau pe cineva pentru a se potrivi unei schimbări în curs” (Andresen și Gronau, 2005), astfel putându-se aprecia că transformarea continuă reprezintă soluția adaptării cu succes la un mediu schimbător. Cu toate acestea în cazul structurilor organizaționale mari, mai ales al celor care și-au dovedit eficiența la un moment dat în timp, transformarea nu numai că poate intra în conflict cu inerenta interție organizațională, dar poate reprezenta și o serioasă sursă de risc. O soluție viabilă pentru depășirea și minimalizarea riscurilor generate de transformare o constituie determinarea și înțelegerea trendurilor și în consecință identificarea noilor caracteristici de mediu generate de acestea.

Cel mai important element de luat în considerare când discutăm despre necesitatea de transformare a capabilităților Organizației Tratatului Atlanticului de Nord (NATO) se referă la principalele caracteristici ale mediului de securitate în care aceste capabilități sunt destinate să opereze. În consecință atât NATO cât și alte organizații internaționale (IO) cu responsabilități în domeniul securității sunt preocupate de determinarea principalelor trenduri și caracteristici ale mediului de securitate viitor, precum și de impactul pe care acestea l-ar putea avea rolului de furnizor de securitate pe care aceste organizații îl au în principal.

O serie de studii elaborate de Comandamentul Aliat pentru Transformare (ACT)¹ alături de cele elaborate de OSCE, Comisia Europeană, Consiliul Național pentru Informații al S.U.A. și alte organizații reliefează modificarea mediului de securitate la începutul secolului prezent, ceea ce generează o serie nouă de provocări și amenințări globale. Anumiți factori cauzali prezentați de toate aceste studii nu numai că au un potențial ridicat de a defini trendurile globale – motiv pentru care o parte au fost prezentați în Noul Concept Strategic al NATO adoptat de summit-ul de la Lisabona din 2010 – dar prezintă și o relevanță deosebită din perspectiva înțelegerii dinamicii mediului uman, după cum urmează:

- *Competiția ideologiilor și a perspectivelor geopolitice.* Acest aspect se referă la dezacordul, ostilitatea și confruntarea generate de diferențele culturale, religioase și de valori sau a perspectivelor geopolitice diferite ale actorilor internaționali. Modificarea situației de securitate globale generează transferul de la certitudinea confruntării între superputeri spre incertitudinea interacțiunilor complexe dintre actorii statali și non-statali.
- *Alocarea resurselor naturale.* Majoritatea studiilor care abordează acest subiect subliniază ca esențiale aspectele referitoare la disponibilitatea, accesibilitatea, prețul și competiția pentru aceste resurse. Cu toate că se estimează că acestea vor continua să fie disponibile în cantități suficiente pentru a susține atât creșterea populației cât și a economiei globale, nivelul de acces și distribuția acestor resurse vor fi inegale, manifestându-se prin anumite lipsuri la nivel local și regional, ce pot provoca instabilitate socială și dezacorduri între state, generând astfel surse de conflict.² Competiția pentru resursele precum apa sau hrana este puțin probabil că va genera conflicte interstatale, însă ne putem aștepta la dispute interne sau inter-

¹ *The Multiple Futures Project (MFP) (2009) și Strategic Foresight Analysis (SFA) Report (2013).*

² UK MOD Development, Concepts and Doctrine Centre (DCDC), *Global Strategic Trends – Out to 2040*, 2010, p.73.

regionale generate de încercarea anumitor grupuri umane de a-și securiza accesul la aceste resurse vitale.¹

- *Globalizarea.* Acest aspect se referă la nivelul de integrare funcțională și al schimburilor comerciale ale economiilor naționale și regionale, iar toate documentele de referință, inclusiv cele militare², consultate pe parcursul documentării o prezintă ca factor determinant al mediului de securitate. Se estimează că puterile emergente vor juca un rol din ce în ce mai important în ecuația integrării economice, modificând echilibrul de forțe la nivel global de la hegemonie la pluralism național. Datorită tendinței de consolidare a poziției unor actori internaționali în detrimentul celorlalți generând tensiuni între identitățile naționale și cele de grup, globalizarea este legată în mod direct de competiția perspectivelor geopolitice. Cu toate că în general globalizarea contribuie la o dezvoltare constantă a intereselor economice comune între și dintre state, nu s-ar putea afirma că ea reprezintă soluția certă împotriva rivalităților și suspiciunilor internaționale.³

- *Complexitatea, impredictibilitatea și incertitudinea.* Globalizarea, competiția pentru resurse, competiția ideologică și tensiunile dintre structurile politice și sociale combinate cu diferențele culturale, religioase și ideologice pot genera alte aspecte cu impact deosebit asupra mediului de securitate, respectiv complexitatea, impredictibilitatea și incertitudinea. Marea majoritate a studiilor menționate subliniază faptul că mediul de securitate viitor va fi dominat de complexitate și impredictibilitate, aspecte ce vor constitui o adevărată provocare la adresa solidarității aliaților, având în vedere faptul că unitatea de valori, partajarea sarcinilor și anagjamentul față de deciziile comune reprezintă elementele cheie ale unei alianțe. Implicațiile derivate din scenariile “viitorurilor multiple” sugerează că mediul de securitate va suferi o modificare continuă generată de evoluții în domeniile politic, social, tehnologic și militar ce nu pot fi prevăzute cu certitudine în prezent.

- *Factorul demografic.* Trendurile sociale și demografice actuale vor avea un impact semnificativ asupra evoluției mediului de securitate amplificând potențialul apariției și intensitatea conflictelor intrastatale generate de actori non-statali.⁴ Creșterea populației globale poate avea efecte sociale semnificative cum ar fi extinderea urbanizării, adâncirea faliilor dintre clasele sociale, sărăcie, șomaj și migrație; toate acestea putând reprezenta surse de conflict. Diferențele demografice semnificative dintre țările dezvoltate și cele în curs de dezvoltare vor continua astfel că în timp ce statele dezvoltate se vor confrunta cu fenomenul de îmbătrânire și scădere a populației cele în curs de dezvoltare vor avea o populație din ce în ce mai tânără în continuă creștere, ce ar putea crea o serie de probleme majore din punctul de vedere al securității în situația în care această creștere nu este corelată cu nivelul de dezvoltare economică. Trendurile tehnologice, culturale și economice au potențialul de a alimenta tendințele de negare a comunităților și instituțiilor tradiționale, mai ales în statele dezvoltate, iar pe măsură ce fracturarea societății

¹ Canada National Defence, *The Future Security Environment 2008-2030 Part 1: Current and Emerging Trends*, ianuarie 2009, p.5.

² AJP-3.10, Doctrina Întrunită Aliată pentru Operații de Informații (noiembrie 2009) și studiul “*The Future Security Environment (FSE)*”, produs de Sub-divizia Intelligence a Comandamentului Aliat pentru Transformare (HQ SACT, 2007).

³ NATO, *NATO 2020: Assured Security; Dynamic Engagement - Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO*, mai 2010.

⁴ National Intelligence Council, Long Term Strategy Group, *2025 Security Environment: Final Report*, June 2008.

devine tot mai accentuată în aceste țări însăși existența statului național poate fi pusă la îndoială.¹

- *Tehnologia și inovația.* Utilizarea tehnologiei a devenit un factor din ce în ce mai important al mediului de securitate și se referă la ritmul exponențial de creștere a inovației tehnologice, evoluția continuă a diferitelor tehnologii, precum și gradul de diseminare și nivelul de accesibilitate al acestora, ce conferă o marjă de acțiune tot mai largă atât pentru actorii non-statali cât și pentru simplii indivizi. Proliferarea armelor de distrugere în masă, a armamentului pe bază de laser, a mijloacelor de război electronic, a nano- și bio-tehnologiilor, precum și a tehnologiilor spațiale va avea un impact major asupra mediului de securitate.² Dependența tot mai mare a infrastructurilor critice de sistemele de rețele informatice corelată cu nivelul de accesibilitate a celor mai noi tehnologii în domeniu determină ca amenințările informatice, respectiv securitatea cibernetică să devină probleme de interes major din punct de vedere al securității.

- *Aspectele privind mediul înconjurător.* Modificările climatice trebuie privite prin prisma efectelor semnificative pe termen lung cu impact asupra relațiilor internaționale deoarece aspecte precum criza tot mai pronunțată a resurselor de apă potabilă și cererile tot mai mari de resurse energetice vor avea un impact tot mai pronunțat asupra mediului de securitate în zonele de interes ale NATO. Raportul din 2013 al Forumului Economic Mondial subliniază importanța înțelegerii schimbărilor din domeniul energetic și cele ale altor resurse naturale avertizând că aceste aspecte nu trebuie examinate doar din perspective cantitative și de distribuție ci în cadrul mai larg al ecosistemelor de utilitate societală.³ Schimbările climatice afectează cu precădere statele în curs de dezvoltare, aflate deja sub presiunea problemelor economice și tensiunilor sociale, exacerbând și mai mult potențialul de instabilitate deja existent.

Caracteristicile operațiilor viitoare ale NATO. Importanța dimensiunii umane în conflictele militare

Ca o consecință directă a caracteristicilor mediului de securitate descrise anterior, apreciem că viitoarele operații militare se vor caracteriza în special prin:

- *Mediul operațional complex* reprezentat de anagajarea simultană a forțelor armate în întreg spectrul operațional – aerian, terestru, maritim, cosmic și cibernetic – în operații cu un ritm din ce în ce mai ridicat, în care mijloacele non-cinetice vor avea un rol tot mai important;
- *Operații multinaționale întrunite cu caracter expediționar*, care implică dezvoltarea unor capacități expediționare solide din partea NATO având în vedere că zonele de instabilitate cu risc major de conflict se află în afara teritoriului Alianței;
- *Creșterea probabilității confruntării cu amenințările hibride*⁴, deoarece amenințările de securitate vor fi generate cu precădere de o formă de confruntare

¹ Allied Command Transformation, *Strategic Foresight Analysis 2013 Report*, 2013.

² Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization (2010).

³ *Global Agenda*, World Economic Forum Annual Meeting 2013.

⁴ Se referă la acele amenințări de securitate generate de adversari ce au capacitatea de a recurge adaptiv atât la mijloace convenționale cât și neconvenționale pentru a-și realiza obiectivele, după cum stipulează input-urile comandamentelor strategice cu privire la noul concept NATO privind contribuția militară la contracararea amenințărilor hibride. Principala caracteristică a acestui tip de amenințări o reprezintă executarea unor combinații de acțiuni – convenționale și neconvenționale – îndreptate împotriva unor obiective atât militare cât și

hibridă caracterizată prin angajarea unor capacități convenționale, neregulate și infraționale integrate operațional și tactic până la cel mai mic nivel posibil, desfășurate în special în mediul urban sau în acele zone în care Alianța nu dispune de un sprijin adecvat;

- Confruntarea cu *adversari neconvenționali dispersați* este o consecință directă a provocării generate de amenințările hibride și reprezintă o importantă schimbare de paradigmă de la conceptul tradițional al confruntării între super-puteri unde inamicul este identificat ca actor statal spre interacțiuni cu grad de complexitate sporit între actori statali și non-statali. Deoarece NATO și-a demonstrat capacitatea de a desfășura operații convenționale rapide și eficiente, statele cu care se confruntă vor recurge tot mai mult la sprijinirea și exploatarea unor subsituenți (cum ar fi elemente teroriste sau infraționale) capabili să genereze provocări și amenințări asimetrice, care să le permită să contracareze eficient interesele, obiectivele și acțiunile Alianței fără a se angaja în acțiuni directe, astfel că rolul acestui tip de adversari va deveni tot mai important în operațiile militare viitoare;
- *Urbanizarea confruntării armate* este generată de trendurile de creștere demografică din țările în curs de dezvoltare ce prevăd că până în anul 2025 mai mult de 60% din populația lumii va trăi în orașe. Din perspectivă militară mediul urban ridică o serie de probleme deosebite datorită caracteristicilor specifice și cerințelor și limitărilor pe care le impune: efective numeroase pentru desfășurarea acțiunilor militare; limitări severe ale eficienței puterii de foc; executarea manevrei într-un mediu de confruntare multidimensional; precum și prezența în număr ridicat a populației civile;
- *Populația – centru de greutate al operațiilor* deoarece în viitor zonele de operații se vor suprapune tot mai mult cu zone dens locuite și în consecință populația va deveni un element cheie al mediului operațional, astfel că a câștiga sprijinul acesteia va reprezenta cerința de bază pentru obținerea succesului;
- *Comprehensivitatea* este generată de experiența operațiilor recente care au demonstrat că forțele armate nu dispun de capacitățile necesare pentru a gestiona exclusiv într-o manieră eficientă provocările generate de complexitatea operațiilor de stabilitate și reconstrucție astfel că abordarea multidisciplinară și intensificarea cooperării interagenții în cadrul acestui tip de operații devin imperios necesare.

Conflictele prezente relevă un nou tip de amenințări asimetrice, inedite, subtile și nedefinite, iar adversarii se amestecă și se ascund în rândurile populației locale, care în cele din urmă devine parte integrantă a mediului operațional. În conflictele actuale amenințările sunt disimulate în rândul populației ceea ce sporește complexitatea și incertitudinea operațională prin obstrucționarea identificării acestora, astfel că a câștiga sprijinul populației devine un aspect esențial pentru neutralizarea acestui tip de amenințări asimetrice. Cu toate că populația civilă a reprezentat întotdeauna un element important al mediului operațional, pe măsură ce adversarii mută intenționat desfășurarea conflictului în mijlocul acesteia, rolul populației capătă o importanță sporită, iar a-i câștiga sprijinul devine centrul de greutate al operației atât pentru NATO cât și pentru adversarii săi.

civile într-un mediu operațional din ce în ce mai larg cuprinzând și domenii imateriale, nelimitate din punct de vedere fizic cum ar fi cele financiar, cibernetic sau media. Acest tip de acțiuni sunt greu de atribuit unui anumit actor sau adversar, la fel cum este extrem de dificilă identificarea inițiatorului lor, și poate constitui rezultatul cooperării dintre state-sponsor, organizații teroriste sau infraționale, guverne corupte sau indivizi.

Recunoașterea importanței aspectelor umane ca factor al confruntării armate nu este un fenomen nou, iar pe parcursul istoriei o serie de personalități¹ și instituții² au fost preocupate de influențarea acestor aspecte în sprijinul realizării obiectivelor proprii. Deși cunoașterea inamicului a constituit întotdeauna unul dintre principiile de bază ale confruntării militare, atât operațiile militare cât și decidenții de securitate au avut adeseori de suferit datorită lipsei unei cunoașteri aprofundate a unor culturi și societăți străine. Etnocentrismul, prejudecățile și asumările bazate pe modul de gândire propriu au avut consecințe nefaste asupra unor conflicte militare cum ar fi ofensivele nord-vietnameze (1968 și 1975), războiul sovieto-afgan (1979-1989), preluarea puterii de către șiiți în Iran (1979), invazia Kuweitului de către Irak (1990), testele nucleare indiene (1998) sau al doilea război din Irak (2003-2011). (McFate, 2005, 42)

Pentru a putea contracara provocările de securitate emergente cunoașterea aspectelor umane cu privire la orice posibil adversar ar trebui considerată ca prioritară, impunându-se o transformare imediată a paradigmei conceptuale NATO deoarece, pe de o parte, natura adversarului s-a schimbat fundamental comparativ cu perioada războiului rece, iar pe de alta, mediul operațional actual s-a modificat fundamental în ultimii douăzeci de ani ca rezultat al globalizării și al noilor caracteristici ale mediului de securitate. O serie de studii recente au demonstrat cât se poate de clar că este absolut necesar ca NATO să întreprindă eforturi mai consistente pentru înțelegerea mediului uman și a fi în măsură astfel să comunice mai eficient cu populația locală, autorități și alți actori din zona de operații pentru a-și îndeplini cu succes misiunile.

Operațiile recente din Kosovo, Afganistan și Libia demonstrează că înțelegerea atât a mediului uman din zona de conflict cât și a motivațiilor populației de a sprijini fie activ, fie pasiv oponentii Alianței sunt aspecte cheie ce trebuie luate în considerare pentru dezvoltarea capacităților NATO. Lipsa cunoașterii aspectelor umane poate avea consecințe serioase și nedorite, în timp ce, dimpotrivă, înțelegerea culturii adversarului poate face o diferențiere pozitivă la toate nivelele: strategic, operativ și tactic. (McFate, 2005, 44) Neînțelegerea aspectelor umane poate genera stabilirea unor obiective nerealiste la nivel strategic, dezvoltarea unei imagini publice negative la nivel operațional și punerea în pericol atât a trupelor proprii cât și a populației civile la nivel tactic. (McFate, 2005, 45)

Succesul operațiilor viitoare va depinde de tot mai mult de integrarea în procesul de planificare militară a cunoștințelor din domeniul științelor sociale ce au potențialul de a facilita exploatarea la scară largă a aspectelor umane. În ciuda unor progrese moderate în ceea ce privește recunoașterea importanței acestor aspecte pentru operații, cum ar fi Strategia de Abordare Comprehensivă sau actualizarea procesului de planificare al operațiilor, Alianței nord-atlantice încă îi lipsesc programele, sistemele, modelele, personalul specializat și structurile organizatorice adecvate pentru a putea contracara cu succes amenințările prezente și viitoare.

În lipsa unei surse centralizate de cunoștințe și analize cu privire la aspectele umane comunitățile militară și politică, cărora aceste informații le sunt necesare în cea mai mare măsură, trebuie să se rezume la sursele proprii, insuficiente în cele mai multe situații. (McFate, 2005, 46) Cu toate acestea, dezvoltarea unor mecanisme eficiente de accesare într-o manieră oportună a cunoștințelor și informațiilor, existente dispersat la diferite nivele în cadrul statelor membre, de către decidenți și planificatori, ar contribui la îmbunătățirea semnificativă la nivelul NATO a gradului de înțelegere a dimensiunii umane a mediului operațional.

¹ Sun Tzi 544-496 Î.C., Alexandru cel Mare 356–323 Î.C., Niccolò Machiavelli 1469–1527 D.C., Thomas Edward Lawrence 1888–1935 D.C., etc

² De exemplu Biroul de etnologie americană înființat în timpul războaielor indiene (1865-1885) sub conducerea maiorului John Wesley Powell.

Aspectele umane ale mediului operațional

Înțelegerea aspectelor umane ale mediului operațional își are originea în sincopelile cu care NATO s-a confruntat în operațiile recente în ceea ce privește înțelegerea și adaptarea la dimensiunea umană a teatrelor de operații în care a desfășurat acțiuni militare. După cum rezultă din trendurile actuale și în viitor preponderența operațiilor Alianței va consta în operații de răspuns la situații de criză non-articol 5 (NA5CRO) desfășurate în afara teritoriului propriu, astfel că înțelegerea dimensiunii umane a mediului operațional și transformarea capacităților acționale în acest sens vor continua să reprezinte o prioritate pentru NATO în vederea executării cu succes a acestui tip de operații. Apreciem că reușita unui astfel de demers depinde nemijlocit de identificarea unor soluții concrete pentru sporirea cooperării și coordonării acțiunilor Alianței cu organizațiile internaționale, cu diferitele structuri guvernamentale din cadrul statelor membre, cu mediul academic și think-tank-urile, precum și cu diferite organizații neguvernamentale pe baza principiilor strategiei de abordare integrată.

În vederea realizării unei înțelegeri unitare a problematicii abordate apreciem că *aspectele umane ale mediului operațional* reprezintă un set complex de elemente, factori, procese, interacțiuni și percepții dintr-o societate afectată de un nivel ridicat de violență ce au capacitatea nu numai de a influența operațiile unor forțe armate ci chiar de a determina rezultatul final al conflictului. Aceste aspecte se referă la factorii psihologici, culturali și sociali în relație cu contextul istoric, politic, instituțional, economic, militar și legal generate de o situație de criză. Aspectele umane au o deosebită relevanță pentru operațiile de stabilitate și reconstrucție, de contrainsurgență, de menținere/impunere a păcii, precum și alte operații similare.

Analiza acestor aspecte poate fi concentrată în șapte domenii prezentând următoarele aspecte principale de interes:

1. Motivația acțiunilor umane
 - Înțelegerea factorilor care generează acțiunile indivizilor contribuie la îmbunătățirea relaționării cu persoanele aparținând unui civilizații sau culturi diferite;
 - Cunoașterea faptului că satisfacerea nevoilor fundamentale tinde să reprezinte principala prioritate a indivizilor indiferent de cultura căreia îi aparțin vine în sprijinul inter-relaționării culturale;
 - Observarea răspunsurilor comportamentale și emoționale la diferite situații conduce la identificarea motivațiilor fundamentale ale acțiunilor umane;
 - Crearea unor nivele de așteptare ridicate fără a fi și satisfăcute generează situații conflictuale, chiar și în cazul satisfacerii așteptărilor de nivel inferior;
 - Normele morale au un rol important atât asupra manierei în care indivizii încearcă să își satisfacă nevoile fundamentale cât și în ceea ce privește opțiunile comportamentale;
 - Observarea modului în care rețelele individuale se suprapun și interacționează poate revela potențialul de cooperare sau conflict;
 - În cadrul unui grup sau al unei comunități indivizii au tendința de a recurge la acele decizii care minimalizează costurile personale și maximizează recompensele materiale.
2. Înțelegerea mediului uman:
 - Înțelegerea acestui mediu favorizează și managementul contactului inițial cu o cultură diferită, dar și procesul de adaptare la cultura respectivă;
 - Comunitățile locale reprezintă o sumă de grupuri umane cu nivele diferite de influență, motivate de factori naturali și contextuali;

- Comunitățile umane trebuie analizate temporal din perspectiva dinamicii schimbării și nu ca succesiune de imagini statice fără fundament;
 - Odată cu desfășurarea într-o anumită zonă forțele NATO devin un actor principal în cadrul respectivei comunități, iar succesul lor poate depinde de abilitatea de a trata cu respect opiniile membrilor acelei comunități, pe de o parte, iar pe de alta, de a furniza acele îmbunătățiri ale situației locale pe care comunitatea respectivă și le dorește;
 - Înțelegerea răspunsurilor anterioare ale unei comunități la situațiile conflictuale poate contribui la anticiparea reacțiilor la un nou conflict sau la o intervenție a NATO;
 - Crearea unei structuri de analiză a aspectelor umane poate furniza nivelul de cunoaștere necesar planificării în avans a potențialelor operații viitoare;
 - Integrarea metodelor de analiză specifice științelor umaniste și sociale în procesul de analiză a informațiilor asigură mijloacele necesare studierii eficiente a proceselor care determină atitudinile, credințele și opiniile diferitelor culturi.
3. Comunicarea inter-culturală:
- Acest proces reprezintă elementul cheie în crearea raportului cu o altă cultură;
 - Multiculturalismul intrinsec specific NATO constituie un avantaj substanțial în portretizarea alianței față de potențialii interlocutori;
 - Înțelegerea modului în care populația locală își procură informațiile și adaptarea mesajelor la nivelul audienței țintă sunt elemente fundamentale ale unei comunicări eficiente;
 - “Competența inter-culturală” trebuie să constituie o cerință de bază pentru personalul militar și civil destinat să interacționeze cu reprezentanții altor culturi;
 - Înțelegerea mediului cultural și social, mai ales a sistemului social cu dinamica și subsistemele sale specifice, este fundamentală pentru o comunicare inter-culturală constructivă.
4. Dinamica situației locale:
- Cu toate că înțelegerea acestei dinamici reprezintă o adevărată provocare, deopotrivă pentru forțele NATO dar și pentru populația locală, ea este de importanță critică pentru realizarea obiectivelor strategice ale misiunii;
 - Înțelegerea mecanismelor și echilibrelor de putere constituie un element cheie pentru înțelegerea situației locale;
 - Stabilirea unor obiective operaționale adaptate la specificul situației locale prin identificarea unui echilibru corespunzător între ceea ce se dorește la nivel strategic, ceea ce poate fi acceptat la nivel local și ceea ce se poate realiza de forțele desfășurate în teren constituie cerința de bază pentru succesul unei operații;
 - Schimbările de situație trebuie gestionate luând în considerare faptul că și o schimbare pozitivă generează sentimente de insecuritate, rezistență, teamă sau pierdere a identității.
5. Percepția și acceptarea operațiilor NATO:
- Legitimitatea constituie fundamentul acceptării prezenței forțelor NATO de către populația locală;
 - NATO poate își poate îndeplini parțial obiectivele strategice fără a se angaja în acțiuni de luptă, doar prin influențarea eficientă și pozitivă a percepțiilor;
 - Aplicarea principiilor validate de experiența ONU în operații de sprijinire a păcii poate îmbunătăți substanțial performanțele NATO în executarea operațiilor de stabilitate și reconstrucție;

- Angajamentul liderilor cheie alături de legătura și mentoratul operațional constituie domenii noi de acțiune în sprijinul îndeplinirii obiectivelor operaționale;
 - Strategia de informare publică și comunicarea sunt elemente critice pentru realizarea obiectivelor la toate nivelele.
6. Determinarea atitudinilor față de operațiile NATO:
- Înțelegerea oportună a atitudinilor populației față de acțiunile forțelor NATO poate contribui la îmbunătățirea succesului operațional;
 - Atitudinile sunt imput-uri deliberate ale intențiilor și comportamentului;
 - Pentru realizarea modificării comportamentale este necesară înțelegerea și influențarea convingerilor și/sau atitudinilor individuale în direcția dorită;
 - Analiza periodică a atitudinilor populației poate veni în sprijinul procesului de planificare operațională atât pe termen scurt cât și pe termen lung;
 - Utilizarea mijloacelor tehnice moderne contribuie la îmbunătățirea culegerii datelor specifice, precum și la îmbunătățirea analizei acestora.
7. Transformarea capacităților NATO pentru a se adapta mai bine mediului uman:
- Operațiile recente au demonstrat că dimensiunea umană a mediului de acțiune reprezintă un element determinant al rezultatului unei operații militare ce impune transformarea capacităților existente și chiar dezvoltarea unor capacități noi;
 - Înțelegerea aspectelor umane specifice zonei de operații este esențială pentru planificarea unei operații reușite;
 - Provocările generate de complexitatea mediului operațional actual și viitor impun dezvoltarea unui concept în acest domeniu și implementarea aspectelor umane ca o nouă capacitate integrată prin adaptarea modului de gândire; organizării; proceselor decizionale; tacticilor, tehnicilor și procedurilor precum și a programelor educaționale și de instruire;
 - Orice eventual program de transformare a capacităților în acest domeniu trebuie să se bazeze pe principiile strategiei de abordare integrată și să se axeze pe direcțiile de acțiune specifice Sistemului de dezvoltare a integrării a capacităților întrunit¹: DOTMLPFI (doctrină, organizare, instruire, asigurare materială, leadership, personal, facilități/infrastructură și interoperabilitate);
 - Implementarea unui sistem de planificare operațională integrată nu numai că ar permite NATO să își coordoneze acțiunile cu principalii actori internaționali (organizații internaționale și neguvernamentale) încă din fazele premergătoare ale operațiilor, dar ar facilita și o mai bună integrare a resurselor umane și materiale naționale și internaționale, prevenind disfuncționalitățile din interacțiunea civilo-militară;
 - Integrarea cunoștințelor și metodologiei specifice științelor sociale poate îmbunătăți semnificativ maniera militară tradițională de înțelegere a dimensiunii umane a mediului operațional.

Premizele creării disciplinei SOCINT

Inteligența culturală este o teorie managerială și a psihologiei organizaționale care postulează faptul că înțelegerea impactului zestrei culturale a unui individ asupra comportamentului său este esențial în asigurarea eficienței activității și în măsurarea abilității de angajare cu succes în orice mediu/cadru social. Inteligența culturală facilitează cunoașterea culturală, solicitând un anumit nivel de empatie; pentru organizația militară, inteligența

¹ Joint Capabilities Integration Development System.

culturală reprezintă abilitatea de a lua decizii în baza înțelegerii tuturor factorilor culturali¹, și reprezintă un atribut epistemic al liderului.

Dincolo de aspectul specific dezvoltării cunoașterii, cu aplicabilitate universală, abordarea volumului de date și informații specifice acestui mediu din perspectiva Intelligence presupune, la nivel strategic, înțelegerea sistematică a obiceiurilor, atitudinilor morale și culturii populațiilor străine în vederea îmbunătățirii eficacității inițiativelor de securitate națională (Patton, 2010). În acest sens, capabilitatea SOCINT:

- urmărește determinarea unor răspunsuri operaționale pentru scenarii indezirabile din punct de vedere cultural;
- facilitează discernerea impactului imediat al acestui răspuns și evaluarea efectelor în detrimentul operației;
- condiționează comportamentul trupelor și facilitează comunicarea eficientă;
- sprijină procesul de identificare a indicatorilor și avertizărilor;
- asigură succesul operațiilor sub acoperire, etc.

Operațiile militare sunt direct dependente de toți factorii de impact, cuantificabili sau mai puțin previzibili, care determină cursurile de acțiune, influențează procedurile și efectele și, în cele din urmă, asigură succesul sau provoacă insuccesul acțiunii. Analiza informativă a mediului operațional, ca parte a procesului decizional, marchează în mod elocvent trecerea de la modelul analitic specific războiului convențional, unde spațiul de referință era unul bidimensional, geografic (câmpul de luptă – *battlefield*), completat ulterior, odată cu dezvoltarea importanței forțelor aeriene, cu dimensiunea aerospațială (spațiul de luptă – *battlespace*), la mediul operațional multidimensional (*operational environment*), care integrează aspectele sociale în peisajul acțiunilor militare. Acest fapt vine ca o recunoaștere a emergenței operațiilor neconvenționale, centrate pe populație, în care amenințările prevalente sunt de natură asimetrică sau hibridă, acestea reclamând adaptarea capacităților și procedurilor de culegere și prelucrare a informațiilor.

Indivizii și rețelele umane fiind vectori ai amenințărilor, comunitățile umane reprezintă centrul de gravitate al operațiilor, iar înțelegerea și interpretarea corectă a mecanismelor motivaționale și relaționale, raportate la o multitudine de condiționări psiho-sociologice și funcționale, devine o cerință fundamentală a spectrului de colectare și a abordărilor analitice din cadrul disciplinei Intelligence.

Figura 3.1 prezintă procesul tradițional de analiză a factorilor operației în procesul de luare a deciziei – misiunea, inamicul, terenul, timpul, trupele proprii, cărora li se adaugă considerațiile privind populația civilă. Modelul analitic aplicat acestui din urmă factor cuprinde ansamblul de elemente care definesc în mod general comunitățile umane. Spațiile geografice de dispunere, structurile organizării sociale, capabilitățile deținute de comunități, organizațiile prezente în zonă, caracteristicile populației și evenimentele vieții de zi cu zi din zona de operații (elemente întrunite în acronimul ASCOPE) interferează cu ritmul operațiunii și relaționează, direct sau indirect, cu diferite formațiuni ale structurii de forțe.

¹ factorii culturali includ: limba, societatea, economia, obiceiurile, istoria, religia

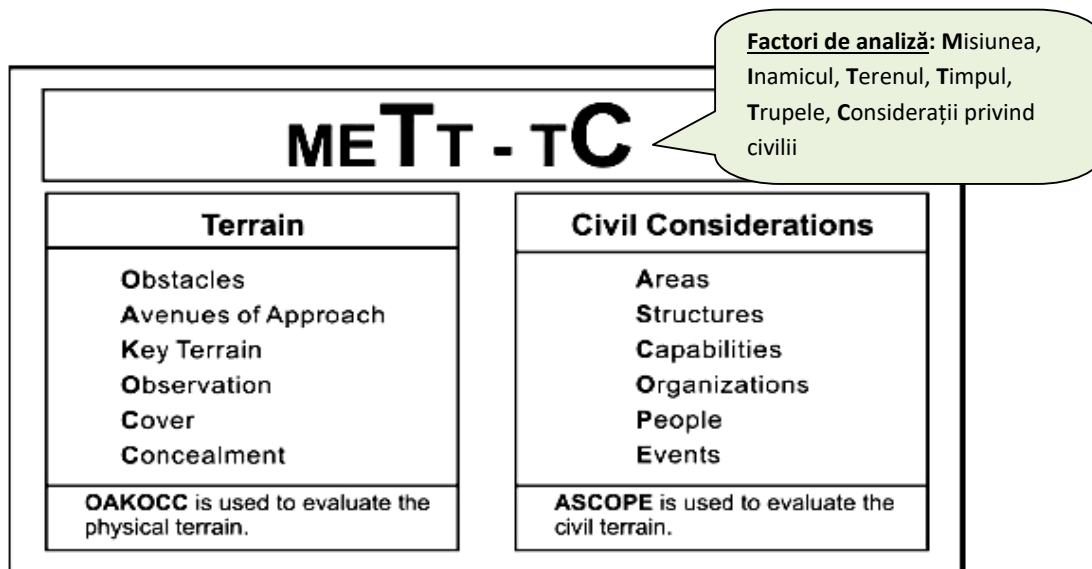


Figura 3.1 Factorii de analiză ai operației; ASCOPE – elemente de referință în formularea considerațiilor privind populația civilă (FM 3-05.40 (FM 41-10) 2006, fig. 1-3, 1-4)

Dincolo de abordarea tradițională, prevalența operațiilor în medii predominant umane a dus la necesitatea dezvoltării unor modele mai elaborate de înțelegere a comunităților cu care se interacționează, astfel încât să faciliteze comunicarea și sprijinul primit din partea acestora.

În acest proces analitic îmbunătățit (cum e cel specific operațiilor împotriva insurgenței), considerațiilor privind civilii (ASCOPE, figura 3.1) le sunt aplicate o serie de variabile cunoscute (în jargon militar) ca PMESII (*political, military/ security, economic, social, infrastructure, and information*) – politic, militar/ de securitate, economic, social, de infrastructură și informație (figura 3.2).

	P Political	M Military	E Economic	S Social	I Infrastructure	I Information
A Area	District boundary, provincial boundary, party affiliation areas	Coalition/ANSF bases, historic ambush/IED sites	Bazaar areas, farming areas, livestock dealers, auto repair shops	Traditional picnic areas, bazaars, outdoor Shura sites	Irrigation networks, water tables, areas with medical services	Radio, TV, & newspaper coverage areas, word of mouth gathering points
S Structures	Provincial/district centers, Shura halls, polling sites	Provincial/district police HQ, INS known leader house/business	Bazaar, wheat storage, banks	Mosques, wedding halls, popular restaurants	Roads, bridges, electrical lines, gabion walls, dams	Cell, radio, TV towers, print shops
C Capabilities	Dispute resolution, local leadership, INS ability to have impact	ANSF providing 24/7 security, QRF presence, INS strength/weapons	Access to banks, ability to withstand drought, development	Strength of tribal/village traditional structures, mullahs	Ability to build/maintain roads, walls, check dams, irrigation systems	Literacy rate, availability of electronic media, telephone service
O Organization	Political parties, INS group affiliations, GOV & NGO organization	Coalition & ANSF present, INS groups present	Banks, large landholders, cooperatives, economic NGOs	Tribes, clans, families, sports Shuras, youth Shuras	Government ministries, construction companies	News organizations, influential mosques, INS IO groups
P People	Governors, councils, Shura members, elders, mullahs, parliamentarians	Coalition, ANSF, INS military leaders	Bankers, landholders, merchants, money lenders	Mullahs, Malliks, elders, Shura members, influential families	Builders, road contractors, local development councils	Media owners, mullahs, Malliks, elders, heads of families
E Events	Elections, Shurahs, Jirgas, provincial council meetings, speeches	Kinetic events, unit RIEs, loss of leadership, operations	Drought, harvest, business opening, loss of business, good/bad crop	Friday prayers, holidays, weddings, deaths, births, bazaar days	Road/bridge construction, well digging, center/school construction	Friday prayers, publishing dates, IO campaigns, project openings, CIVCAS incidents

Figura 3.2 Spectrul analitic complex al mediului operațional uman (după Doctrina contrainsurgență)

În general, și fără pretenții de exhaustivitate, PMESII descriu substanța și caracteristicile adversarului, facilitând determinarea punctelor sale tari și slabe. Factori suplimentari de analiză pot fi adăugați în funcție de specificul operației, iar flexibilitatea și ajustabilitatea acestui model lasă loc dezbaterilor asupra diferitelor încercări de operaționalizare a unor noi concepte menite să faciliteze o înțelegere și integrare adecvată a aspectelor umane în mediul operațional.

Importanța dată factorului uman a mers până la a caracteriza noul mediu operațional ca ”teren uman”¹ – de altfel un sugestiv joc de cuvinte promovat în cadrul armatei SUA; la nivel operaționalizat, programul ”Sistemele Terenului Uman” (Human Terrain Systems/HTS)² a fost lansat ca inițiativă menită „să furnizeze comandanților și statelor majore echipe socioculturale în scopul îmbunătățirii nivelului de înțelegere a populației locale și de a aplica această cunoaștere în procesul decizional”³. În acest sens, sunt folosiți specialiști din domeniul antropologiei, sociologiei, științei politice, studiilor regionale și lingvistice, proveniți, cu predilecție, din mediul civil – fapt ce a dus la o serie de critici provenite din lumea academică cu privire la etica unui astfel de demers (Price, 2011; Lucas, 2009) sau chiar la folosirea HTS ca acoperire pentru activitatea de Intelligence⁴.

Din 2012, HTS este promovat ca o capacitate esențială în fazele incipiente ale stării de criză în orice zonă de interes pe glob (Hodges, 2012), contribuția sa fiind marcată în special în segmentul dezvoltării cunoașterii.

O altă inițiativă a armatei SUA este ”Sociocultural Behavior Capability Areas Framework” (Cadrul domeniilor de capacitate ale comportamentului sociocultural), gestionat prin Programul pentru cercetare și inginerie din cadrul Departamentului pentru Apărare al SUA, program ce urmărește dezvoltarea abilității de a anticipa comportamentul grupurilor sau al indivizilor cheie în context operațional, în baza unui set de patru capacități (figura 3.3):

- a. Capacitatea de a înțelege (capacități de sprijin prin percepție și comprehensibilitate, în baza științelor sociale și comportamentale, a caracteristicilor și dinamicilor socioculturale în mediul operațional);
- b. Detectarea (capacități de descoperire, distingere și localizare a semnelor socioculturale relevante operațional prin colectarea, procesarea și analiza datelor comportamentale socioculturale);
- c. Anticiparea (capacități de urmărire și anticipare a schimbărilor la nivelul entităților sau în cadrul fenomenelor de interes, orientate multidimensional, prin folosirea intensivă a diferitor categorii de senzori și modelarea mediului);
- d. Atenuarea (capacități de dezvoltare, prioritizare, execuție și măsurare a cursurilor de acțiune fundamentate pe științele sociale și comportamentale). (Schmorrow, 2011)

¹ ”populația umană în mediul operațional [...] după cum este definită și caracterizată prin date socioculturale, antropologice și etnografice, sau provenind din alte surse non-geografice” (Kipp et al., 2006)

² Programul este gestionat de către United States Army Training and Doctrine Command (TRADOC), devenind din 2010 un program permanent în cadrul armatei SUA

³ <http://humanterrainsystem.army.mil/>

⁴ <http://www.ncanthros.org/>; la nivel operational, HTS nu este parte a ciclului Intelligence, dar este acceptat ca și facilitator pentru Intelligence (US Army Military Intelligence Center of Excellence (2011) Military Intelligence Professional Bulletin: Human Terrain System, 37 (4). PB34-11-4. în http://www.fas.org/irp/agency/army/mipb/2011_04.pdf)

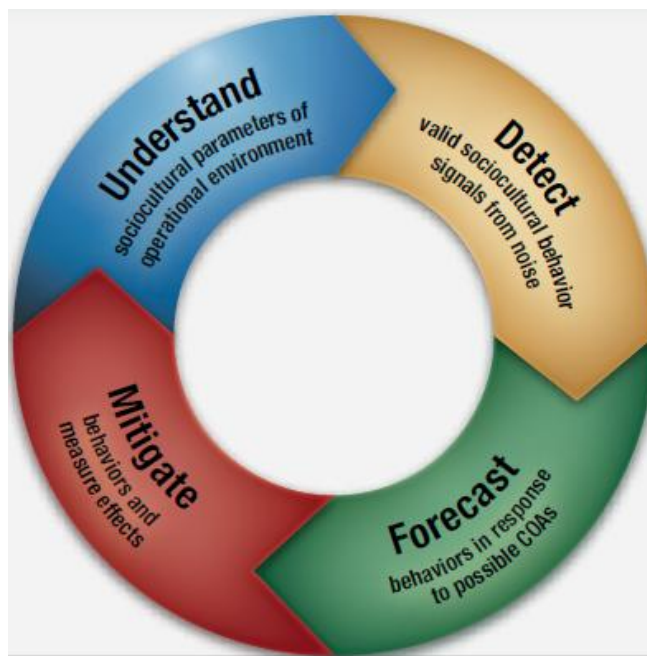


Figura 3.3 Cadrul domeniilor de capabilitate ale comportamentului sociocultural (Schmorrow, 2011)

Proiectul "Sociocultural Behavior Capability Areas Framework" este bazat pe fundamente științifice solide, cum ar fi cele oferite de Programul de modelare a comportamentului uman socio-cultural/ Human Social Culture Behavior (HSCB) Modeling Program (figura 3.4), și urmărește conectarea produselor proprii la o serie de capabilități ale armatei SUA, cum ar fi: Capabilitatea de Analiză a Rețelelor Sociale, Consorțiul Cunoașterii Culturale, capabilitatea de "radar" social și Sistemul Integrat de Avertizare Timpurie în caz de situație de criză, Modelul Mediului Operațional Național, etc. (Schmorrow, 2011).



Figura 3.4 Programul de modelare a comportamentului uman socio-cultural (HSCB), newsletter 2012, în <http://www.dtic.mil/biosys/files/HSCB-news-winter-2011.pdf>

Relevanța cunoașterii mediului uman este recunoscută și în NATO, primele încercări de conceptualizare făcând referire la această disciplină ca și ”capabilitate socio-culturală”, în cadrul spectrului larg al Intelligence. Această capabilitate exploatează competențele științelor umane¹ în a furniza informații de bază și date răspunzând cererilor de informații ale factorilor decizionali, în măsură să fundamenteze estimări ale capabilităților și abilităților actorilor din zona de interes, sprijinind decisiv procesul de planificare operațională.

Cu toate acestea, mediul academic încă dezbate diferența între Intelligence socio-cultural (SOCINT) și analiza socio-culturală (subsumată *dezvoltării cunoașterii*). Dacă Intelligence îmbunătățește abilitățile perceptive ale atitudinilor curente, dar și a schimbărilor paradigmatică sau comportamentale, analiza socio-culturală îmbunătățește abilitățile de a înțelege modalitatea în care aceste atitudini, paradigme sau comportamente se formează sau diferă la nivel local și cum se relaționează cu alte fenomene culturale (Knotwell, 2013).

Una dintre structurile NATO cele mai avizate în ce privește relaționarea cu mediul civil, Centrul de Excelență NATO pentru Cooperare Civili-Militari (CCOE), a introdus conceptul de Advanced Cultural Competence (ACC) – Competență Culturală Avansată, ca model de aprofundare și înțelegere a aspectelor socio-culturale generale și specifice². Pornind de la noțiunea de cultură ca gen proxim al modelelor antropologice definitorii pentru comunitățile umane, CCOE distinge cinci dimensiuni culturale ale acestora, cu relevanță operațională:

- a. dimensiunea fizică (sistemul teritorial);
- b. dimensiunea economică (resurse, activități lucrative și comerciale, etc.);
- c. dimensiunea socială (clase sociale, gen, vârstă);
- d. dimensiunea politică (diviziunea puterii, participarea în procesele decizionale);
- e. dimensiunea simbolică, identitară (credeințe, istorie).

Cunoașterea acestor dimensiuni facilitează o serie de abilități ale forțelor dislocate: identificarea intențiilor actorilor, construirea încrederii, convertirea opiniilor, gestionarea percepțiilor, înțelegerea mecanismelor comunităților, înțelegerea culturii, permițând identificarea amenințărilor ca fricțiuni între diferite realități și interese. Din punct de vedere al referințelor doctrinare/ procedurale, CCOE nu își propune un demers complex, limitându-se la intenția de publicare a unor îndrumare care să acopere aspecte specifice subsumate dimensiunilor socio-culturale identificate. În orice caz, acestea vor reprezenta o resursă utilă în orice fundamentare ulterioară a unei capabilități SOCINT.

SOCINT reprezintă rezultatul analizei și coroborării de date și informații din domeniul cunoașterii socio-culturale, fapt practicat de secole în mediul militar, dar neinstituționalizat ca atare. Kerry Patton propune mai mult o descriere decât o definiție tehnică a SOCINT, văzută ca abordare sistemică ce se bazează pe înțelegerea legăturilor, nodurilor și conectorilor ce construiesc rețelele umane multidimensionale în cadrul societăților, pornind de la faptul că într-un sistem cognitiv nu există actori izolați, ci doar interconectați. Abordarea realităților socio-culturale din perspectivă sistemică permite corectarea sistemelor disfuncționale prin identificarea elementelor afectate și aplicarea măsurilor corective necesare – în cadrul unor proiecte, programe, etc (Patton, 2010).

Chiar dacă Patton încearcă o definiție funcțională a SOCINT (*”direcționarea, colectarea, analiza și producerea de informații sociale și culturale”*), pornind de la logica construcțiilor termonologice în NATO, propunem o definiția a SOCINT ca *intelligence provenit din prelucrarea de date și informații de natură socio-culturală*, cu mențiunea că o

¹ antropologia, studiile culturale, demografia, istoria, geografia umană, științele politice, psihologia socială, sociologia, etc.

² <http://www.cimic-coe.org/content/scope/acc.php>

dezvoltare ulterioară a fundamentării operaționale a termenului trebuie să clarifice o serie de aspecte critice legate de:

- direcționare: care trebuie făcută în baza unor competențe specifice (unde dezvoltarea cunoașterii în domeniul socio-cultural, ca și capacitate epistemică, joacă un rol deosebit¹);
- managementul cererilor de intelligence (identificarea câmpurilor funcționale ale capabilității socio-culturale și construirea unui model al input-urilor științelor umane);
- colectarea de date și informații socio-culturale (din surse deschise, de către operatori umani, etc.);
- analiza informațiilor socio-culturale (urmând pașii analizei critice; coroborarea cu date și informații provenite din alte surse);
- diseminarea produselor de intelligence socio-cultural (canale, clasificare);
- distincția între SOCINT și dezvoltarea cunoașterii.

Algoritmii acțiunii socio-culturale presupune parcurgerea unor pași (identificarea problemei, identificarea sistemului, înțelegerea cauzalității, prezentarea de soluții posibile), însă valoarea ca produs de intelligence vine odată cu integrarea în logica procesului de pregătire informațională a mediului operațional, menit să identifice actorii din zona de acțiune/ interes, să sprijine înțelegerea acestora ca sisteme și să permită anticiparea acțiunilor pe care toți acești actori le vor întreprinde în relația cu elementul militar.

Figura 3.5 oferă imaginea finală obținută prin suprapunerea elementelor de analiză (PMESII-ASCOPE) specifice operațiilor centrate pe mediul uman.

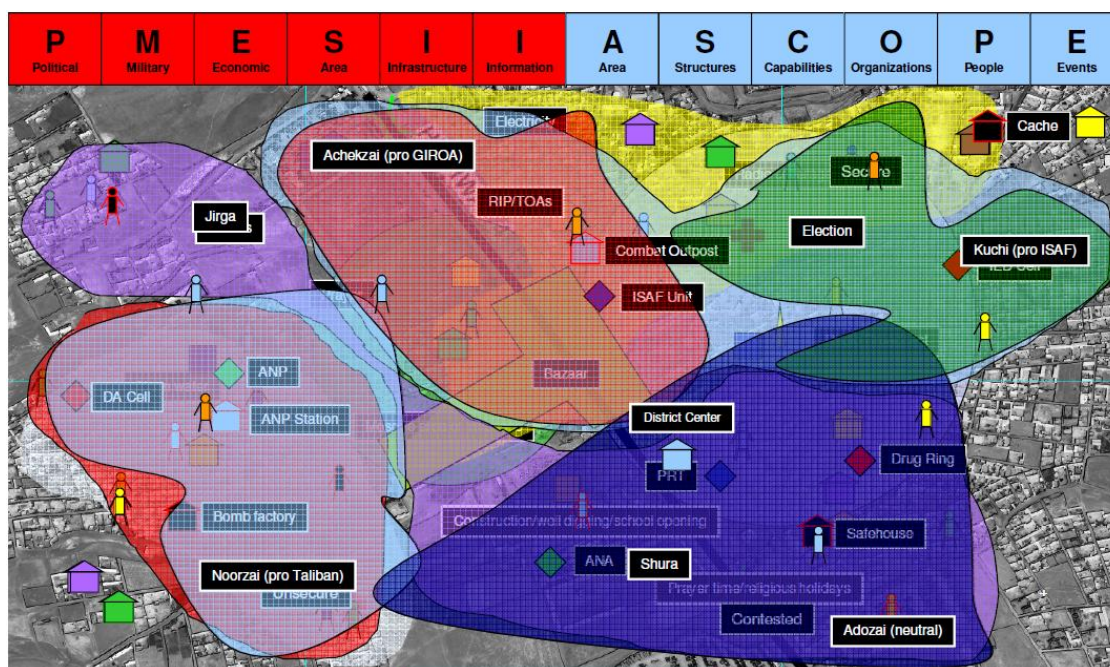


Figura 3.5 Pregătirea informațională a mediului operațional – overlay (după Doctrina contrainsurgență)

Practica operațională a mers mai departe în ce privește integrarea aspectelor socio-culturale în cadrul capabilității Intelligence, dar și la nivel de dezvoltare a cunoașterii în fundamentarea diferitelor tipuri de operații. Platforma CIDNE (Combined Information Data Network Exchange/ Schimbul prin Rețea a Informațiilor Combinat) reprezintă o bază de date

¹ Această capacitate poate fi suplinită prin existența unui grup de consilieri calificați

interconectată ce furnizează abilitatea ca diferite comunități naționale sau multinaționale disparate să capteze, gestioneze și distribuie datele de care dispun în sprijinul oricărei operații prin intermediul unei interfețe web¹ (figura 3.6).

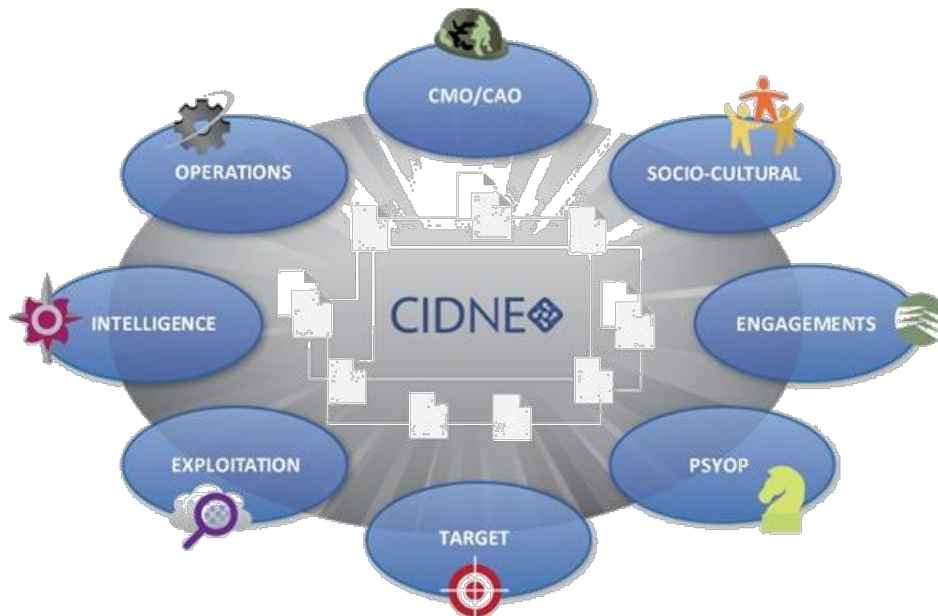


Figura 3.6 Platforma CIDNE – contributori (<http://www.issinc.com/products/cidne/>)

În ceea ce privește SOCINT, CIDNE asigură atât repozițorul achizițiilor senzorialor umani, cât mijloacele necesare vizualizării din perspectivă sistemică a rețelelor umane formale și informale, facilitând reprezentarea acestora în baza unor indecși dinamici și furnizând structurilor de analiză produse customizate deosebit de utile în activitatea acestora (figura 3.7).



Figura 3.7 – Platforma CIDNE – vizualizarea rețelelor umane (<http://www.issinc.com/products/cidne/>)

¹ www.issinc.com

Concluzii

Instituționalizarea considerațiilor referitoare la aspectele umane în cadre conceptuale bine definite se dovedește tot mai mult o necesitate, date fiind condițiile concrete în care amenințările la adresa securității se materializează.

Dincolo de soluții temporare, cum ar fi folosirea de consilieri specializați în diferite discipline umaniste pentru sprijinirea eforturilor într-o situație bine determinată, sau cuprinderea caracteristicilor mediului uman sub umbrela dezvoltării cunoașterii, se impune dezvoltarea disciplinei SOCINT ca și ramură distinctă în cadrul capacității Intelligence.

Acest fapt presupune o solidă fundamentare doctrinară, care să construiască un algoritm credibil al modalității în care științele sociale contribuie la ciclul intelligence, să identifice formele și modalitățile de colectare a datelor și informațiilor, utilizarea acestora în procesele analitice și să marcheze finalitatea produselor ca Intelligence acțional.

SOCINT urmărește să răspundă întrebărilor legate de motivația comportamentelor și modul în care acestea sunt condiționate de către percepții, credințe, obiceiuri, ideologii, religie, etc. (Sorrentino, 2011), sprijinind procesele decizionale la toate nivelurile – strategic, operațional sau tactic, și determinând modalitatea în care resursele la dispoziția factorilor de decizie sunt folosite în vederea atingerii obiectivelor propuse.

Bibliografie

1. ANDRESEN, K., GRONAU, N. (2005) *An Approach to Increase Adaptability in ERP Systems*, în: *Managing Modern Organizations with Information Technology: Proceedings of the 2005 Information Resources Management Association International Conference*
2. BROWN, Donald E. (1991) *Human Universals*, McGraw-Hill, San Francisco
3. ERLICH, Kate, CARBONI, Inga (2012) *Inside Social Network Analysis*
4. HODGES, Jim (2012) *Cover Story: U.S. Army's Human Terrain Experts May Help Defuse Future Conflicts*, în <http://www.defensenews.com/article/20120322/C4ISR02/303220015/Cover-Story-U-S-Army-8217-s-Human-Terrain-Experts-May-Help-Defuse-Future-Conflicts>
5. KIPP, Jacob, GRAU, Lester, PRINSLOW Karl, DON SMITH, Captain (2006) *The Human Terrain Systems: a CORDS for the 21st Century*, Military Review, September-October, <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GefTRDoc.pdf&AD=ADA457490>
6. KNOTWELL, J. (2013) *Socio-cultural Analysis (SCA) Different from Intelligence—Complementary but Different*, în <https://www.culturalknowledge.org/socio-cultural-analysis-sca-different-from-intelligence%E2%80%94complementary-but-different.aspx>
7. LUCAS, George R., Jr. (2009) *Anthropologists in Arms: The Ethics of Military Anthropology*, Claremont Institute Series on Statesmanship and Political Philosophy, Kindle Edition
8. MACKAY, Andrew, TATHAM, Steve (2011) with a chapter by Rowland, Lee, *Behavioural Conflict: Why Understanding People And Their Motivations Will Prove Decisive in Future Conflict*
9. MARC, Alexandre, WILLMAN, Alys, ASLAM, Ghazia, REBOSIO, Michelle, BALASURIYA, Kanishka (2012) *Societal Dynamics and Fragility: Engaging Societies in Responding to Fragile Situations*. Washington DC: World Bank. DOI: 10.1596/978-0-8213-9656-8. License: Creative Commons Attribution CC BY 3.0
10. McFATE, Montgomery (2005) *The Military Utility of Understanding Adversary Culture*, in *Joint Force Quarterly*, Issue 38
11. McKINLAY, John (2002) *Cooperation in the conflict zone*, www.nato.int/acad/fellow/99-01/mackinlay.pdf
12. NELSON, C. Richard (2006) *How should NATO handle Stabilisation Operations and Reconstruction efforts?*, The Atlantic Council of the United States, Policy paper
13. PATTON, Kerry (2010) *Sociocultural Intelligence: A New Discipline in Intelligence Studies*, Continuum Intelligence Studies, Kindle Edition
14. PRICE, David H. (2011) *Weaponizing Anthropology: Social Science in Service of the Militarized State*, Counterpunch
15. SCHMORROW, Dylan (2011) *Sociocultural Behavior Reserach and Engineering in the Department of Defense Context*, Office of the Secretary of Defense, <http://www.dtic.mil/biosys/files/SBRE2011.pdf>

16. SORRENTINO, Diana (2011) *Socio-Cultural Intelligence. Understanding the Theories, Practice and Importance of the Sociological and Cultural Discipline as it applies to your Collection and Analysis of Intelligence Data*, in [http://www.brgresearchgroup.com/uploads/Article - SocioCultural Intelligence - 2011_02_10_02.pdf](http://www.brgresearchgroup.com/uploads/Article_-_SocioCultural_Intelligence_-_2011_02_10_02.pdf)
17. STORTI, Craig (2001), *The art of crossing cultures*, Intercultural Press, Inc
18. AAP-06 (2012), *NATO glossary of terms and definitions*
19. AAP-15 (2012), *NATO glossary of abbreviations used in NATO documents and publications*
20. AJP-01(D) (2010), *Allied Joint Doctrine*
21. AJP-3.10 (2009), *Allied Joint Doctrine for Information Operations*
22. AJP-3.4(A) (2010), *Allied joint doctrine for Non-article 5 crisis response operations*
23. AJP-3.4.1 (2001), *Peace support operations*
24. Allied Rapid Reaction Corps (ARRC), Commanders Initiative Group (CIG) – Programme Paper: ISP PP 2010/01, *Operationalizing the Comprehensive Approach*, March 2010
25. Canada National Defence (2009) *The Future Security Environment 2008-2030 Part 1: Current and Emerging Trends*, January
26. Defense Science Board (DSB) (2009) *Report of the Defense Science Board Task Force on Understanding Human Dynamics*, March
27. National Intelligence Council, Long Term Strategy Group (2008) *2025 Security Environment: Final Report*, June
28. NATO (2010) *NATO 2020: Assured Security; Dynamic Engagement – Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO*, May
29. NATO Allied Command Transformation (2007) *The Future Security Environment (FSE)*, produced by the Intelligence Sub-Division
30. NATO Allied Command Transformation (2013) *Strategic Foresight Analysis 2013 Report*
31. NATO Allied Command Transformation, Università di Bologna, Istituto Affari Internazionali (2012) *Dynamic Change, Rethinking NATO's Capabilities, Operations and Partnerships*, Academic Conference
32. Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization (2010)
33. U.S. Center for Army Lessons Learned (2011) *Afghanistan Provincial Reconstruction Team Handbook*, February
34. UK MOD Development, Concepts and Doctrine Centre (DCDC) (2010) *Global Strategic Trends – Out to 2040*
35. US Army FM-307 (FM 100-20) (2003) *Stability Operations and Support Operations*, Headquarters, Department of the Army
36. World Economic Forum Annual Meeting (2013) *Global Agenda*

CAPITOLUL 4 INTELLIGENCE DIN SURSE UMANE. ÎNTRE SPIONAJ ȘI CULEGEREA DE INFORMAȚII DIN SURSE UMANE LA NIVEL OPERAȚIONAL ȘI TACTIC

Introducere. De la spionaj la HUMINT

Culegerea de informații din surse umane este o practică ce a existat din cele mai vechi timpuri, depășind bariere de civilizație, cultură sau istorie. Pornind de la necesități militare, de control asupra teritoriilor ocupate, folosite pentru depășirea competitorilor în diferite domenii – de la producție, comerț și până la cercetarea științifică - practicile clandestine de a colecta informații de la alte persoane și-au dovedit valoarea într-o multitudine de circumstanțe critice.

Păstrându-și relevanța (chiar caracterul indisponibil) ca generator de intelligence, culegerea de informații din surse umane a îmbrăcat binecunoscuta "haină" conceptuală a spionajului.

Într-o abordare specifică realităților securitare specifică secolului XX, spionajul este definit ca *"activitatea de culegere secretă a unor date și informații de importanță politică sau militară despre o altă țară, sau descoperirea secretelor unei companii, prin folosirea spionilor"* (Oxford Advanced Learner's Dictionary, 2010), statutul spionului fiind dezvoltat în cadrul convențiilor de la Haga și de la Geneva privind dreptul războiului și dreptul internațional umanitar (D.I.U.).

Articolul 29 al Regulamentului anexă la Convenția a IV-a de la Haga, din 1907, enunță elemente constitutive ale statutului spionului, prevăzând că acesta este un individ care *„lucrând pe ascuns sau sub pretexte mincinoase, adună ori încearcă să adune informații în zona de operațiuni a unui beligerant, cu intenția de a le comunica părții adverse"*¹, făcând totodată distincție față de unitățile de cercetare, încadrate cu militari în uniformă (nedeghizați), trimiși în recunoaștere în teritoriul inamic, în zona operațiilor militare.

Protocolul I Adițional la Convențiile de la Geneva 1977² aduce elemente noi în definirea spionului, legate de spațiul de acțiune („teritoriul controlat de către o parte adversă”), statutul militarilor rezidenți al acestui teritoriu care culeg informații de interes militar (și care nu sunt asimilați spionilor dacă nu acționează sub pretexte false ori clandestin, beneficiind de statutul de prizonieri de război), precum și condiționarea statutului de spion de locația/momentul capturării (înainte de a se alătura forțelor cărora le aparține – fapt ce nu exclude urmărirea ulterioară în justiție pentru violări ale Dreptului Războiului (Johnson și alții, 2013).

În timp de conflict militar, spionii acționează în cadrul unor misiuni acoperite sau clandestine, pentru a obține informații cu caracter preponderent militar despre inamic (potențial uman, starea moralului, dotare, amplasamente, planuri de operații etc.). În această situație, potrivit dreptului internațional cutumiar și convențional, chiar dacă sunt participanți la conflicte, spionilor capturați nu li se recunoaște statutul de combatant (și protecția aferentă garantată de către D.I.U.). Singura garanție care i se poate asigura unui spion este aceea de a fi judecat în conformitate cu legile statului care l-a capturat, după o judecată prealabilă.

În acest context, trebuie subliniat faptul că spionajul nu este o activitate specifică războiului; spionii acționează în egală măsură pe timp de pace, fiind cetățeni ai unui stat ori

¹Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907, în <http://www.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=090BE405E194CECBC12563CD005167C8>

²Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, în <http://www.icrc.org/applic/ihl/ihl.nsf/ART/470-750057?OpenDocument>

persoane fără cetățenie (în serviciul unui stat) care acționează împotriva altui stat culegând date și informații secrete pe care le transmit agențiilor de apartenență.

Avansul tehnologic fulminant din ultimele decenii, concretizat în diferite soluții tehnice și tipuri de senzori, dispozitive și aparatură de comunicare și supraveghere capabile să acopere o mare parte din nevoile de informare ale factorilor decizionali, a dus la o scădere a relevanței culegerii de informații din surse umane. Disciplinele tehnice, GEOINT, IMINT, SIGINT, COMINT, ELINT, precum și fluxul informațional specific societății bazate pe cunoaștere, ca sursă a OSINT, au prevalat ca fiind sigure din punct de vedere al protecției operatorilor, totodată furnizând date concrete, bazate pe suport real.

Cu toate acestea, evoluția spectrului de amenințări în lumea globalizată, precum și caracterul operațiilor militare recente și actuale, au determinat ca informațiile din surse umane (HUMINT) să revină în prim-planul interesului atât a serviciilor și agențiilor statale din domeniul securității, cât și în mediul militar. Nivelul de utilizare al acestei capacități dictează și caracteristicile definitorii pentru modul în care resursele, mijloacele și procedurile specifice disciplinei sunt percepute.

Astfel, putem vorbi despre HUMINT la nivel strategic, gestionat de către serviciile de informații/ contrainformații în plan intern, sau serviciile de informații externe ale statelor, prin intermediul instituției atașaturii militare, dar și în mod acoperit, prin mijlocirea unor rețele de spionaj, în funcție de interesele de securitate naționale și opțiunile existente¹. Riscurile rezultate din activitatea clandestină sunt deosebit de ridicate, națiunile în cauză putând recurge la deportarea, închiderea sau chiar executarea spionilor capturați. În cazul imunităților diplomatice², persoanele implicate în acte de spionaj pot fi declarate "persona non grata" și obligate să părăsească teritoriul țării respective.

La nivel militar operațional-tactic, HUMINT este abordat ca "*intelligence derivat din informațiile colectate de la sau furnizate de către surse umane*" (AAP-6, 2013), în cadrul unui spectru larg de acțiuni și misiuni specifice, care implică – într-o viziune comprehensivă a operației – toți militarii ca "senzori umani" (într-un cadru bine determinat), precum și structuri specializate în culegerea și managementul acestui tip de informații.

În cadru național se manifestă abordări diferențiate în ce privește nivelul de clasificare a documentelor doctrinare referitoare la acest subiect, din rațiuni de securitate. În NATO, documentele de standardizare referitoare la HUMINT (AJP-2.3, Doctrina aliată întrunită pentru HUMINT și AintP-5, Doctrina NATO pentru proceduri HUMINT³) au un nivel de clasificare care nu permite accesul larg la consultarea acestora, primând principiile securității informației ("nevoia de a cunoaște"); în schimb, manualul american FM 2-22.3, care detaliază aspecte specifice operațiilor de colectare a informațiilor din surse umane, este postat pe internet, fără restricții de acces⁴.

Și la nivel conceptual apar diferențe notabile în ce privește structurile, funcțiunile și procedurile HUMINT. Școala anglo-saxonă de Intelligence include în spectrul HUMINT operațiile cu sursele, întâlnirile cu persoanele oficiale, interogarea persoanelor reținute,

¹În cazul SUA, FBI este responsabil pentru culegerea de informații din surse umane pe plan intern, iar CIA – pe lângă alte componente – este însărcinată cu colectarea informației în afara granițelor, prin folosirea întreg spectrului Intelligence, în cadrul unor operații cu caracter deschis sau sub acoperire (<http://www.fbi.gov/about-us/intelligence/disciplines>)

²Decretul nr. 566/1968 pentru ratificarea Convenției cu privire la relațiile diplomatice, Viena, 18 aprilie 1961 publicată în B.Of. nr. 89/8.07.1968, în http://www.google.ro/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCkQFjAA&url=http%3A%2F%2Fwww.just.ro%2FPortals%2F0%2FCooperareJudiciara%2FGhidCooperare%2520Penal%2FJurisdicti e%2F2a.doc&ei=Wy4NU91dw73KA_OJgtAD&usq=AFQjCNEALWJhM17xAXPT34Mcp-VnYOcKag

³documentul este în curs de revizuire, sub noua denumire de "Proceduri, tehnici și tactici HUMINT în NATO"

⁴FM 2-22.3 (FM 34-52) Human Intelligence Collector Operations, 2006, în <http://www.fas.org/irp/doddir/army/fm2-22-3.pdf>

precum și interviewarea civililor sau a propriului personal, în anumite circumstanțe (Beall, 2009). Doctrina franceză înglobează în HUMINT (în limba franceză ROHUM – renseignement d'origine humaine) atât culegerea de informații ca rezultat al interacțiunii interpersonale (conversation) – ROHUM-C – cât și informațiile obținute prin observare, fără contact interpersonal cu adversarul – asimilat recunoașterilor în adâncimea dispozitivului inamic (reconnaissance – de unde acronimul ROHUM-R) (Poucet, 2006, 74).

Dezvoltarea istorică a capacității înregistrează chiar programe de cercetare concentrate asupra dezvoltării unei laturi neconvenționale a HUMINT – obținerea de informații prin mijloace paranormale (clarviziune sau telepatie), unde SUA a fost concurată de Uniunea Sovietică (Bremseth, 2001).

Un algoritm teoretic de bază al operației de culegere de informații din surse umane cuprinde¹:

- identificarea nevoilor de informații;
- determinarea locației informației;
- identificarea persoanelor care au acces la informația respectivă;
- construirea scenariului pentru întâlnirea și evaluarea indivizilor cu acces la informația dorită;
- identificarea persoanei susceptibile și recrutarea acesteia ca agent;
- menținerea unei legături securizate cu agentul și preluarea de la acesta a fluxului de informații urmărit.

Dezvoltarea resurselor necesare colectării și analizei informațiilor din surse umane necesită timp; totodată, operatorii HUMINT sunt vulnerabili în fața tacticilor de inducere în eroare ale serviciilor de contrainformații (Margolis, 2013). Acestea sunt doar o parte din limitările acestei discipline, însă sunt contrabalansate de avantajele pe care HUMINT le oferă. Pe lângă costul relativ redus în comparație cu disciplinele tehnice de culegere a informațiilor, aspectele acoperite de sursele umane sunt greu accesibile altor senzori; folosirea agenților este o resursă valoroasă; agenții sunt experți în domeniile de interes, cu vizibilitate asupra evenimentelor sau lucrurilor ce fac obiectul culegerii de informații (Margolis, 2013).

Nivelul tactic al culegerii de informații din surse umane solicită atât cunoștințele și abilitățile militare, cât și trăsăturile de personalitate ale operatorilor HUMINT. Manualul pentru contrainsurgență al Armatei SUA descrie operatorul HUMINT ca fiind capabil să "acționeze cu un minim de echipament și să fie dislocat în orice mediu operațional, în sprijinul ofensivei, a luptei de apărare, în cadrul operațiilor de stabilitate și reconstrucție sau în sprijinul civililor"². Pregătirea operatorului HUMINT include elemente aprofundate de cunoaștere a aspectelor socio-culturale în aria de operații, limba locală, limbajul non-verbal, etc.

Chiar dacă nu este o disciplină dependentă de tehnologie, sprijinul cu sisteme și aparatură specifică este menit să îmbunătățească performanța generală a acestei capacități. Pe lângă programele informatice destinate instruirii, managementului operațiilor, gestionării surselor și raportării/ schimbului de informații, regăsim la nivel tactic aparatură individuală menită să sprijine operatorii în colectarea de date (Ackerman, 2006):

- Aparatură de înregistrare audio-video;
- Dicționare digitale portabile cu translator;
- Aparatură de înregistrare a datelor biometrice;
- Tehnică de comunicații și transmitere de date;
- Detectoare de minciuni portabile, etc.

În principiu, elementele HUMINT acționează în zone de responsabilitate atribuite, acoperind sectoare ale mai multor unități, coordonarea cu aceste limitându-se la aspecte de

¹<http://www.dhra.mil/perserec/adr/counterintelligence/counterintelligence.pdf>

²FM 3-24, Counterinsurgency, December 2006, 5-39

control tactic. În anumite circumstanțe operaționale, cum ar fi contrainsurgența, eficiența echipei HUMINT este dată de integrarea atât în mediul de culegere (menținând contact zilnic cu comunitatea), cât și de relația directă și constantă cu subunitatea sprijinită (Beall,2009). Această practică pozitivă la nivel tactic este confirmată și de generalul Flynn, fost locțiitor al Șefului de Stat Major pentru Intelligence în cadrul ISAF, cu acoperire pentru întreg spectrul culegerii de informații și al procesului analitic (Flynn și alții, 2010).

Dezvoltarea capabilității HUMINT, în toate aspectele definiției, rămâne un deziderat puternic legat de experiența practică. Un model pentru dezvoltarea unei capabilități HUMINT comprehensive este oferit de R. Steele, antrenând viziunea transparenței care să angreneze cu titlu permanent atât comunitățile, cât și entitățile specializate în colectarea de informații din surse umane (figura 4.1).

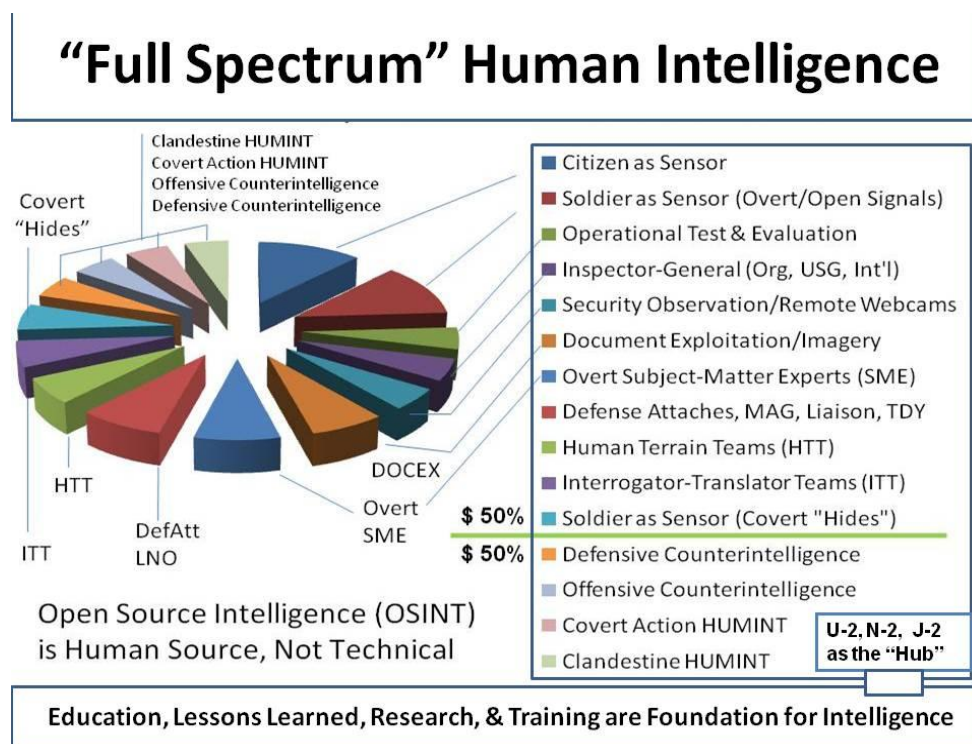


Figura 4.1 HUMINT într-o abordare comprehensivă (Steele, 2010)

Cadrul larg al dezvoltării capabilității HUMINT în NATO

Adaptarea Alianței la mediul de securitate este un proces continuu, în măsură să asigure dislocabilitatea, sustenabilitatea și superioritatea forței, precum și capacitatea de a răspunde unei game largi de provocări, în concert cu alte organizații. Conceptul Strategic al NATO din 2010¹ exprimă viziunea Alianței și definește prioritățile sale în materie de securitate, identificând tipurile de operații ce fundamentează parametrii de dezvoltare a capabilităților militare ale Alianței² - proces reconfirmat la Summitul NATO din 2012 la Chicago³.

¹<http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf>

²Procesul de planificare a apărării în NATO se bazează pe Directiva Politică emisă în 2011, în vederea atingerii obiectivelor stabilite prin noul Concept Strategic

³http://www.nato.int/cps/en/natolive/official_texts_87593.htm?mode=pressrelease

Apărarea colectivă, managementul crizelor și cooperarea în materie de securitate – dincolo de aspectele politico-militare – reclamă o abordare pragmatică, graduală, dictată de noile realități ale lumii globalizate, marcată de provocările crizei financiare și economice prelungite, competiția politico-economică, dezvoltarea spectrului de amenințări și fragilizarea statală.

Între obiectivele curente ale procesului de planificare a apărării în NATO, domeniul Intelligence este direct vizat de ambiția Alianței de a-și menține și dezvolta capacitatea de proiecție a forței la distanță strategică, în cadrul unor operații derulate în paralel, fapt ce necesită un sprijin corespunzător cu informații pentru apărare, într-un cadru operațional larg, ce implică relația cu o multitudine de parteneri.

Evaluarea provocărilor, identificarea indicatorilor și semnalarea avertizărilor aferente riscurilor de securitate provenite din diferite medii, asociate categoriei de amenințare (amenințări în mediul cibernetic, proliferarea/ uzul armelor de distrugere în masă, securitatea energetică) sau tipologiei emergenței acesteia (terorism, eșuare statală, competiția de putere și pentru accesul la resurse) sunt elemente care solicită efectiv spectrul informațiilor pentru apărare, al supravegherii și recunoașterilor întrunite (JISR¹), domeniu în care NATO este dependent de contribuția națiunilor.

Pachetul de capabilități pentru apărare adoptat la Chicago prevede, ca element critic pe termen lung, asigurarea superiorității informaționale; aceasta se bazează pe acțiunea coerentă a diferite tipuri de senzori de culegere a informațiilor și capacități de prelucrare și diseminare a acestora, în toate domeniile acționale.

Un prim pas în vederea îmbunătățirii acestei capabilități este proiectul NATO pentru implementarea sistemului propriu de supraveghere aeriană a spațiului terestru (AGS – Alliance Ground Surveillance), un pas important în asigurarea mijloacelor necesare constituirii unei capabilități robuste ISR. Datele culese vor acoperi un larg spectru de cereri de informații, de la identificarea elementelor/ pozițiilor în teren ale forțelor din zonele de interes, aspecte privind mobilitatea acestora și până la înregistrarea efectelor dezastrelor naturale (Sirak, 2013) – însă, cu toată acuratețea lor, acestea nu sunt suficiente pentru realizarea unui tablou complet și complex, la nivel strategic și operativ, asupra realității multidimensionale ale acestora. În acest scop, produselor de imaginerie ale AGS li se adaugă și rezultatele obținute de celelalte elemente ale spectrului Intelligence.

În cele ce urmează, vom aborda starea actuală și modalitatea în care capabilitatea HUMINT în NATO își poate demonstra relevanța (unicitatea) și utilitatea, profilând o proiecție a dezvoltării acesteia pe termen scurt și mediu, în scopul asigurării necesarului de informații din surse umane în procesul de planificare a apărării.

Coordonate ale capabilității HUMINT în NATO

Acronimul DOTMLPFI (Doctrină, Organizare, Educație și Instruire, Sprijin logistic/ baza materială, Conducere/ leadership, Personal, Infrastructură și Interoperabilitate) reprezintă coordonatele ce definesc o capabilitate militară în NATO. O scurtă trecere în revistă a acestor aspecte este edificatoare pentru starea actuală, provocările și perspectivele pe care disciplina HUMINT le are în NATO, cu efecte directe în modelarea componentelor de specialitate naționale.

Doctrina – asimilată în acest caz procesului de standardizare (elaborare și implementare a standardelor), cu acoperire asupra aspectelor teoretice legate de principiile și procedurile de referință ale manifestării capabilității în plan operațional, este unul dintre aspectele în continuă dezvoltare în NATO. În conformitate cu reglementările NATO privind

¹Joint Intelligence Surveillance Reconnaissance

procesul de elaborare și mentenanță a documentelor de standardizare, aceste publicații sunt revizuite la fiecare trei ani – fapt ce asigură implementarea periodică a elementelor necesare conformării cu evoluțiile factorilor obiectivi, armonizării cu alte documente de standardizare, implementării rezultatelor procesului de lecții învățate și bune practici, etc.

La acest nivel, disciplina HUMINT beneficiază de formularea clară a principiilor, proceselor și responsabilităților de bază în domeniu, cuprinse în Politica HUMINT în NATO, document aflat în responsabilitatea Statului Major Internațional – Divizia Intelligence. Un rol deosebit de important în elaborarea documentului l-a avut Grupul de lucru NATO HUMINT (NHWG), inițiatorul acestui demers, precum și HCOE, care prin expertiza asigurată în procesul de ajustare, adjudecare și implementare a comentariilor/ propunerilor națiunilor, a marcat prima contribuție importantă în domeniul fundamentării teoretice a disciplinei HUMINT în NATO.

Nivelul următor în domeniul documentelor de standardizare HUMINT îl reprezintă Doctrina NATO HUMINT (AJP-2.3). Prima revizuire a standardului a fost încheiată cu succes la 6 iunie 2013, când acesta a fost promulgat de către directorul Agenției NATO pentru standardizare. La data redactării acestui material, 21 națiuni au ratificat și urmează să implementeze doctrina la nivel național, printre care și România.

În completarea doctrinei vine o clasă de documente suplimentare, menite să prezinte elementele structurale ale HUMINT și funcțiunile acestora, tehnicile, tacticile, procedurile de lucru la nivel de stat major și activitățile corespondente ciclului informațional, integrarea tehnologiilor de sprijin ale procesului de culegere, procesare și diseminare a informației, etc.

AintP-5 (*Doctrina pentru proceduri HUMINT în NATO*), standard aflat în proces de revizuire și care va fi publicat sub noua denumire ”*Tehnici, tactici și proceduri HUMINT în NATO*”, este documentul care abordează în mod detaliat modalitatea de punere în practică a principiilor teoretice ale disciplinei.

Custodia ambelor documente aparține HCOE, fiind preluată de la Marea Britanie în cursul anului 2012.

Un alt plan de reglementare a activității HUMINT în NATO este reprezentat de Directiva SHAPE¹ pentru HUMINT, document ce trasează liniile directoare, în baza fundamentului doctrinar, a modului în care structurile de comandă operaționale ale NATO transpun în practică cerințele specifice ale acestei discipline.

În cadrul fundamentării capacității HUMINT în NATO, aspectele teoretice sunt completate de conturarea cerințelor privind **dotarea materială și cu tehnologie**.

Dotarea materială este abordată în cadrul proiectului HCOE privind suportul tehnic și tehnologic necesar desfășurării activității de către operatorii și structurile de stat major HUMINT, în vederea culegerii, prelucrării și diseminării de informații², menit să asigure interoperabilitatea și să elimine decalajele calitative prin asigurarea unei referințe clare în materie de cerințe funcționale.

Pe lângă facilitățile de dezvoltare tehnologică oferite de Organizația NATO pentru Știință și Tehnologie (NSTO) și Agenția NATO pentru Comunicații și Informatică (NCIA), este notabilă, la acest capitol, existența unui sector solid de cercetare și producție industrială în domeniul securității, capabil să satisfacă cerințele operaționale ale disciplinei (conform politicilor și în baza programelor naționale privind dotarea cu tehnică și tehnologii de apărare).

Din punct de vedere **organizațional**, elementele de structură ale arhitecturii HUMINT în NATO sunt descrise în documentele de standardizare corespunzătoare; cu toate acestea, anumite aspecte lasă loc dezbaterilor – și așa menționa aici modul în care structurile HUMINT

¹ Supreme Headquarters Allied Powers Europe – statul major al Comandamentului Aliat pentru Operații

²Proiectul ”*NATO HUMINT Operator Toolset*”, promovat de către HCOE în cadrul procesului NATO de dezvoltare conceptuală

sunt reprezentate în teatrele de operații (raportat la prevederile doctrinare), absența unor elemente HUMINT în măsură să acționeze la nivel strategic-operațional pentru situațiile de criză, în sprijinul proceselor de identificare a indicatorilor și avertizării, precum și asigurarea contribuției în primele faze ale procesului decizional și al planificării (estimările specifice și pregătirea informațională a mediului operațional întrunit), precum și o delimitare mai clară a modului de armonizare a activităților HUMINT cu cele ale altor discipline cuprinse sub umbrela aceluiași element de stat major.

Practica prevederilor doctrinare va determina schimbările necesare eficientizării acțiunii acestora (atât structural – organigrama, cât și funcțional – fișa postului), corelate cadrului larg al capacității Intelligence.

Din acest punct de vedere, un rol deosebit de important îl are **procesul de educație și instruire** în conformitate cu standardele NATO, care vine să completeze capacitățile naționale de pregătire (acolo unde acestea există) și să armonizeze particularitățile de interpretare naționale prin furnizarea de cursuri, seminarii și exerciții menite să asigure un nivel corespunzător al cunoștințelor teoretice și abilităților practice pentru forțele dislocabile în operațiile NATO.

HCOE reprezintă un punct de reper solid ca furnizor de educație și instruire pentru disciplina HUMINT în NATO; aplicația pentru statutul de *șef de departament* pentru această disciplină va întări relevanța instituției prin noile atribuții legate de formularea cerințelor de instruire, autoritatea curriculară și controlul calității, aliniind standardele de pregătire ale NATO la cerințele exprimate în cadrul procesului Bologna. Aspectelor legate de pregătirea individuală li se adaugă cele de instruire colectivă¹, unde sunt antrenate și **calitățile de conducere (leadership)** la nivel tactic, precum și relațiile de colaborare cu Școala NATO de la Oberammergau (Germania)².

La nivel de **personal**, principala cerință în NATO este legată de calitatea și nivelul de calificare a cadrelor (personalului din formațiunile) puse la dispoziția Alianței de către națiuni. Cerințele în acest sens sunt formulate, în mod descriptiv, în fișa postului asociată unei anumite poziții și prin cerințele operaționale specifice.

În ce privește disciplina HUMINT, trăsăturile de personalitate/ aspectele calitative pe care trebuie să le întrunească personalul aferent sunt abordate în doctrina și procedurile NATO – iar acestea trebuie cumulate calităților unui militar combatant. Se urmărește ca acestea să fie dezvoltate în sensul includerii unor modele de fișă a postului la toate nivelurile ierarhice din cadrul organigramei HUMINT, astfel încât să faciliteze procesul de formulare a cerințelor de instruire în disciplină, în baza sarcinilor identificate. Această direcție de acțiune este corelată cu dezvoltarea STANAG 2555 – *Instruirea în domeniul Intelligence în NATO*, precum și cu abordările Grupului de lucru NATO pentru instruirea în domeniul Intelligence.

HCOE, prin serviciile de educație și instruire oferite în cadrul NATO, se constituie într-un facilitator de excepție în ce privește creșterea calității profesionale a personalului provenit din forțele armate ale națiunilor fără tradiție în domeniu și promotor al interoperabilității prin promovarea numitorului comun al specialității pentru toți militarii NATO – doctrina și procedurile NATO HUMINT. Dincolo de fundamentarea teoretică a aspectelor strict legate de tehnica activității specifice, realitatea operațiilor NATO din ultimii ani a demonstrat necesitatea dezvoltării capacității epistemologice (Kis, 2012) a personalului militar la toate nivelurile – iar disciplina HUMINT este una dintre cele mai expuse în ce privește nevoia de deschidere către o multitudine de cunoștințe legate atât de actorii operației militare întrunite, cât și cei ai mediului operațional – aspecte socio-culturale, istorice, religioase, politice, economice, etc (Simion, 2013 a).

¹HCOE este gazda anuală a exercițiului NATO HUMINT "Steadfast Indicator"

²HCOE asigură experți pentru modulele HUMINT din cadrul unor cursuri de specialitate Intel ale Școlii NATO

Din punct de vedere al **infrastructurii** necesare dezvoltării capabilității HUMINT în NATO, putem identifica la nivelul Alianței cadrul unic oferit de HCOE, singura instituție care pune la dispoziția NATO (și a națiunilor aliate) facilitățile de educație și instruire de care dispune. Din acest punct de vedere, avantajul funcționării unui centru de excelență dedicat disciplinei, care vine să completeze facilitățile naționale, este evident, dacă se impune să facem o comparație cu cadrul de dezvoltare a altor capabilități în NATO (Simion, 2013 b).

Toate aceste aspecte determină cadrul **interoperabilității** elementelor naționale HUMINT în arhitectura disciplinei în NATO; acesta este în permanentă transformare, urmând criteriile de eficiență funcțională și răspunzând nevoilor de îmbunătățire a tuturor aspectelor definitorii.

O scurtă analiză SWOT¹ în ce privește dezvoltarea capabilității HUMINT în NATO

Punctul forte al dezvoltării disciplinei HUMINT în NATO îl reprezintă acțiunea conjugată dintre Grupul de lucru NATO HUMINT (NHWG), Grupul de lucru NATO pentru tehnologie HUMINT (NHTWG) și HCOE – garantată la nivelul Politicii HUMINT în NATO prin asigurarea unității de coordonare – fapt ce facilitează, în strânsă relație cu responsabilii din cadrul ACO și ACT, promovarea unei viziuni unitare, coerența în abordare și accesul la resursele necesare transpunerii în practică a proiectelor aferente.

Noii termeni de referință ai NHWG se vor concentra asupra proiecției arhitecturii HUMINT în NATO pe termen scurt, mediu și lung, urmărind îmbunătățirea structurilor și sporirea relevanței produselor și serviciilor specifice la nivel strategic și operațional. În plus, abordările de tip analitic, studiile profesionale, produsele rezultate din procesarea lecțiilor învățate și a bunelor practici, noile concepte operaționale inițiate în cadrul disciplinei, sunt de natură să asigure un proces susținut de transformare a disciplinei și la nivel operativ-tactic.

Elementele cheie în domeniul acțional în ce privește criteriile de interoperabilitate le constituie pârgھیile din domeniul standardizării – prin custodia doctrinei și a procedurilor HUMINT în NATO (incluzând capacitățile de dezvoltare doctrinară, racordate atât la progresul în domeniul conceptual, cât și la realitățile teatrelor de operații) și cele de diseminare/ implementare, asigurate prin procesul de educație și instruire.

În plină reformă structurală și funcțională, sistemul de educație și instruire în NATO oferă HCOE oportunitatea de excepție de a-și dezvolta competențele și demonstra abilitățile de furnizor de astfel de servicii. Prin asumarea responsabilității de șef de departament pentru procesul de educație și instruire în domeniul HUMINT în NATO, relevanța HCOE se va extinde în materie de autoritate curriculară și în ce privește controlul calității pregătirii personalului HUMINT.

Opțiunea logică pentru instruire personalului națiunilor aliate care nu dețin facilități proprii de instruire în domeniul HUMINT, la nivel de bază, rămâne un centru NATO – în acest caz, HCOE. Bineînțeles, până nu demult, această nevoie era asigurată prin aranjamente bilaterale sau prin trimiterea de cadre la cursuri de specializare în diferite țări; ambele opțiuni prezintă limitări la capitolul avantaje (inclusiv cel economic), reprezentate de coerența dezvoltării capabilității HUMINT proprii și nevoia de interoperabilitate în conformitate cu standardele NATO (școlile cu tradiție, cu o valoare recunoscută, renunță mai greu la reperatele curriculare care le-au consacrat, la ”brandul” pe care și l-au construit, în favoarea îmbrățișării unor noi principii de instruire).

Serviciile de educație și instruire pe care le oferă HCOE se bazează pe cererile de instruire formulate la nivelul NATO, fiind studiate diferite opțiuni de design, modulare, simulare și sprijin material și cu infrastructura necesară unor procese educaționale moderne.

¹Strengths, Weaknesses, Opportunities, Threats/ Puncte tari, puncte slabe, oportunități, amenințări

Legată de procesul de educație și instruire, identificăm o problemă care privește atât încheierea ciclului de pregătire, cât și atestarea în materie de personal în NATO – evaluarea acestuia, în absența unei referințe Aliate în ce privește criteriile de certificare pentru diferite tipuri de activități din spectrul HUMINT. Chiar dacă rămâne o responsabilitate națională, standardizarea acestui aspect în NATO (aliniat cerințelor funcționale) ar fi de natură să contribuie la comunalitatea criteriilor de competență utilizate, facilitând crearea unui corp de cadre calificat, la dispoziția Alianței.

Domeniul tehnologic înregistrează, la rândul său, decalaje în ce privește dotarea națiunilor cu tehnică și tehnologie specifică. Eforturile HCOE, ale NHTWG și coordonarea SHAPE cu NCIA sunt de natură ca, prin promovarea unor produse standardizate NATO în acest domeniu, să contribuie la asigurarea unității de efort în ce privește dotarea structurilor HUMINT și implementarea unor programe unitare destinate managementului activității și gestionării informației (schimbul de informații, fluxul de rapoarte). Totodată, la nivelul HCOE, se studiază oportunitățile de pregătire a unor module de instruire în domeniul tehnologiilor HUMINT, într-o abordare flexibilă, ajustată nevoilor specifice.

Asupra misiunii, obiectivelor, produselor și serviciilor HCOE – relevante pentru reliefaarea reperelor de suport în procesul de dezvoltare a capacității HUMINT în NATO, vom reveni, pe larg, în următorul capitol.

Încheiem această parte subliniind necesitatea ca disciplina HUMINT în NATO să continue procesul de dezvoltare, asumându-și noi valențe – relevanța la nivel strategic, în procesul de evaluare a situației de securitate, identificarea de indicatori și avertizări, sprijinirea luptei împotriva terorismului, pătrunderea în spațiul cibernetic, etc. Perspectiva unei capacități HUMINT care să își piardă expresia operațională odată cu finalizarea operațiilor NATO nu trebuie să devină o provocare la adresa „supraviețuirii” acestei discipline de culegere a informațiilor, ci dimpotrivă, un imbold pentru fructificarea oportunităților de îmbunătățire a tuturor aspectelor care o definesc.

Relevanța aspectelor umane ale mediului operațional pentru HUMINT

Însăși definiția HUMINT ca și *“capacitate de culegere, procesare și diseminare a informațiilor din surse umane”* relevă nu doar conexiunea dintre structurile HUMINT și dimensiunea umană a mediului operațional, ci, mai mult, necesitatea imperioasă pentru o foarte bună înțelegere a mediului de acțiune – populația din zona de operații – ca premisă fundamentală pentru îndeplinirea cu succes a misiunilor specifice.

Astfel, o reflectare mai accentuată a aspectelor umane ale mediului operațional în procesul de pregătire al structurilor HUMINT constând în aprofundarea înțelegerii impactului pe care factorii psihologici, culturali și sociali în relație cu contextul istoric, politic, instituțional, economic, militar și legal generate de o situație de criză îl au asupra desfășurării operațiilor militare ar avea ca o primă consecință îmbunătățirea nivelului de competență interculturală al operatorilor – interfața structurilor de informații militare cu populația locală. Acest aspect s-ar concretiza în perfecționarea capacității de comunicare și relaționare a operatorilor cu grupurile țintă, conferindu-le astfel abilități sporite de dezvoltare a raporturilor interpersonale.

O altă îmbunătățire generată de o mai bună cunoaștere a aspectelor umane s-ar manifesta în domeniul pregătirii premergătoare dislocării în teatrul de operații printr-o înțelegere aprofundată a particularităților specifice zonei respective de operații, mai ales în ceea ce privește caracteristicile populației locale. În legătură cu această aspect trebuie menționat faptul că una dintre concluziile pregnante rezultate din participarea personalului HCOE la activitățile de instruire a forțelor NATO organizate de Centrul de instrucție a

forțelor întrunite¹ de la *Bydgoszcz*, Polonia, o reprezintă observația cvasi-generală a participanților de diferite naționalități că nivelul de familiarizare culturală asigurat prin diferite forme de instruire – naționale și/sau multinaționale – este insuficient în raport cu cerințele impuse de realitatea din teatrele de operații. Ameliorarea calitativă și cantitativă a pregătirii pe această linie contribuie semnificativ la familiarizarea corespunzătoare a personalului cu zona în care urmează să acționeze; consecințele directe ale acestui fapt concretizându-se atât în diminuarea efectelor șocului cultural cât și în reducerea perioadei de adaptare la specificul zonei de operații și creșterea eficienței acționale.

Din perspectivă acțională valorificarea cunoașterii aspectelor umane ale mediului operațional se poate concretiza prin creșterea nivelului de înțelegere a cererilor de informații pe această linie – a căror pondere este estimat a se amplifica direct proporțional cu importanța tot mai crescută pe care comandamentele strategice și operaționale o acordă înțelegerii comprehensive a mediului operațional – de către structurile HUMINT în vederea planificării, organizării, pregătirii și executării misiunilor specifice de culegere, precum și a analizei acestei categorii de informații.

Analiza operațiilor recente desfășurate de Alianța Nord-Atlantică corelată cu caracteristicile mediului de securitate actuală relevă nivelul tot mai ridicat de integrare a domeniului militar cu alte domenii (social, politic, economic, științific, cultural) și implicit necesitatea dezvoltării capacității epistemologice a sistemului militar pentru a putea genera capacități adecvate complexității unui mediu operațional comprehensiv specific operațiilor multinaționale întrunite actuale.

Concluzii

Dezvoltarea capacității de culegere, procesare și diseminare a informațiilor din surse umane (HUMINT) în NATO cunoaște o dezvoltare fără precedent, în toate aspectele ce definesc reperele cuantificabile ale arhitecturii disciplinei – doctrina, organizarea, educația și instruirea, baza materială, leadershipul, personalul, infrastructura și interoperabilitatea.

Procesul de transformare și adaptare a capacității HUMINT nu este unul ușor; determinarea obiectivelor pe termen scurt, mediu și lung, a liniilor directe, asigurarea resurselor necesare facilitării activităților subsecvente procesului, armonizarea intereselor și limitărilor națiunilor, deschiderea către diferite forme de parteneriat, evoluția tehnologică, deficiențele operaționale și funcționale semnalate – sunt numai câteva dintre provocările ce necesită o abordare pragmatică și totodată diplomatică în vederea găsirii de soluții rezonabile și viabile, care să fie apoi transpuse în practică la nivelul Alianței.

Capabilitatea HUMINT în NATO reprezintă un model de implicare a națiunilor într-un efort comun de dezvoltare și transformare a unei discipline de culegere a informațiilor care și-a dovedit particularitatea și necesitatea în condițiile specifice oferite de mediul actual de securitate.

Pașii importanți făcuți până la acest moment reprezintă doar un preambul ce obligă la păstrarea determinării, la abordarea pragmatică a provocărilor cu care se confruntă comunitatea de interes HUMINT în NATO, găsirea numitorului comun a intereselor naționale în acest domeniu și alinierea lor la cerințele NATO.

Interoperabilitatea în domeniul HUMINT în NATO rămâne o temă de actualitate, în toate dimensiunile sale. Deschiderea către diferitele formule de parteneriat pe care o putem anticipa pe termen mediu și lung trebuie să ne găsească pregătiți din toate punctele de vedere – o bază doctrinară solidă, structuri organizaționale suplă, eficiente, beneficiind de un management al informației performant, sprijinite cu mijloace tehnologice adecvate. Personalul

¹ NATO Joint Force Training Center (JFTC)

HUMINT trebuie să beneficieze de formule de educare și instruire aliniate standardelor NATO, evaluat conform criteriilor de performanță ale NATO și răspunzând cerințelor specifice fișei postului.

Numai o abordare complexă a tuturor aspectelor legate de managementul capacității, o viziune clară privind transformarea acesteia și asigurarea unității de acțiune a națiunilor sunt hotărâtoare în acest sens.

Bibliografie

1. ACKERMAN, Robert K. (2006) *Defense HUMINT Needs Technology, Too*, în <http://www.afcea.org/content/?q=node/1202>
2. BEALL, David (2009) The HUMINT Heresies: The Disposition of Human Intelligence Collection in Counterinsurgency, in *Military Intelligence*, PB 34-09-2 Volume 35 Number 2 April – June, 2009, https://www.fas.org/irp/agency/army/mipb/2009_02.pdf
3. BREMSETH, L. R. (2001) *Unconventional Human Intelligence Support: Transcendent and Asymmetric Warfare Implications of Remote Viewing*, Marine Corps University, Marine Corps Combat Development Command, Quantico, VA, în <http://www.lfr.org/lfr/csl/library/Bremseth.pdf>
4. FLYNN, Michael T., POTTINGER, Matt, BATCHELOR, Paul D. (2010) *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan*, Center for a New American Security, în http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf
5. FM 2-22.3 (FM 34-52) Human Intelligence Collector Operations (2006) în <http://www.fas.org/irp/doddir/army/fm2-22-3.pdf>
6. http://www.nato.int/cps/en/natolive/official_texts_87593.htm?mode=pressrelease
7. <http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf>
8. JOHNSON, William J. (Editor-in-Chief), ROBERTS, Wayne (Co-editor), DiMEGLIO, Richard P., BISHOP, Owen B., CHERRY, John R., GILLMAN, Andrew D., LINDQUIST, Todd L., LEE, David H., STIGALL, Dan E., WILLIAMS, Winston S. (2013) *Law of Armed Conflict Deskbook*, International and Operational Law Department the Judge Advocate General's Legal Center and School, U.S. Army Charlottesville, Virginia, în http://www.loc.gov/frd/Military_Law/pdf/LOAC-Deskbook-2013.pdf
9. KIS, Alexandru (2012) *Human Security and the Human Aspects of the Operational Environment – A Systems View*, pp. 221-235, in Teodor FRUNZETI, Marinela-Adi MUSTAȚĂ, *Science in the Mirror – Towards a New Method of Paradigm Comparison*, Éditions du Tricorne, Geneva, Switzerland, 2012
10. MARGOLIS, Gabriel (2013) *The Lack of HUMINT: A Recurring Intelligence Problem*, in *Global Security Studies, Spring 2013, Volume 4, Issue 2*, University of North Carolina Wilmington
11. NATO Standardization Agency, *NATO Glossary of Terms and Definitions (English and French) AAP-6*, (2013), <http://nsa.nato.int/nsa/zPublic/ap/aap6/AAP-6.pdf>
12. Oxford Advanced Learner's Dictionary, 8th edition, Oxford University Press, 2010
13. POU CET, Emmanuel (2006) *Le renseignement de source humaine, espoirs et problèmes*, în revista "Doctrine" N° 09
14. SIMION, Eduard (coordinator) (2013a) *The Human Aspects of the Operational Environment*, NATO HUMINT Centre of Excellence, CNI Coresi SA, Oradea
15. SIMION, Eduard (2013b) *Centrele de Excelență NATO și transformarea Alianței Nord-Atlantice*, Editura Universității din Oradea
16. SIRAK, Michael C. (2013) *AGS: A 'Game Changer' for NATO Intelligence and Interoperability*, Air Force Magazine, September 16
17. STEELE, Robert D. (2010) *Human Intelligence: all humans, all minds, all the time*, Advancing Strategic Thought Series, <http://www.StrategicStudiesInstitute.army.mil/>

CAPITOLUL 5. OSINT ÎN ACTIVITATEA DE INTELLIGENCE

Intelligence în lumea globalizată: surse secrete vs. surse deschise

Odată cu explozia multilaterală a fluxurilor informaționale facilitate de deschiderile specifice procesului de globalizare, sursele publice de informare, accesibile publicului larg, au captat deopotrivă interesul comunităților de Intelligence, devenind în foarte scurt timp bazinul de culegere de date și informații esențiale pentru completarea și îmbogățirea cunoașterii dobândite prin metodele clasice (surse secrete umane – a se vedea capitolul dedicat HUMINT, sau surse secrete tehnice – SIGINT, MASINT, ACINT, etc.), contribuind decisiv la formularea avertizărilor situaționale și prospectarea evoluției tuturor tipurilor de amenințări.

Funcția analitică a OSINT (Intelligence din surse deschise/ Open Source Intelligence) este interpretabilă pe două paliere de referință: pe de o parte, susținerea documentării necesare componentei operaționale (Intelligence de bază), pe de altă parte dezvoltarea analizelor strategice referitoare la tendințele de evoluție a unor riscuri sau amenințări pe termen mediu și lung la adresa intereselor și valorilor fundamentale ale statului și societății.

Produsele de Intelligence provenite din date și informații din surse deschise sunt folosite la toate nivelurile de referință (în mediul militar, de la palierul strategic până la cel tactic) din multiple rațiuni:

- ca punct de plecare al unei informări, când aduc un plus de valoare unei problematice de interes;
- pentru a oferi o perspectivă istorică asupra cadrului general al unei informații (incluzând contextul politic, socio-economic, tehnic, geografic, etc.);
- pentru a proteja/ acoperi sursele secrete;
- pentru a completa și a întregi unele date/informații;
- pentru a valida informații din alte surse;
- pentru a adăuga criterii de ierarhizare a cunoașterii;
- pentru cercetarea unui context;
- pentru dezvoltarea de politici și planificarea acțiunilor în diferite medii;
- pentru fundamentarea investițiilor în echipamente, etc. (Steele, 1997)

Avantajele utilizării OSINT rezidă din faptul că datele și informațiile din surse deschise pot fi accesate ușor și au un cost relativ redus în comparație cu cel necesar pentru obținerea de informații din surse secrete sau private. De asemenea, OSINT asigură o acoperire greu de egalat asupra unei game largi de subiecte de interes, într-un cadru care nu necesită aplicarea unor măsuri de securitate atât de stricte precum în cazul surselor secrete, fiind extrem de utile atunci când trebuie să fie realizate documente menite a fi diseminate în medii din afara cadrului securizat (parteneri, conferințe, întâlniri internaționale, organizații globale sau mass-media). Tot în acest cadru, prin trimiterea la informațiile din surse deschise, acestea pot fi folosite pentru a proteja surse secrete și a nu desconfira tehnici și proceduri de obținere a informației de către serviciile specializate.

Accesul facil la date și informații din surse deschise în cadrul procesului OSINT este pus în balanță de cantitatea imensă a acestora, stabilirea nivelului de încredere a sursei de proveniență și credibilitatea sa (de unde și valoarea informativă), precum și de aspecte reclamate de procesarea efectivă a datelor și informațiilor, raportat la formă, indexarea lor, volatilitatea surselor on-line sau limba de publicare. Pentru a descrie caracteristicile masei de date și informații disponibile la nivel global este popular termenul de "big data" – definit printr-o serie de parametri relevanți¹:

¹ http://www.sas.com/en_us/insights/big-data/what-is-big-data.html

- volumul imens de date și informații acumulat istoric, în creștere exponențială, atât în mod structurat cât și nestructurat (cu efect direct asupra abilității de căutare și detectare a datelor și informațiilor relevante);
- viteza de propagare fără precedent, care solicită reacția instituțională adecvată;
- multitudinea de formate, combinații, varietăți ce antrenează dificultăți în prelucrarea datelor și informațiilor;
- variabilitatea, constând în fluctuații în timp și spațiu ale fluxurilor informaționale;
- complexitatea datelor și informațiilor raportat la sursă, conexiuni, relaționări, ierarhii, etc.

OSINT – delimitări terminologice

NATO definește clasa de Intelligence din surse deschise (OSINT) ca fiind Intelligence derivat din informațiile disponibile în mod public sau cu distribuție/ acces public limitat, însă fără a fi clasificate (AAP-6)¹. Directorul pentru Intelligence Național și Departamentul pentru Apărare al SUA completează această definiție prin specificarea atributului oportunității (încadrarea într-un orizont de timp pentru diseminare), precum și caracterul direcționat al OSINT (trebuie să răspundă cerințelor de informații specifice formulate de beneficiar), ambele aspecte fiind definitorii pentru orice disciplină de culegere a informațiilor².

În aceeași idee, ATP-2-22.9 – publicația tehnică privind OSINT în cadrul armatei SUA, preia definiția acestei discipline de Intelligence din FM-2.0, raportată la produsele de Intelligence rezultate din informații public disponibile, colectate, exploatare și diseminate în timp oportun audienței adecvate, în scopul adresării unor cerințe specifice de Intelligence sau a unor cerințe de informare.

Schauerer și Störger observă necesitatea accesării în mod legal a informației public accesibile (Schauerer și Störger, 2013); astfel, produsele de Intelligence derivate din surse sau folosind mijloace accesibile în mod public, însă în mod ilegal – a se vedea Wikileaks, în cazul căruia legalitatea exploatării scurgerilor de informații clasificate este puternic dezbătută – nu pot fi considerate OSINT.

Culegerea de date și informații din surse umane în mediul virtual (on-line) în mod pasiv (adică ce este postat, disponibil) diferențează OSINT de ceea ce putem numi ”cyber”-HUMINT, adică o prezență activă a operatorilor HUMINT în cadrul rețelelor de socializare pe Internet cu scopul de a elicită indivizi cu potențial informativ în vederea obținerii de date și informații exploatabile.

De asemenea, OSINT diferă de simpla documentare din surse publice prin faptul că i se aplică procesul de prelucrare a informației (etapele ciclului Intelligence) pentru a crea produse informative (Intelligence) care să răspundă direcționării/ cerințelor formulate de către utilizatorii finali. Parte a acestui ciclu, procesul tehnic de colectare, procesare și diseminare a produselor obținute din datele și informațiile din surse deschise cuprinde o serie de funcționalități automatizate sau nu, aflate în continuă dezvoltare (figura 5.1).

¹ în 2001, OSINT era considerat în NATO – conform NATO Open Source Intelligence Handbook – informație neclasificată descoperită în mod deliberat, selectată, filtrată și diseminată unei audiențe desemnate cu scopul de a răspunde unei întrebări specifice

² după definiția din secțiunea 931 a Public Law 109-163, *National Defense Authorization Act for Fiscal Year 2006*, în <http://www.gpo.gov/fdsys/pkg/PLAW-109publ163/html/PLAW-109publ163.htm>

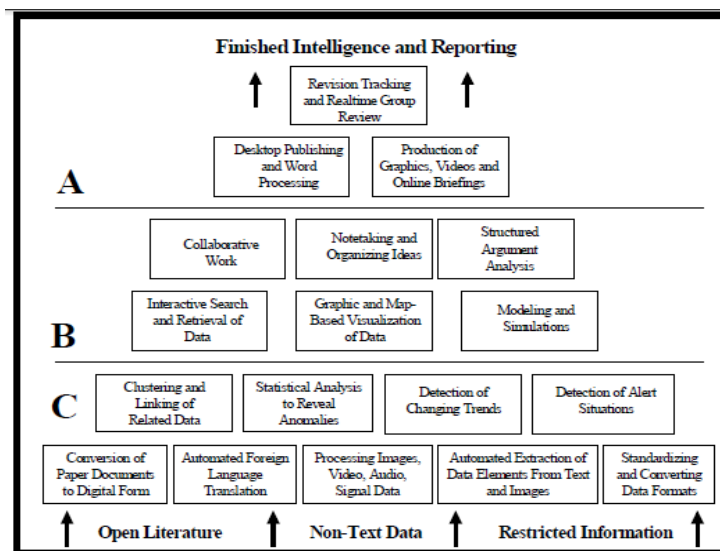


Figura 5.1 Elemente de software în ciclul OSINT (NATO Open Source Intelligence Handbook, 2001, fig. 6)

Odată exprimate cerințele de informare ale factorilor decizionali, procesul de planificare și pregătire a exploatării datelor și informațiilor din surse deschise trebuie să țină cont de o serie de aspecte fundamentale (ATP-2-22.9, 2012,2-7):

- determinarea gradului de încredere a surselor deschise;
- determinarea credibilității conținutului informației;
- complianța informațiilor obținute cu scopul urmărit;
- securitatea operațiilor;
- nivelul de clasificare a produsului final OSINT raportat la cerințele de diseminare;
- coordonarea – în special la nivel operativ/tactic, sincronizarea cu ritmul operațional;
- dezinformarea sau înșelarea;
- proprietatea intelectuală și drepturile de copyright;
- cerințe lingvistice;
- existența sistemelor automatizate de prelucrare a datelor (traducere, sortare, indexare, colare, etc.).

Clasificarea surselor deschise

Informațiile din surse deschise reprezintă pachete de date disponibile public pentru informarea în masă, prezentate sub formă scrisă, electronică sau orală. În general, acestea nu fac obiectul unor limite privind dreptul de proprietate (excepție cele protejate de drepturi de copyright), nu sunt clasificate și sunt obținute pe căi legale. Din punct de vedere al modalităților de procurare, unele sunt gratuite, iar altele sunt supuse unor taxe de abonament etc.

După Open Knowledge Foundation, platformele de transfer a datelor și informațiilor trebuie să întrunească cel puțin trei condiții pentru a se încadra în cerințele definitorii pentru surse deschise, cu privire la: disponibilitatea și accesarea datelor și informațiilor, posibilitatea de re folosire și redistribuire a acestora, precum și participarea neîngrădită la aceste resurse¹ - din acest punct de vedere fiind discutabilă taxarea accesului, interdicția de reproducere în virtutea drepturilor de autor, etc.

¹ Open Knowledge Foundation (2014) *Open Data Handbook Documentation*, Release 1.0.0

Legat de înțelegerea corectă și coerentă a ce reprezintă disciplina OSINT, trebuie făcută distincția între noțiunea de ”informații din surse deschise” și ”Intelligence din surse deschise”. Folosirea sintagmei ”**open source**” înțelege ca ”**surse (de informare) deschise (accesibile publicului)**” poate crea o serie de confuzii prin asocierea cu expresia ”**open source**” consacrată în comunitatea informaticienilor, unde se traduce prin programe a căror cod-sursă este public disponibil și modificabil¹. De aceea, recomandăm folosirea termenului de ”**informații din surse deschise**” – ”**open source information – OSINF**”, care stau la baza producerii OSINT.

NATO Open Source Intelligence Handbook (2001) distinge patru categorii noționale asociate capabilității OSINT:

1. **Date din surse deschise** (Open Source Data – OSD), primare (neprelucrate), provenite din surse primare (fotografii, înregistrări, imagini satelitare, scrisori particulare);
2. **Informații din surse deschise** (Open Source Information – OSI), provenite din prelucrarea inițială a datelor (cuprinse în ziare, cărți, transmisii audio-video);
3. **Intelligence din surse deschise** (Open Source Intelligence – OSINT), rezultată în urma unui proces deliberat de descoperire, selecție, analiză și diseminare către beneficiar (răspunzând unor cerințe prioritare de Intelligence);
4. **OSINT validat** (OSINT-V) reprezintă un produs informativ cu grad înalt de credibilitate, de regulă confirmat de informații provenite din surse secrete.

Vorbind strict despre OSINT, atât datele cât și informațiile din surse deschise (OSD și OSI) sunt asimilabile ca ”materie primă” pentru procesul de producție a produsului final, care intră în procesul de analiză integrată a produselor similare provenite din toate sursele disponibile (”all-source analysis”) pentru elaborarea de Intelligence în sprijinul factorilor decizionali.

La nivelul etapei de colectare, putem face referință la date și informații din surse deschise provenite din:

- a. media (ziare, radio, televiziune, etc.);
- b. date profesionale sau academice (lucrări științifice, expuneri în conferințe și seminarii, produse ale asociațiilor profesionale, literatura gri);
- c. datele publice (rapoarte guvernamentale, date demografice, audieri, discursuri, dezbateri legislative, conferințe de presă, avertizări, contracte, etc.)²;
- d. date provenite din comunitățile virtuale și rețelele de socializare (ex. Facebook, Twitter, etc.)³, websiteuri de distribuție de materiale video (ex. Youtube), bloguri, etc.;
- e. observare și raportare a unor evenimente și date (de către amatori în diferite domenii, monitori radio, relatări ale observatorilor, opiniile unor experți, etc.);
- f. platforme on-line furnizând date geospațiale și de imagerie (ex. Google Earth) sau alte date cu suport tehnic (din domenii diverse), ori produse de natură culturală, economică, socială ale unor instituții independente/ think-tank.

Participarea la forumuri publice a personalului implicat în culegerea de date și informații din surse deschise presupune respectarea *regulilor casei*; astfel, obiceiurile și legile locale trebuie cunoscute și respectate, un exemplu elocvent fiind reprezentat de regula cunoscută ca *Chatham House Rule* (care recunoaște participanților libertatea de a utiliza informațiile recepționate, însă fără a fi atributabile vre-unuia dintre vorbitori și fără a divulga

¹ <http://opensource.org/>

² <http://www.fbi.gov/about-us/intelligence/disciplines>

³ <http://www.sri.ro>

identitatea și afilierea participanților¹; invocarea acestei clauze marchează trecerea de la informația publică din sursă deschisă la date din surse confidențiale).

În funcție de suportul de difuzare, conținut și modul de diseminare, sursele deschise pot fi clasificate în două categorii:

C. clasice:

- *publicații periodice* (ziare și reviste), agenții de știri, cărți (de specialitate, de telefoane, „Pagini auri”, monitorul oficial, anuare), materiale documentare (broșuri și studii), hărți și fotografii;
- *literatura gri* – totalitatea materialelor care nu sunt disponibile prin intermediul canalelor tradiționale (mass-media) de publicare, distribuție sau control biografic. Sursele de literatură gri pot fi ONG-urile, instituțiile de învățământ și cercetare, companii comerciale, agenții guvernamentale, mediul academic², asociații formale și informale, cluburi etc. În această categorie se încadrează: documentare științifice și tehnice, rapoarte guvernamentale, bugete, statistici demografice, audieri, dezbateri legislative, conferințe de presă, discursuri, dar și informațiile din medii profesionale și academice: conferințe, simpozioane, documente elaborate de asociații profesionale, lucrări academice și ale experților din diverse domenii. Principalele dificultăți întâmpinate în exploatarea literaturii gri ține de faptul că este dificil de identificat și procurat (nefiind la îndemâna publicului larg); intrarea în posesia literaturii gri este posibilă numai pe timpul unor evenimente, despre care culegătorul trebuie să aibă cunoștință și la care să aibă acces; este greu de procesat deoarece de regulă este într-un format nestandard, de multe ori numai în format tipărit, redactate într-o multitudine de limbi, le lipsesc date de identificare a autorilor, data apariției etc.
- *transmișiile audio-video în eter* (radio și televiziune).

b. online: denumite generic *new-media* și reprezentând orice produs media digital care este interactiv și distribuit prin rețele informatice sau totalitatea textelor, sunetelor, imaginilor și elementelor grafice prelucrate pe computer și reunite în baze de date (enciclopedii electronice, bloguri, comunități virtuale, social networks, files-sharing, ediții electronice ale presei tradiționale, portaluri informaționale, lumi virtuale, forumuri, biblioteci digitale etc.).

Mijloacele de comunicare în masă (presa, televiziunea, radioul și publicitatea) reprezintă sursa cu caracter deschis preponderent. Tipologiile consacrate presei se fundamentează pe criterii, precum aria de difuzare, conținutul, periodicitate etc. Criteriile utilizate în clasificarea publicațiilor se aplică și în cazul audiovizualului.

Rolul Internetului și *new media* în obținerea OSINT

Din 1994, Internetul – o complexă rețea de rețele³ – a luat amploare în lume, având un impact uimitor asupra tuturor aspectelor vieții. Internetul și creșterea exponențială a numărului persoanelor cu acces la acesta aproape oriunde în lume, apariția forumurilor de discuții pe diferite subiecte, a rețelilor de socializare on-line – pe lângă oportunitățile de

¹ <http://www.chathamhouse.org/about/chatham-house-rule/>

² În mediul academic, literatura gri este reprezentată de lucrări publicate fără asumarea responsabilității de către un editor și circulată în afara circuitelor comerciale (ex. preprinturile, care conțin lucrări de cercetare, rapoarte tehnice etc., puse în circulație mai ales în spațiile academice, pentru a face cunoscute ultimele noutăți, ultimele gânduri, ultimele realizări, în beneficiul comunității științifice, sacrificând girul științific în favoarea rapidității informării (Stoica, 2011)

³ <http://www.internetsociety.org/internet>

dezvoltare a cunoașterii – oferă un potențial major pentru noi instrumente și tehnologii de culegere, analiză și diseminare a informației la nivel global.

Exploatarea Internetului în scopul colectării de informații se poate realiza utilizând mijloace precum motoarele de căutare (Google, Yahoo, Bing, etc.), cât și bloguri, forumuri, rețele de socializare, legăturile de tip „Peer to Peer”¹, programele de tip „Rich Site Summary (RSS) feeds”².

Deși nu există o definiție general acceptată a *new media*, aceste produse fiind percepute diferit de diversele categorii de utilizatori, ele sunt apreciate ca reprezentând orice produs media digital care este interactiv și distribuit prin rețele informatice sau totalitatea textelor, sunetelor, imaginilor și elementelor grafice prelucrate pe computer și reunite în baze de date. Dacă mijloacele media clasice cuprind transmiterea de emisiuni prin mijloace terestre (analogice), prin cablu sau satelit, materiale media pe suport fizic (CD, DVD, ziare, reviste, cărți), comunicații terestre și servicii poștale, tehnologiile *new media* se bazează pe rețele de calculatoare și transmisii mobile/ wireless (Internetul, websiteuri, jocuri video digitale) (figura 5.2).



Figura 5.2 Media clasică vs. *new media*³

O distincție aparte între cele două categorii este făcută de specialiștii Universității din Utah (SUA) raportat la relația media-consumator/beneficiar. Astfel, distingem mijloacele media clasice asociate acțiunii de *a pune la dispoziție* („împinge”) produsele specifice dinspre serviciile specializate către clienți fără o selecție prealabilă (PUSH), pe când canalele de distribuție *new media* furnizează servicii personalizate în funcție de relevanța manifestată la nivelul clientului – *media on demand* – selectate dintr-un larg volum de conținut-sursă, în forma preferată de aceștia (interactivitate – PULL)⁴. Astfel, *new media* acoperă accesul solicitat către un conținut informațional fără limitări (virtuale) de timp și spațiu, pe orice

¹ aceste legături permit celor ce le folosesc să își conecteze computerele prin intermediul internetului, oriunde în lume, cu scopul de a face schimb de fișiere; sunt deseori situații în care aceste rețele sunt folosite pentru activități în afara legii, ca evitarea plății drepturilor de autor pentru diferite produse – filme, muzică, etc., sau distribuirea de materiale pornografice interzise (<http://www.fbi.gov/scams-safety/peertopeer>)

² RSS este o familie de formate de fluxuri web, realizate în format XML și folosite pentru *Web syndication*. RSS este folosit (printre altele) pentru știri, bloguri și podcasting - distribuția fișierelor în format multimedia (de obicei fișiere audio dar și video).

³ http://www.media.utah.edu/MODwiki/index07de.html?title=University_of_Utah_Strategy_for_MOD&printable=yes

⁴ <http://www.media.utah.edu>

suport digital, permițând totodată conexiunea inversă (feedback) interactivă și participarea creativă a beneficiarului.

În acest context, *social media* reprezintă interacțiunea socială între oameni care, în cadrul unor comunități și rețele virtuale, crează, împărtășesc sau schimbă informații și idei (Ahlqvist și alții, 2008); aceasta cuprinde și suportul tehnologic bazat pe Web pentru crearea platformelor interactive. Un spectru al social media este reprezentat în figura 5.3, de unde putem enumera câteva exemple¹:

- **Social Bookmarking.** (Del.icio.us, Blinklist, Simpy) – facilitează interacțiunea prin etichetarea paginilor web și funcțiunea de căutare în seria paginilor web etichetate de alte persoane;
- **Social News.** (Digg, Propeller, Reddit) – facilitează interacțiunea prin votarea articolelor și comentarea lor;
- **Social Networking.** (Facebook, Hi5, Last.FM) – facilitează interacțiunea prin adăugarea de prieteni, comentarea profilelor acestora, adeziunea la grupuri și purtarea de discuții;
- **Social Photo and Video Sharing.** (YouTube, Flickr) – facilitează interacțiunea prin schimbul de fotografii și videoclipuri, precum și comentarea acestora;
- **Wikis.** (Wikipedia, Wikia) – facilitează interacțiunea prin prin adăugarea de articole și editarea celor existente.



Figura 5.3 Spectrul media de socializare²

Numărul imens de website-uri corporate/ personale, bloguri, forumuri publice, popularitatea fără precedent a rețelelor sociale (sute de milioane de conturi), dar și creșterea exponențială a conținutului generat de utilizatori și diversitatea limbilor și a pachetelor în care este livrată informația sunt principalele provocări pentru OSINT (Anexa 1 – Infografic privind evoluția rețelelor sociale).

¹ <http://webtrends.about.com/od/web20/a/social-media.htm>

² <http://primetime.co.ug/services/social-media/>

Din această perspectivă, aproape fiecare etapă a procesului OSINT (planificare, culegere, procesare, analiză, diseminare) reprezintă o reacție și o încercare de adaptare la dinamica mediului online, fiind direct influențate de noile tehnologii și de rapiditatea cu care sunt preluate și dezvoltate de utilizatori.

În același timp, accesul facil la informații ascunde o altă realitate: să fii informat nu este suficient. Este necesar ca informația să fie validată și prelucrată pentru a deveni un produs de intelligence, proces ce necesită tehnică, mijloace și timp.

Dificultățile întâmpinate în procesul de identificare și validare a surselor sunt generate de caracteristicile Internetului și facilitățile oferite de acest mediu, respectiv anonimatul relativ al utilizatorilor și transmiterea virală a unor informații ce pot fi relevante.

Validarea poate îmbrăca două forme: verificarea informației și validarea sursei. Verificarea credibilității informației vehiculate în mediul online trebuie să aibă în vedere¹:

- determinarea scopului probabil al paginii și a informației postate; existența suspiciunilor privind obiectivitatea (reclame ascunse, propagandă și activism, etc.);
- categoria de date și informații furnizate – *primare* sau *secundare*; existența dreptului de copyright sau a referințelor legate de informația furnizată (sursa primară – răspândirea informațiilor prin transmiterea/ preluarea concomitentă a acestora pe diverse rețele de bloguri, forumuri, site-uri de știri și platforme de socializare ridică problema descoperirii acesteia); credibilitatea linkurilor furnizate/ nivelul de reputație;
- gradul de complexitate și organizare a paginii; gradul de actualizare și mentenanță a websiteului (în vederea evitării paginilor ”zombi”, cu informații perimate);
- posibilitatea de verificare a informației furnizate din alte surse.

Totodată, în procesarea datelor și informațiilor din mediul on-line necesară filtrarea conținutului pentru a elimina informațiile care se repetă; permisivitatea acestui mediu în privința preluării conținutului, duce de multe ori la copierea și postarea informațiilor fără menționarea autorului, sau sub o formă modificată. În acest sens, se impune verificarea tuturor surselor de referință oferite, și compararea materialelor pentru a identifica asemănările/ diferențele care pot indica sursa/ autorul primar.

Evaluarea informației din punct de vedere a credibilității se raportează la un sistem de referință cu un grad ridicat de complexitate, distingând – în baza unor criterii specifice (ATP 2-22.9, 2-8,2012):

1. informații confirmate (confirmate de alte surse independente; logice în sine; în concordanță cu alte informații referitoare la subiect);
2. informații probabil adevărate (neconfirmate de alte surse; logice în sine; în concordanță cu alte informații referitoare la subiect);
3. informații posibil adevărate (neconfirmate de alte surse; logice în sine în mare măsură; în concordanță cu anumite informații referitoare la subiect);
4. informații îndoielnice (neconfirmate de alte surse; posibile, dar ilogice; fără alte informații referitoare la subiect disponibile);
5. informații improbabile (neconfirmate de alte surse; ilogice în sine; contrazise de alte informații referitoare la subiect);
6. dezinformare (neintenționat false; ilogice în sine; contrazise de alte informații referitoare la subiect; confirmate de alte surse independente);
7. înșelare (în mod deliberat false; contrazise de alte informații referitoare la subiect; confirmate de alte surse independente)
8. informații imposibil de evaluat (nu există bază de evaluare a validității informației).

¹ <http://www.mhhe.com/mayfieldpub/webtutor/judging.htm>

În ce privește evaluarea nivelului de încredere a sursei datelor și informațiilor din mediul virtual și validarea acestora, tot Internetul ne oferă și resursele instrumentale necesare. Un exemplu în acest sens – de exemplu pentru *bloguri*¹ – urmează pașii unui algoritm ce acoperă²:

- a. identificarea numelui celui care a înregistrat domeniul (în acest scop se poate folosi, de exemplu, aplicația **Whois Domaintools**³, unde se înscrie adresa sursei și se lansează căutarea – a se vedea figurile 5.4 și 5.5); exemplul folosit analizează comparativ blogul Comandantului Comandamentului Aliat pentru Operații (SACEUR – Supreme Allied Commander Europe), generalul Philip Breedlove, în raport cu blogul lui Aymenn Jawad Al-Tamimi, jurnalist, free-lancer, absolvent al Oxford University, partener prin Shillman-Ginsburg Fellow la Middle East Forum (figura 5.6);



Figura 5.4 Blogul SACEUR (<http://www.aco.nato.int/saceur2013/blog/>) vs blogul lui Aymenn Jawad Al-Tamimi (<http://www.aymennjawad.org/blog/>)



Figura 5.5 Pagina de căutare a aplicației WHOIS LOOKUP DOMAINTOOLS (<http://whois.domaintools.com/>)

whois.domaintools.com/nato.int		whois.domaintools.com/aymennjawad.org	
IP Address	152.152.31.120 is hosted on a dedicated server	— Whois & Quick Stats	
IP Location	Brussels Hoofdstedelijk Gewest - Brussels - Nato Headquarters	Email	aa1892@hotmail.com grayson@levy.org.il is associated with ~36 domains
ASN	AS198946 NATO-AS North Atlantic Treaty Organization, BE (registered Jun 28, 2012)	Dates	Created on 2010-08-13 - Expires on 2020-08-13 - Updated on 2012-10-15
Whois History	954 records have been archived since 2006-09-29	IP Address	207.58.137.242 - 36 other sites hosted on this server
Whois Server	whois.iana.org	IP Location	Texas - Mcallen - Servint
— Website		ASN	AS25847 SERVINT - Servint, US (registered May 17, 2002)
Website Title	NATO - Homepage	Domain Status	Registered And Active Website
Server Type	Apache	Whois History	35 records have been archived since 2010-08-14
Response Code	200	IP History	3 changes on 3 unique IP addresses over 4 years
SEO Score	85%	Hosting History	2 changes on 3 unique name servers over 4 years
Terms	3512 (Unique: 971, Linked: 1740)	Whois Server	whois.pir.org
Images	149 (Alt tags missing: 42)		
Links	343 (Internal: 309, Outbound: 34)		

Figura 5.6 Date privind identitatea blogurilor, obținute prin aplicația WHOIS LOOKUP DOMAINTOOLS pentru blogurile de referință

¹ Blogul este un jurnal deschis publicului, publicat on-line, care oferă informații, comentarii, opinii despre un subiect predilect, în format text, audio sau video. Spațiul online al blogurilor și al bloggerilor este cunoscut drept "blogosferă" (Tree Works) și antrenează un spectru extrem de larg de persoane din toate domeniile – politic, economic, cultural, științific, etc.

² <http://caddereputation.over-blog.com/article-35587388.html>

³ <http://whois.domaintools.com/>

- b. etapa a doua constă în vizualizarea gradului de cotare/ citare/ recunoaștere/ popularitate a blogului pe web (criteriu aplicabil oricărui site), în baza numărului de legături (linkuri) existente în relația cu alte surse și a traficului înregistrat (folosind, în acest sens, instrumente ca MOZ Open Site Explorer¹); dincolo de validarea credibilității în baza criteriilor menționate, acest demers poate să conducă și la identificarea sursei primare a datelor/ informației și compararea credibilității cu alte bloguri (figurile 5.7 – 5.9);



Figura 5.7 Pagina de căutare a aplicației MOZ Open Site Explorer (<http://moz.com/researchtools/ose>)

Figura 5.8 Evaluarea blogului SACEUR pe platforma MOZ Open Site Explorer²

	http://www.aco.nato.int/saceur2013/blog/who-are-the-men-behind-the-masks.aspx	www.aymennjawad.org/blog/
Page Authority:	✔ 52	18
Page MozRank:	✔ 3.56	2.75
Page MozTrust:	✔ 5.03	4.86
Internal Equity-Passing Links:	1	✔ 2
External Equity-Passing Links:	✔ 45	0
Total Internal Links:	1	✔ 2
Total External Links:	✔ 47	0
Total Links:	✔ 48	2

Figura 5.9 Captură a studiului comparativ între blogul SACEUR și blogul lui Aymenn Jawad Al-Tamimi, realizat pe platforma MOZ Open Site Explorer¹

¹ <http://moz.com/researchtools/ose>

² <http://moz.com/researchtools/ose/links?site=http%3A%2F%2Fwww.aco.nato.int%2Fsaceur2013%2Fblog%2Fwho-are-the-men-behind-the-masks.aspx>

- c. etapa a treia constă în verificarea înscrierii blogului într-o comunitate tematică, de practică profesională, etc., menită să asigure o atare recunoaștere a sursei (ca resurse instrumentale în acest scop pot fi folosite aplicații ca TouchGraph Navigator² - figura 5.10);

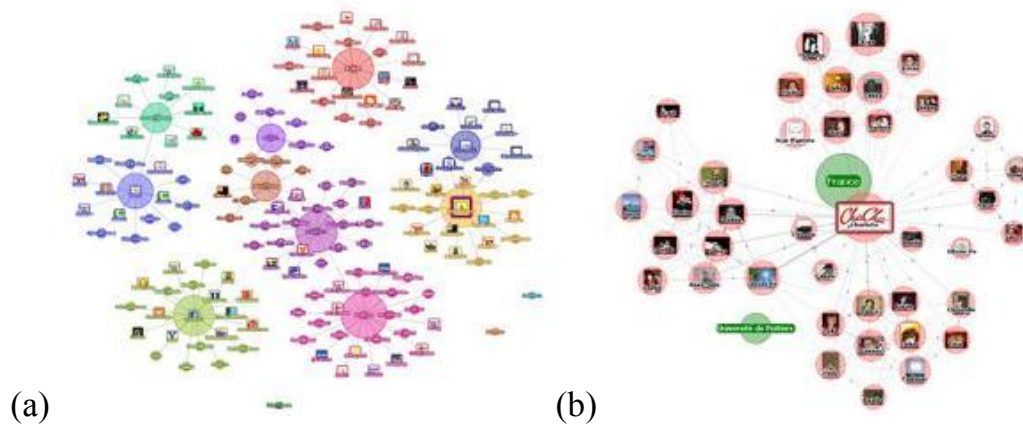


Figura 10 Reprezentări grafice realizate cu ajutorul TouchGraph Navigator: (a) cartografierea rețelei web în baza datelor obținute prin Google; (b) cartografierea rețelei web în baza datelor obținute prin Facebook³

- d. etapa următoare privește modalitatea practică de sondare a gradului de recunoaștere a unui blog în cadrul comunității sale (contabilizarea trimerilor/linkurilor către acesta, comentariile primite, interacțiunile din blogosferă – prezența autorului blogului pe alte platforme, difuzarea prin Twitter, numărul de abonați la fluxul RSS) și, implicit, a legitimității sale într-un domeniu de interes.

Parcursul acestor etape este relativ suficientă pentru determinarea nivelului de încredere a unei surse on-line, încadrând-o într-una din cele cinci clase în mod general considerate de către comunitățile de intelligence – sursă de încredere, de regulă de încredere, de încredere relativă, de regulă non credibilă, non-credibilă sau imposibil de evaluat, datorită lipsei referințelor necesare⁴. În mod specific, caracteristicile claselor rezultate în urma evaluării sunt definite de criteriile de valoare ce se raportează la modalitatea de manifestare în spațiul virtual⁵.

Pe de altă parte, conținutul generat de utilizatorii rețelelor sociale presupune o monitorizare constantă a site-urilor de acest tip, precum și interacționarea cu aceștia pentru a fi acceptați/ invitați în grupurile personale. Similar, aplicațiile de tip „Second life” (lumi virtuale) și „Team Speak” (folosit pentru comunicarea online între membrii unei echipe de *gammeri*) oferă un mediu de relaționare extrem de eficient și dificil de monitorizat.

Toate acestea presupun eforturi pentru optimizarea fluxului informativ. Fluxul informativ pe principiul “o singură sursă – un singur echipament de prelucrare – un singur analist – unul sau mai multe rezultate” a devenit ineficient în condițiile “avalanșei

¹

<http://moz.com/researchtools/ose/comparisons?page=1&site=http%3A%2F%2Fwww.aco.nato.int%2Fsaceur2013%2Fblog%2Fwho-are-the-men-behind-the-masks.aspx>

² <http://www.touchgraph.com>

³ <http://caddereputation.over-blog.com/article-25657258.html>

⁴ <https://www.fishnetsecurity.com/6labs/blog/threat-intelligence-evaluating-sources-and-information-they-provide>

⁵ un alt exemplu elocvent este oferit de lucrarea “Verification Handbook. An ultimate guideline on digital age sourcing for emergency coverage” (Silverman și alții, 2014), care expune metodologia de lucru și instrumentele on-line necesare determinării nivelului de credibilitate a informației, dar și algoritmi de culegere de date și informații în mediul virtual

informaționale”. Arhitectura analist – server, distribuită după cerințele informaționale tot mai multe, reprezintă soluția care răspunde cel mai bine nevoilor de prelucrare, analiză, producție și diseminare a informațiilor.

OSINT – emergența ca disciplină recunoscută în Intelligence

Ca disciplină de culegere a informațiilor, activitatea subsumată OSINT a fost considerată multă vreme doar o capabilitate atașată comunităților de Intelligence specializate (complementară datelor și informațiilor obținute din surse secrete). Totuși, importanța și oportunitățile oferite de OSINT în peisajul lumii globalizate a determinat o serie de schimbări, instituționalizarea acestei discipline în cadrul unor agenții specializate, cu deschidere către comunități de interes mai mult sau mai puțin restrânse, fiind o opțiune luată în considerare de tot mai multe state.

Astăzi, comunitățile OSINT cuprind entități din spectrul guvernamental, al serviciilor specializate de Intelligence, al forțelor armate și structurilor de securitate națională, în cadrul autorităților din domeniul implementării legii și chiar din domeniul afacerilor.

Istoria recentă a OSINT ca disciplină de Intelligence începe în 1988, odată cu evidențierea de către generalul Alfred M. Gray, Jr. a avantajelor evidente ale acesteia ca capabilități în contextul geopolitic creat de disoluția Uniunii Sovietice (Gray,1990); acest avânt de promovare a OSINT a fost materializat mai târziu, prin reforme (sau încercări de reformă) repetate ale comunității de Intelligence ale SUA (crearea, în 1992, sub auspiciile National Security Act a unui birou pentru informații din surse deschise; reliefarea OSINT ca resursă prioritară de către comisia Aspin-Brown, în 1996; recomandarea, în 2004, a Comisiei 9/11 privind înființarea unei agenții pentru Intelligence din surse deschise, întărită anul următor de raportul Comisiei SUA pentru Capabilități de Intelligence cu privire la Armele de Distrugere în Masă (Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction – Comisia WMD), ce recomanda crearea unui directorat OSINT în cadrul CIA), culminate cu deschiderea, în noiembrie 2005, a *National Intelligence Open Source Center*¹, în cadrul CIA.

Conform recomandărilor din raportul din martie 2005 al Comisiei WMD, OSINT trebuie inclus în procesul de Intelligence integrat (toate sursele) datorită valorii particulare pe care acesta o are, concretizată în: oferirea de informații diversificate, de ansamblu, actualizate (cu păstrarea perspectivei istorice) și cu acoperire globală, facilitarea înțelegerii informațiilor din surse secrete, protejarea surselor și metodelor secrete prin asigurarea de referințe la informații din surse deschise².

La nivelul Uniunii Europene (UE) putem menționa eforturile Centrului Întrunit de Cercetare al Comisiei UE (Joint Research Centre – JRC³), care prin instrumente ca: European Media Monitor (EMM) și OSINT Suite⁴ asigură sisteme de analiză avansate pentru monitorizarea media tradițională și socială (figura 5.11).

¹ <http://www.cnn.com/2005/POLITICS/11/08/sr.tues/>

² Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, pp. 378–379, http://en.wikipedia.org/wiki/Iraq_Intelligence_Commission

³ <https://ec.europa.eu/jrc/>

⁴ <http://btn.frontex.europa.eu/resources/tools/emm-open-source-intelligence-suite-emm-osint-suite>



Figura 5.11 Europe Media Monitor – News brief. Sistemul prezintă ultimele știri indexate după subiect, din surse ce cuprind portaluri la nivel global, în 43 limbi (actualizate la fiecare 10 minute), cuprinzând analiza, colajul/ agregarea informației și emiterea de alerte¹

Eforturile în cadrul NATO de a stabili cadrul general al capacității OSINT s-a materializat în publicarea unui număr de manuale practice între 2001 și 2002 (figura 5.12).

Prima publicație din serie – *NATO Open Source Intelligence Handbook* (nov. 2011)² – urmărește familiarizarea audienței cu problematica OSINT. Al doilea volum – *NATO OSINT Reader* (februarie 2012)³ – se constituie într-un compendiu al nivelului global al cunoașterii în domeniul folosirii datelor și informațiilor din surse deschise în vederea elaborării produselor de Intelligence.



Figura 12 Seria de manuale NATO pentru OSINT (2011-2012)

¹ <https://ec.europa.eu/jrc/en/scientific-tool/europe-media-monitor-newsbrief>

² http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf

³ http://www.au.af.mil/au/awc/awcgate/nato/osint_reader.pdf

Al treilea din seria dedicată OSINT, îndrumarul NATO "Intelligence exploitation of the Internet" – octombrie 2002¹ abordează subiectul din perspectiva ciclului Intelligence, descriind aspectele specifice ale tuturor etapelor subscrise acestuia – direcționare, colectare, procesare și diseminare – oferind totodată o serie de resurse documentare deschise pe diferite domenii de interes (terorism, contrainformații, criminalitate transfrontalieră, date geopolitice și militare, date tehnice, etc. – cu rezerva anului publicării acestora). Îndrumarul oferă un reper excelent de orientare în sistematizarea direcționării activității de culegere de date și informații din surse deschise (planificarea și formularea cerințelor de informații prioritare), direcționare preluată în activitatea de culegere efectivă a datelor și informațiilor de pe platforma Internet. Aspectele tehnice ale planificării colectării de date și informații de pe Internet sunt sprijinite de dezvoltarea unor algoritmi practici de identificare a conceptelor cheie, determinarea indecșilor de căutare, strategiile și procedurile efective de căutare și descrierea modalității de utilizare a motoarelor de căutare.

Procesarea datelor și informațiilor din surse deschise trebuie să țină cont de câteva repere fundamentale în această activitate, în primul rând legată de credibilitatea surselor (determinarea surselor primare ale datelor și informațiilor accesibile pe Internet, a proprietarilor domeniilor, etc.). Listele de control pentru evaluarea surselor în vederea validării – incluse în categoriile: pagini web activiste, pagini web de afaceri/marketing, pagini web pentru știri, pagini web informative și pagini web personale – urmăresc o serie de criterii relevante în determinarea nivelului acestora: autoritatea (responsabilitatea) asupra conținutului, acuratețea informației (legătura cu aspecte factice, comprehensibilitatea mesajului), obiectivitatea, gradul de actualitate, nivelul de acoperire a subiectului.

În ce privește diseminarea produselor OSINT, dincolo de forma de prezentare, un aspect important îl reprezintă nivelul de clasificare a acestora. OSINT rezultat poate fi accesibil publicului larg (pentru a justifica decizii politice), circulat în cadrul unor comunități de interes naționale sau internaționale (pentru verificarea și validarea acesteia sau pentru orientarea culegerii de informații din surse secrete) sau poate să beneficieze de diseminare limitată, secretul acesteia fiind legat de interese strategice (Schauer și Störger, 2010).

Actualmente, dezvoltarea capabilității OSINT în NATO este sprijinită de activitatea unui grup de lucru dedicat (NATO OSINT Working Group), subordonat NATO Air Force Armaments Group (NAFAG)/ Joint Capability Group on Intelligence Surveillance and Reconnaissance (JCGISR)/ All Source Intelligence Integration Sub Group (ASIISG) (Grupul pentru Armamente al Forțelor Aeriene NATO/ Grupul pentru Capabilitate Întrunită pentru Intelligence, Supraveghere și Recunoașteri/ Sub-grupul pentru Integrarea Intelligence din toate Sursele).

La nivel doctrinar, responsabilitatea dezvoltării doctrinei OSINT pentru NATO îi revine Grupului de Lucru pentru Intelligence Întrunit (Joint Intelligence Working Group – JINTWG), având ca și custode responsabil Canada².

În ce privește pregătirea teoretică și practică, dincolo de capacitățile naționale ale statelor aliate, Școala NATO de la Oberammergau furnizează educație de specialitate în cadrul unui curs OSINT de o săptămână, dedicat analiștilor; pe timpul cursului sunt folosite programe informatice specifice, atât comerciale cât și militare³.

Implicații ale OSINT

Dacă informațiile cu privire la sursele secrete și tehnicile, tacticile, procedurile, metodele și tehnologiile folosite în activitatea operativă, precum și parte din relațiile stabilite

¹ <http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB436/docs/EBB-005.pdf>

² orizontul estimativ de timp pentru publicarea doctrine NATO OSINT este 2015-2016

³ https://www.natoschool.nato.int/documents/course_descriptions/Course%20Information%20N2-04.pdf

cu alți actori, sunt tratate cu discreție, fiind în majoritatea cazurilor clasificate, informațiile obținute din surse deschise nu se raportează în mod necesar la proceduri legale complicate sau tehnici de colectare clandestine.

Dincolo de datele și informațiile liber vehiculate în mediul virtual, prin intermediul Internetului – în mod pasiv sau activ – pot fi obținute date referitoare la persoane de interes sau entități țintă. Acestea pot fi reprezentate de persoane cheie în anumite domenii de interes ori cu acces la anumite informații, ori companii activând în diferite domenii, prin intermediul bazelor de date specializate (care stochează, de exemplu, date economice sau cu privire la datoriile firmelor¹, date biografice și adrese ale consumatorilor sau clienților, etc.) – utile în special în domeniul Intelligence competițional, activitatea de marketing, managementul riscului (de exemplu, bazele de date privind persoanele rău-platnice a creditelor contractate²) etc., ori prin elicitarea acestora în cadrul rețelelor sociale ("social engineering" - arta de a manipula persoane pentru a obține date mai mult sau mai puțin confidențiale de la acestea³).

Accesul legal la baze de date se face ori făcând apel la repoziitoare publice, ori prin intermediul a diferite companii specializate în constituirea și gestionarea acestora în interes comercial (precum Lexis-Nexis⁴, D&B⁵ și multe altele), de regulă contra cost. În mediul public, astfel de baze de date pot sprijini autoritățile (examinatori medicali, medicina legală, procuratura) dar și publicul larg să identifice persoane dispărute/ decedați necunoscuți⁶ sau baze de date ce listează persoane date în urmărire⁷. Mai mult, bibliotecile universităților oferă, gratuit sau contra cost, o serie de instrumente de cercetare care fac apel la utilizarea capacităților de culegere și procesare a datelor și informațiilor din surse deschise în scop academic. În toate aceste demersuri trebuie să se țină cont de drepturile de proprietate intelectuală și copyright, în conformitate cu legislația în vigoare.

Pe lângă organizațiile de intelligence guvernamentale/ naționale, OSINT este deja un instrument consacrat în mediul privat/ al afacerilor, în special în cadrul creat de activitățile de Intelligence competițional. În acest context, OSINT este adoptat ca efort sistematic, cu obiective precise, încadrat într-un anumit orizont de timp și desfășurat în parametri de etică profesională în vederea colectării, sintetizării și analizei competitorilor și a mediului extern, cu scopul de a asigura produse de Intelligence acționabil pentru factorii de decizie – a căror acțiuni se vor traduce în performanțe economice și financiare superioare. Acestea se raportează, în mod concret, la asigurarea avertizării situaționale, prevederea evoluțiilor ulterioare ale unor indicatori, managementul riscului și evitarea surprinderii, evidențierea unor potențiale cursuri de acțiune în procesul decizional.

C. Fleisher definește OSINT din perspectiva Intelligence competițional ca reprezentând căutarea, culegerea, exploatarea, validarea, analiza și distribuirea către clienți a produselor rezultate din datele disponibile din surse publice neclasificate (Fleisher, 117, 2008).

¹ de exemplu, portalul <http://www.listafirme.ro/>

² Instituțiile de credit au acces la baze de date specializate în care sunt puse la comun informații despre persoanele care au contractat credite și persoanele care n-au plătit la timp:

- **Biroul de Credit.** Este o bază de date administrată de compania cu același nume, fondată de bănci. Aici, băncile pun la comun informațiile despre clienții care au restanțe mai mari de 30 de zile, inclusiv durata întârzierii și suma datorată, date păstrate timp de 4 ani de la înregistrarea acestora.
- **Centrala Riscului de Credit.** Această bază de date este reglementată și administrată de BNR. Instituțiile pot afla de aici atât informații despre cei cu restanțe, cât și despre alte împrumuturi contractate de un solicitant (credite peste 20.000 lei). Informațiile sunt păstrate în această bază de date timp de șapte ani. (<http://volksbank.ro/ro/Sectiune/Cum-eviti-ratele-impovaratoare-483>)

³ <http://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering>

⁴ <http://www.lexisnexis.com>

⁵ <http://www.dnb.co.uk>

⁶ <http://www.namus.gov/>;

⁷ <http://www.politiaromana.ro/urmariti/urmariti.aspx>

OSINT reprezintă un motor esențial pentru Intelligence, într-un cadru al economiei și securității globalizate, reclamând conlucrarea activă și un real parteneriat public-privat.

Toate aspectele legate de modul de manipulare și utilizare a datelor din surse deschise și a produselor obținute prin prelucrarea acestora presupun respectarea cadrului legal, a drepturilor specifice și a normelor etice. Astfel, culegerea de date și informații din surse deschise referitoare la persoane suspectate de implicare în acțiuni de criminalitate organizată ori terorism nu presupune încălcarea drepturilor acestora.¹ În România, Legea 506/2004 privind prelucrarea datelor cu caracter personal² și protecția vieții private în sectorul comunicațiilor electronice³ nu se aplică prelucrărilor de date cu caracter personal efectuate în cadrul activităților în domeniul apărării naționale și securității naționale, ori în cadrul activităților de combatere a infracțiunilor și de menținere a ordinii publice/ altor activități în domeniul dreptului penal, desfășurate în limitele și cu restricțiile stabilite de lege⁴.

Concluzii

În actualul context geopolitic, potențialul de valorificare și capacitatea surselor deschise de a răspunde pe toate palierele de informare și cunoaștere la nevoile beneficiarilor reliefează importanța OSINT, care se dezvoltă odată cu evoluția tehnologică și a instrumentelor ce pot fi utilizate pentru a gestiona mijloacele de cunoaștere. Într-o societate a cunoașterii în continuă transformare și într-un mediu de securitate fluid și dinamic, marcate de inovațiile în domeniul digital, dezvoltarea OSINT devine motorul progresului în domeniul intelligence.

Potențialul OSINT este puternic promovat de activistul american Robert D. Steele, fost agent CIA, printr-o serie de lucrări ce articulează arhitectura tehnologiei informației globale arondate conceptului ”*Open Source Everything*” – Intelligence din surse deschise cu acoperire și accesibilitate globală (Steele, 2013), formulă considerată ca opțiune onestă și rentabilă într-o lume globalizată.

După cum observă și Steele – dincolo de utopia unei guvernante globale pozitiv orientate spre satisfacerea nevoilor obiective ale comunităților umane, rămâne de rezolvat modalitatea efectivă de operaționalizare a acestei capabilități, atât la nivel național cât și în cadrul instituțiilor de securitate internaționale, astfel încât acest imens potențial să fie exploatat în mod corespunzător.

¹ ***, *Aspecte privind etica profesională în lucrul cu informațiile din surse deschise*, în https://www.sri.ro/fisiere/studii/ETICA_SI_INTELLIGENCE.pdf

² Conform legii, furnizorul unui serviciu de comunicații electronice destinat publicului are obligația de a lua măsuri tehnice și organizatorice adecvate în vederea asigurării securității prelucrării datelor cu caracter personal. Conceptul de protecție a datelor cu caracter personal reprezintă dreptul persoanei fizice de a-i fi apărate acele caracteristici care conduc la identificarea sa și obligația corelativă a statului de a adopta măsuri adecvate pentru a asigura o protecție eficientă. Prin date cu caracter personal se înțeleg acele informații care pot fi puse direct sau indirect în legătură cu o persoană fizică identificată sau identificabilă, cum ar fi: numele, prenumele, codul numeric personal, adresa, telefon, imaginea, vocea, situația economico-financiară, profesia. (<http://www.schengen.mai.gov.ro/Documente/Vizite%20de%20evaluare/Protectia%20datelor%20personale.pdf>)

³ Legea 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, Publicată în Monitorul Oficial, Partea I, nr. 1101 din 25/11/2004, în <http://www.legi-internet.ro/legislatie-itc/date-cu-caracter-personal/legea-privind-prelucrarea-datelor-cu-caracter-personal-si-protectia-vietii-private-in-sectorul-comunicatiilor-electronice.html>, modificată prin Legea nr.272/2006 pentru completarea art.7 din Legea nr.506/2004 și OUG nr.13/2012

⁴ prelucrarea automată și neautomată a datelor cu caracter personal pentru realizarea activităților de prevenire, cercetare și combatere a infracțiunilor, precum și de menținere și asigurare a ordinii publice de către structurile/unitățile Ministerului Administrației și Internelor este reglementată prin Legea nr. 238/2009, republicată în 2012

Putem face apel, totodată, la mijloacele disponibile pentru educare și autoeducare în ce privește aspecte utile ale OSINT în activitatea membrilor comunităților de intelligence

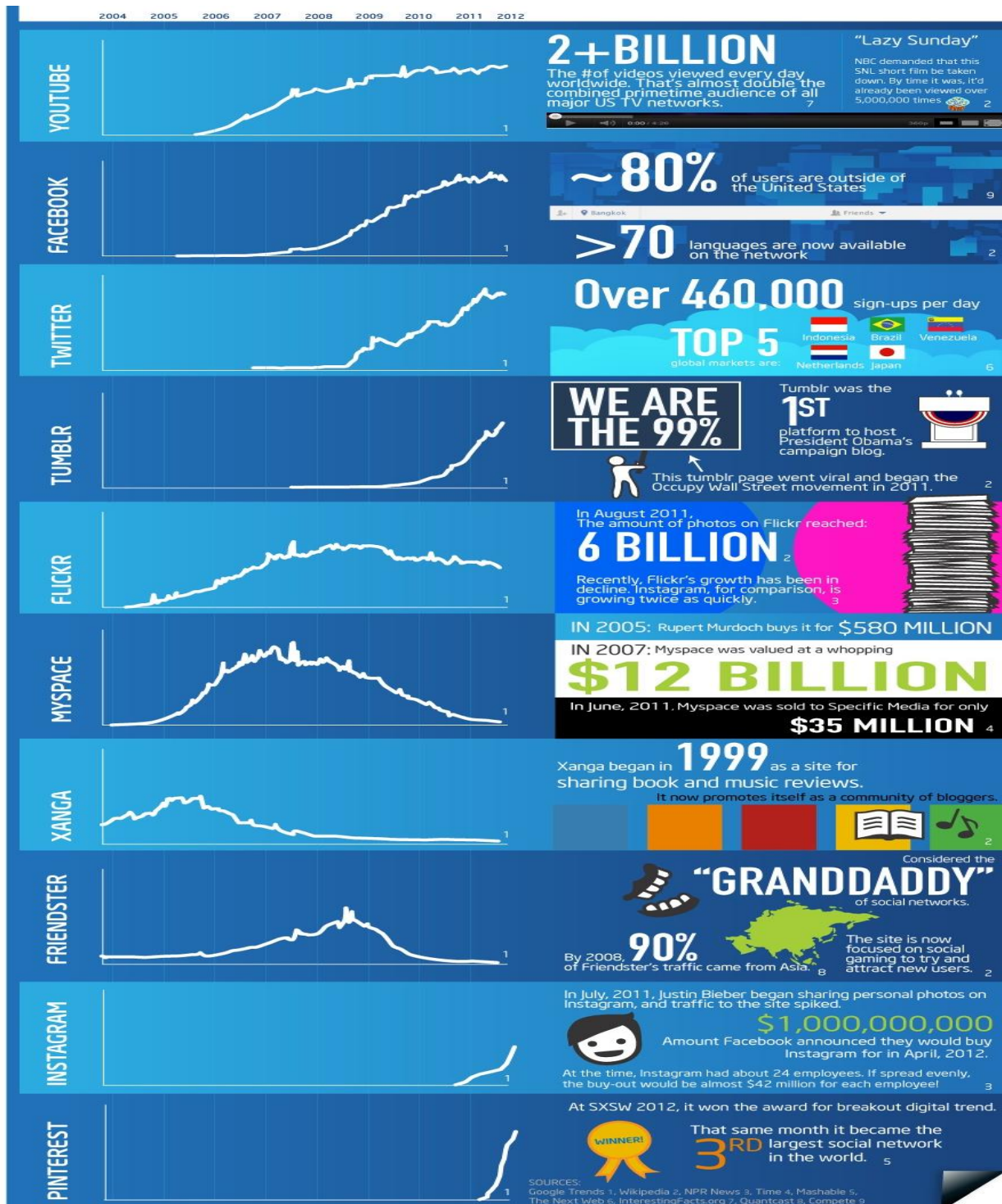
Bibliografie

1. ***, *Aspecte privind etica profesională în lucrul cu informațiile din surse deschise*, în https://www.sri.ro/fisiere/studii/ETICA_SI_INTELLIGENCE.pdf
 2. AHLQVIST, Toni, BACK, Asta, HALONEN, Minna, HEINONEN, Sirkka (2008) *Social Media Roadmaps. Exploring the futures triggered by social media*, VTT Technical Research Centre of Finland, Edita Prima Oy, Helsinki, în <http://www.vtt.fi/inf/pdf/tiedotteet/2008/T2454.pdf>
 3. CIȘMIGIU, Cristian-Victor (2013) *Sursele deschise de informare – oportunități de susținere și dezvoltare ale unui învățământ performant și eficient în domeniul informații pentru apărare*, în *Gândirea Militară Românească*, 1/2013
 4. Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, pp. 378–379, http://en.wikipedia.org/wiki/Iraq_Intelligence_Commission
 5. FLEISHER, Craig (2008) *OSINT: Its Implications for Business/Competitive Intelligence Analysis and Analysts*, în *Inteligencia y Seguridad* no. 4-2008, <http://www.phibetaiota.net/wp-content/uploads/2013/02/2008-Fleisher-on-OSINT-English-and-Spanish.pdf>
 6. GRAY, Alfred M. (1990) *Global Intelligence Challenges in the 1990s*, *American Intelligence Journal* (Winter 1989–1990)
 7. Headquarters, Department of the Army (2012) *ATP 2-22.9 Open-Source Intelligence*, July 2012
 8. Legea 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, Publicată în Monitorul Oficial, Partea I, nr. 1101 din 25/11/2004, în <http://www.legi-internet.ro/legislatie-itc/date-cu-caracter-personal/legea-privind-prelucrarea-datelor-cu-caracter-personal-si-protectia-vietii-private-in-sectorul-comunicatiilor-electronice.html>
 9. NATO SACLANT (2001) *NATO Open Source Intelligence Handbook*, în http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20SINT%20Handbook%20v1.2%20-%20Jan%202002.pdf
 10. NATO SACLANT (2001) *NATO Open Source Intelligence Reader*, în http://www.au.af.mil/au/awc/awcgate/nato/osint_reader.pdf
 11. NATO SACLANT (2002) *Intelligence exploitation of the Internet*, în <http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB436/docs/EBB-005.pdf>
 12. NATO Standardization Agency (2013) AAP-6, *NATO Glossary of terms and definitions* (English and French)
 13. Open Knowledge Foundation (2014) *Open Data Handbook Documentation*, Release 1.0.0
 14. Public Law 109-163, *National Defense Authorization Act for Fiscal Year 2006*, în <http://www.gpo.gov/fdsys/pkg/PLAW-109publ163/html/PLAW-109publ163.htm>
 15. SCHAURER, Florian, STÖRGER, Jan (2013) *The Evolution of Open Source Intelligence*, în *Intelligence Journal of U.S. Intelligence Studies*, Winter/Spring 2013, pp.53-56
 16. SILVERMAN, Craig (editor), *Verification Handbook. An ultimate guideline on digital age sourcing for emergency coverage*, European Journalism Centre, Maastricht, the Netherlands, în <http://verificationhandbook.com/book/index.php>
 17. STEELE, Robert David (1997) *Open Source Intelligence: What Is It? Why Is It Important to the Military?*, în *Open Source Intelligence: READER Proceedings, 1997 Volume II 6th International Conference & Exhibit Global Security & Global Comp*
 18. STEELE, Robert David (2013) *The Evolving Craft of Intelligence*, în Robert Dover, Michael Goodman, Claudia Hillebrand (eds.). *Routledge Companion to Intelligence Studies*, Oxford, UK: Routledge, 31 July, <http://www.phibetaiota.net>
 19. STOICA, Dan S. (2011) *Modele de comunicare științifică*, în <http://www.dstoica.ro/wp-content/uploads/2011/09/Modele-de-comunicare-%C5%9Ftiin%C5%A3ific%C4%83.pdf>
 20. Tree Works, *Blogurile – Metode alternative de comunicare și promovare pentru corporații*, București, în www.tree.ro
- ***
21. <http://btn.frontex.europa.eu/resources/tools/emm-open-source-intelligence-suite-emm-osint-suite>
 22. <http://caddereputation.over-blog.com>
 23. <http://moz.com/researchtools/ose>

24. <http://opensource.org/>
25. <http://primetime.co.ug/services/social-media/>
26. <http://volksbank.ro/ro/Sectiune/Cum-eviti-ratele-impovaratoare-483>
27. <http://webtrends.about.com/od/web20/a/social-media.htm>
28. <http://whois.domaintools.com/>
29. <http://www.aco.nato.int/saceur2013/blog/>
30. http://www.au.af.mil/au/awc/awcgate/nato/osint_reader.pdf
31. <http://www.aymennjawad.org/blog/>
32. <http://www.chathamhouse.org/about/chatham-house-rule/>
33. <http://www.cnn.com/2005/POLITICS/11/08/sr.tues/>
34. <http://www.dnb.co.uk>
35. <http://www.fbi.gov>
36. <http://www.intel.com/content/www/us/en/home-users/social-network-lives-infographic.html>
37. <http://www.internetociety.org/internet>
38. <http://www.lexisnexis.com>
39. <http://www.listaфирme.ro/>
40. <http://www.media.utah.edu>
41. <http://www.mhhe.com/mayfieldpub/webtutor/judging.htm>
42. [http://www.namus.gov/;](http://www.namus.gov/)
43. http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20SINT%20Handbook%20v1.2%20-%20Jan%202002.pdf
44. <http://www.politiaromana.ro/urmariti/urmariti.aspx>
45. http://www.sas.com/en_us/insights/big-data/what-is-big-data.html
46. <http://www.schengen.mai.gov.ro/Documente/Vizite%20de%20evaluare/Protectia%20datelor%20personale.pdf>
47. <http://www.sri.ro>
48. <http://www.touchgraph.com>
49. <http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB436/docs/EBB-005.pdf>
50. <https://ec.europa.eu/jrc/en/scientific-tool/europe-media-monitor-newsbrief>
51. <https://www.fishnetsecurity.com/6labs/blog/threat-intelligence-evaluating-sources-and-information-they-provide>
52. https://www.natoschool.nato.int/documents/course_descriptions/Course%20Information%20N2-04.pdf
53. <http://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering>

Anexa nr. 1 – Infografic privind evoluția rețelelor sociale

(<http://www.intel.com/content/www/us/en/home-users/social-network-lives-infographic.html>)



CAPITOLUL 6. ELEMENTE CHEIE ALE ANALIZEI INFORMAȚIILOR ÎN CONTEXTUL GLOBALIZĂRII

Cerințe ale analizei de Intelligence în lumea globalizată

Activitatea de analiză a informațiilor, etapă esențială a ciclului Intelligence, este puternic solicitată ca urmare a schimbărilor pe care mediul de securitate le înregistrează, asociate cu reformularea priorităților în materie de cereri de Intelligence ale factorilor decizionali, în toate domeniile de interes. Sectoarele de referință exclusive își largesc în permanență aria de acoperire și se întrepătrund, solicitând activitatea conjugată a unei largi palete de senzori/ operatori pentru a culege date și informații din diferite medii, precum și servicii analitice specializate multilateral.

Domeniile de interes informativ depășesc sfera amenințărilor de securitate pur militare sau factorii mediului operațional; capabilitățile și vulnerabilitățile nu mai sunt cântărite exclusiv prin prisma raportului de putere, ci și a impactului economic, socio-cultural, media, etc. Cu toate acestea, după cum o demonstrează criza din Crimeea, materializarea unei amenințări militare clasice nu poate fi exclusă, iar eludarea indicatorilor în acest sens ar fi o greșală strategică costisitoare, cu efecte asupra unui mare număr de națiuni¹.

După B. Buzan, reprezentant al Școlii de la Copenhaga – exponentă a postmodernismului în studiile de securitate (Sarcinski, 2005) – interdisciplinaritatea analizei de securitate privește mai multe dimensiuni: (Buzan, 2000)

- *dimensiunea militară*, care se referă la interacțiunea dintre capabilitățile armate ale statelor cu percepțiile statelor vizavi de intențiile celorlalte;
- *dimensiunea politică*, care analizează stabilitatea organizațională a statelor, a sistemelor de guvernare și a ideologiilor ce le conferă legitimitate;
- *dimensiunea economică*, care include accesul la resurse și la piețele necesare menținerii bunăstării și puterii statului respectiv;
- *dimensiunea socială*, constând în sustenabilitatea identitară;
- *dimensiunea de mediu*, concentrată asupra biosferei ca sistem de suport al existenței umane.

La rândul ei, doctrina britanică recunoaște ca și corespondente planurilor fizic, virtual și cognitiv ale abordărilor de Intelligence reprezentarea planurilor multiple definiții pentru spectrul de interes în activitatea de analiză (figura 6.1):

- lumea fizică (suportul real al evenimentelor);
- rețelele de interacțiune și comunicare (conectivitatea);
- informația (obiectul comunicării);
- persoanele (vectori individuali ai comunicării);
- comunitatea umană (actorii peisajului informațional);
- sfera socială (interacțiunile la nivel de micro-grup sau cele colective).

În procesele decizionale, Guvernele se bazează pe produse analitice combinate ale serviciilor de Intelligence militare și civile în elaborarea planurilor la nivel strategic, acestea fiind în măsură să asigure capacitatea de a **anticipa** trendurile evoluției fenomenelor securitare de interes și a fundamenta conturarea unei **viziuni** coerente, în virtutea abilității predictive a analizei. În plus, O. Frățilă vede în scopul analizei sprijinirea factorilor de decizie în **modelarea viitorului** și nu în precizarea acestuia (Frățilă, 2008).

¹Efectele pe care o situație de criză majoră le are asupra statelor interconectate multidimensional în lumea globalizată reclamă o atenție corelată a națiunilor ce împărtășesc aceleași valori fundamentale, în sensul asigurării avertizării timpurii asupra riscurilor de securitate

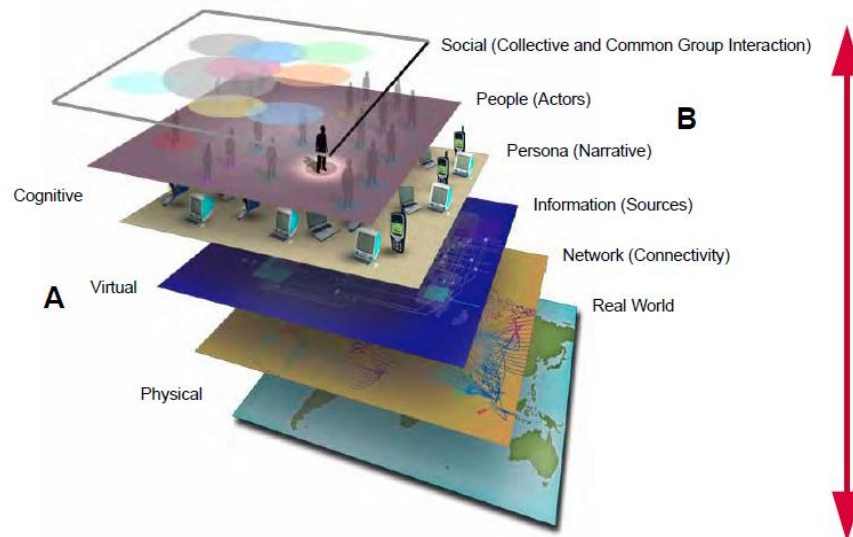


Figura 6.1 Domeniul informațional și câmpurile de analiză¹

În acest sens, analiza de Intelligence ajută la identificarea (Frățiță, 2008):

- oportunităților de a promova interesele statului prin mijloace diplomatice, militare și economice, diplomatie publică și prin acțiuni acoperite;
- vulnerabilităților strategice și tactice ale liderilor, partidelor și grupărilor și mișcărilor ostile statului;
- factorilor care pot fi influențați;
- rezultatului probabil al cursului de acțiune adoptat;
- evaluarea punctelor forte și a celor slabe ale adversarilor.

Capabilitățile analitice fac uz de sisteme de gândire complexe, cu abilități avansate de intuiție, percepție, creativitate, analiză și sinteză, completate de proceduri specifice și tehnologie menită să eficientizeze prelucrarea informației. Aspectelor calitative ale sistemului analitic i se adaugă plus-valoarea conferită de politicile de parteneriat cu alte grupuri sau organizații care activează în domeniu, cu acoperire geografică și pe domenii funcționale cât mai largă.

Doctrina Națională a Informațiilor pentru Securitate (2004) stabilește o serie de principii în baza cărora activitatea de informații se desfășoară într-un stat de drept:

- a. principiul legalității;
- b. caracterul planificat și sistematic al activității de informații;
- c. ofensivitatea și mobilitatea activității de informații;
- d. anticiparea și previzionarea;
- e. obiectivitatea evaluărilor;
- f. informarea exactă, corectă și oportună a factorilor de decizie;
- g. independența, neutralitatea și echidistanța politică;
- h. protecția surselor, metodelor și mijloacelor;
- i. principiul cooperării, conlucrării și colaborării;
- j. cooperarea internațională cu serviciile de informații ale statelor membre ale NATO, UE, precum și cu alte servicii de informații.

La nivelul procesului de analiză, aceste principii sunt reflectate în mod corespunzător, activitatea fiind corelată scopurilor urmărite la nivel de conducere și a planurilor de culegere a

¹The Development, Concepts and Doctrine Centre, UK Ministry of Defence, Joint Doctrine Publication 04 (JDP 04) (2010) *Understanding*, Shrivenham Swindon, Wiltshire, UK

informațiilor ce decurg din acestea. Capacitățile analitice trebuie să fie congruente funcțional cu specialitățile de colectare, rezonante la cerințele de flexibilitate și prioritizare a eforturilor și să fundamenteze abilitatea de previzionare cantitativă și calitativă a evoluției evenimentelor de interes.

În acest sens, din perspectiva interdisciplinarității și pan-naționalului în materie de amenințări de securitate, cooperarea¹, conlucrarea² și colaborarea³ intra și inter-instituțională, pe plan național sau internațional, este o cerință esențială.

Totodată, procesul analitic trebuie să asigure obiectivitatea⁴ evaluărilor și livrarea în timp oportun a produselor solicitate în sprijinul procesului decizional.

Schimbările la nivelul disciplinei Intelligence în lumea globalizată sunt determinate atât de natura noilor tipuri de amenințări la adresa securității internaționale, cât și de orientarea beneficiarilor serviciilor din domeniu (Frățilă, 2008). Un alt factor ce determină schimbări majore la nivelul capabilității este evoluția tehnologică, ce se reflectă la nivelul tuturor etapelor ciclului Intelligence.

Securitatea informației la nivelul produselor de intelligence este o problemă de importanță majoră în asigurarea cerințelor de confidențialitate. În situațiile de criză, pentru prezervarea oportunității și a rapidității de acțiune, se impune limitarea numărului de persoane care au acces la procesul de conducere (implicit, la produsele de analiză), prin constituirea sau activarea unui centru de criză cu atribuții precise. Centrul de criză este sprijinit în mod decisiv de componenta de integrare a tuturor informațiilor, provenite din toate sursele, componentă ce asigură și procurarea, prelucrarea, analiza, difuzarea și evaluarea datelor și informațiilor (Buciuman, 2004).

Analiza în cadrul ciclului Intelligence

Analiza de Intelligence reprezintă un proces sistematic de prelucrare și evaluare a datelor și informațiilor despre un subiect de referință la nivel strategic, operativ, tactic (și tehnic - Pârlog, 2008), fiind componenta de bază în evaluarea situației și conversia avertizării situaționale în înțelegerea fenomenelor de natură securitară și a trendurilor (probabilității) evoluției acestora în timp și spațiu. Partea predictivă a procesului analitic permite factorilor de decizie dezvoltarea cursurilor de acțiune potențiale.

Abordările multitudinilor de probleme din spectrul analizei de Intelligence reclamă diferite metode pentru rezolvarea lor. Printre principiile pe care analiștii trebuie să le aibă în vedere menționăm: (Frățilă, 2008, 165-166)

- căutarea sistematică a informațiilor în toate sursele deschise și exploatarea lor în toate tipurile de produse analitice;
- folosirea instrumentelor analitice ca sprijin și nu ca suplinitor al efortului analitic;
- ne-discriminarea surselor (unele mai privilegiate decât altele) sau a metodelor analitice (analiștii trebuie să utilizeze, în mod constant, o gamă variată de instrumente, metode și tehnici și nici una dintre acestea nu trebuie privită ca excepțională sau alternativă);

¹ **cooperarea** semnifică organizarea, coordonarea, susținerea și realizarea în comun, pe baza unor programe sau planuri de măsuri, de către structuri ale comunității de informații, a unor acțiuni specifice, care vizează obținerea, verificarea și valorificarea informațiilor și produselor informaționale

² **conlucrarea** definește modalitățile concrete de organizare și desfășurare de către personal sau compartimente specializate, în raport de competențe

³ **colaborarea** presupune că serviciile de informații inițiază și dezvoltă proiecte de colaborare cu autorități sau instituții publice pe baza și în executarea dispozițiilor legii

⁴ obiectivitatea presupune atât eliminarea, pe cât posibil, a inferențelor subiective ale analistului în procesul de evaluare și integrare a informațiilor (proces sprijinit de latura tehnologică a prelucrării informației), cât și aspectul legat de neutralitatea ideologică de orice natură

- metodele bazate pe formularea ipotezelor trebuie utilizate frecvent, pe lângă abordările tradițional - inductive bazate pe evidențe;
- utilizarea mai largă a testelor de diagnoză a evidențelor, ce permit îmbunătățirea abilității de a confirma sau nega ipoteze;
- recursul la colaborare ca rutină și nu excepție; etc.

În baza acestor considerente, procesul de analiză cuprinde următoarele etape¹:

1. **Colarea** este prima etapă a analizei, care presupune o grupare inițială a datelor și informațiilor ce se relaționează între ele, rezultând liste de evenimente pentru procesarea ulterioară;
2. **Evaluarea** presupune selectarea unui subiect informațional și determinarea gradului de încredere a sursei și credibilitate a informației (această etapă impune diferențierea informațiilor veridice de cele false, menite să dezinformeze audiența țintă);
3. **Integrarea** implică revederea structurată a informației în scopul identificării faptelor semnificative pentru interpretarea ulterioară prin folosirea unei game variate de instrumente și tehnici².
4. **Interpretarea** este pasul final al procesului analitic, ce valorifică semnificația informației rezultate în urma integrării (Intelligence) în relație cu nivelul curent al cunoașterii, în vederea furnizării unei evaluări finale și integrării altor informații relevante pentru elementele identificate;
5. **Revizuirea continuă** permite actualizarea permanentă a nivelului de cunoaștere, necesară prin raportarea la dinamica evenimentelor în plan securitar. Dincolo de metodologia procesului analitic, feed-backul față de produsele de Intelligence permite reajustarea orizonturilor de investigație (Ioan, 2008) și sporește eficiența activităților de evaluare și integrare. Feed-backul este dezirabil la nivelul tuturor treptelor activității de Intelligence.

După M. Tulică, denumirile etapelor procesului de analiză sunt ușor modificate, dar urmăresc – în general – aceeași secvențialitate a acțiunilor (Tulică,2009,21):

1. **Prelucrarea** este etapa procesului analitic realizată prin operațiuni aplicate datelor pentru a deveni utilizabile;
2. **Coroborarea** este procesul managerial specific de confirmare/infirmare a conținutului unei informații în raport de cunoștințele existente la momentul respectiv;
3. **Integrarea** constă în reuniunea datelor dispartate, obținute succesiv în procesul culegerii sau colectării, reunirea lor după criterii și reguli prestabilite, estimarea veridicității și utilității lor și încorporarea într-o informație de sine stătătoare sau într-un produs informațional;
4. **Analiza** semnifică tratarea informațiilor prin folosirea metodelor logice, analogice, sistemice de analiză, în scopul stabilirii adevărului, incertului sau falsului;
5. **Evaluarea** este etapa procesării informației în care i se stabilește utilitatea și valoarea de destinație.

Rezultatul activității de procesare a informațiilor se materializează în produsele informaționale destinate factorilor decizionali stabiliți de lege potrivit „nevoii de a cunoaște” și individualizate în documente și forme de evidență specifice.

Dintre metodele și procesele specifice analizei de Intelligence le vom prezenta pe cele mai reprezentative.

Astfel, **judecata** este definită în dicționarul *Oxford* ca abilitate de a elabora decizii fundamentate sau a ajungerea la concluzii sensibile¹. La nivelul analiștilor, judecata implică

¹The Development, Concepts and Doctrine Centre, UK Ministry of Defence, Joint Doctrine Publication 04 (JDP 04) (2010) *Understanding*, ShrivenhamSwindon, Wiltshire, UK, para 307, p. 3-3

²tehnicele și principiile de analiză din perspectiva doctrinei britanice sunt prezentate în detaliu în JDP 2-00 (3rd Edition) *Understanding and Intelligence in Support of Joint Operations*, capitolul 5, 2011

trecerea de realitatea descrisă de informațiile disponibile și reprezintă principala modalitate de a îndepărta incertitudinea. Prin natura sa, judecata asigură ciclicitatea procesului de dezvoltare a cunoașterii, permițând tranziția de la cunoscut la necunoscut și din nou la cunoscut.

Cu toate că scopul final al procesului este de a atinge cunoașterea completă, acesta este un ideal greu de atins; toleranța la ambiguitate devine astfel un indicator al nivelului de acoperire informațională a unui eveniment.

Logica situațională, la rândul ei, implică generarea de ipoteze bazate pe elementele concrete ale situației reale – progresiv, pe măsura cunoașterii lor – limitată la un scenariu specific studiat în evoluția sa temporală.

Teoria aplicată, o altă metodă de abordare analitică, se bazează pe aplicarea la realitate a modelelor desprinse din generalizări sugerate de experiența acumulată, permițând depistarea gradului de importanță (semnificația) tendințelor în cadrul evenimentelor studiate.

Prin **comparație**, evenimentele dintr-o zonă sau la un anumit reper cronologic sunt raportate la evenimente similare din alte zone sau la precedente istorice. Ca metodă, comparația diferă de teoria aplicată în care concluziile sunt tratate pe baza unui număr de situații distincte.

Gândirea critică (figura 6.2) constă din procesul de evaluare a informației din perspectiva veridicității informației. Gândirea critică duce la un proces de reflecție asupra înțelesului acestor afirmații, examinând dovezile și raționamentul oferit și judecând faptele.

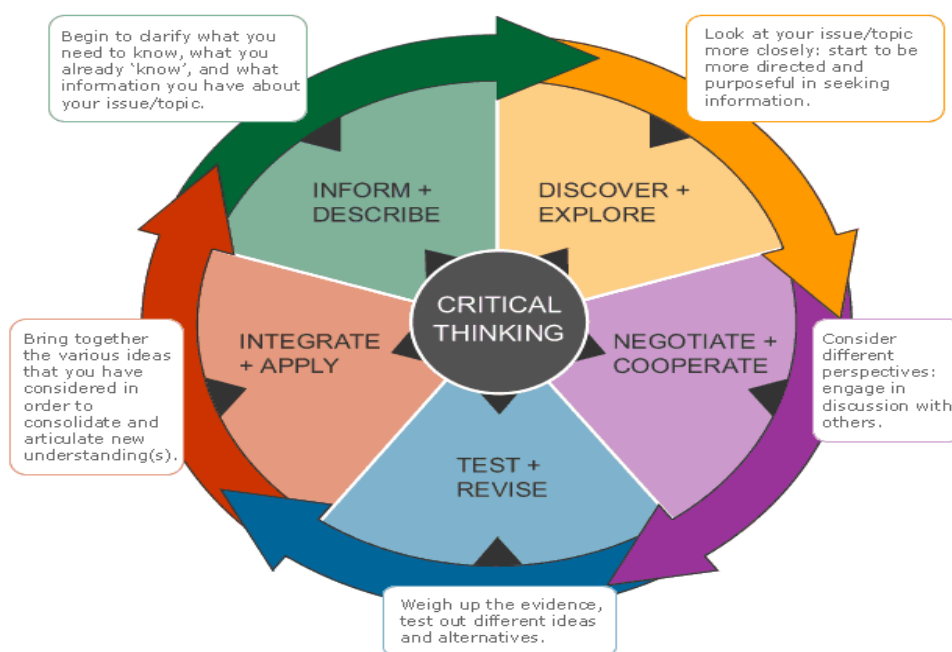


Figura 6.2 Procesul gândirii critice²

Capcane cognitive în activitatea de analiză

În activitatea sa, analistul este supus unor ”capcane” cognitive pe care trebuie să le conștientizeze. După Heuer, majoritatea problemelor cu care se confruntă analiștii țin ori de

¹<http://www.oxforddictionaries.com/definition/english/judgement>

²<http://azizaizmargari.files.wordpress.com/2011/08/critical-thinking-image.gif>

cultura organizațională din care aceștia provin¹, ori de propria personalitate (Heuer, 1999). În această din urmă categorie, specialiștii disting o serie de erori comune, cum ar fi:

- **imaginea în oglindă** (Witlin, 2008) care constă în proiectarea propriei gândiri asupra structurii motivaționale a oponentului și raportarea la propriul sistem de valori în evaluarea unor persoane aparținând altor culturi; informațiile despre subiectul analizat trebuie privite prin prisma gradului lor de obiectivitate (subiectul nu este neapărat așa cum este reflectat de către sursă, care poate prezenta o imagine deformată prin prisma propriului sistem de valori, a abilităților de interpretare a realității sau chiar de propriile prejudecăți sau interese²).
- **fixarea țintei** – tendința prin care analistul poate căpăta fixație asupra uneia dintre ipoteze, căutând doar argumente legate de prejudecățile sale și ignorând alte perspective; o altă formă de fixație a ideii este și dorința de finalizare rapidă a cazului sau absolutizarea modelelor socio-culturale;
- **analogiile inadecvate**, atunci când sunt bazate pe asumptii ale echivalențelor culturale sau contextuale; predispunerea la astfel de analogii apare în cazul studiului insuficient, a lipsei de informații factuale sau neînțelegerea acestora, a inabilității de a corobora date noi cu altele vechi sau simpla negare a conflictului de fapte. Câteva exemple în această categorie sunt:
 - o **preconcepția proporționalității**, ce privește asumarea importanței date anumitor aspecte similare în culturi diferite;
 - o **prezumția acțiunii unitare în cadrul organizațiilor** – fapt contrazis de culturile organizaționale ce diferă de la o națiune la alta.
- **ipoteza actorului rațional** reprezintă folosirea propriilor standarde în judecarea rațiunii comportamentului subiectului – inclusiv nivelul de acceptare a riscului.

Cultura organizațională își pune și ea amprenta asupra activității analitice și a calității produsului de Intelligence. Organizațiile care pun accent exclusiv pe una dintre disciplinele de colectare, suferind un fenomen de specializare funcțională, ori compartimentarea excesivă sau monopolizarea fluxului de informații, sunt doar câteva conjuncturi posibile ce își pun amprenta asupra activității analiștilor.

Analiștii sunt supuși încercărilor de inducere în eroare (intoxicare) din partea adversarului, precum și supraîncărcării compartimentelor de analiză cu informații redundante.

Personalitatea și calitățile personale ale analistului sunt elemente cuantificate în selectarea personalului. Curiozitatea, intuiția, pro-activitatea, spiritul inchizitiv, discernământul, creativitatea, comprehensivitatea, erudiția, cunoașterea limbilor străine, abilitățile de lucru cu sistemele bazate pe tehnologie, toate aceste atribute sprijină succesul profesional la nivelul analizei.

Emergența procesului analitic la nivel tactic

Secțiunea 7 - *Intelligence, Supraveghere și Cercetare în cadrul Corpului Maritim* (Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise/MCISRE) a Conceptelor și programelor USMC pentru 2013³ este subliniat faptul că procesul de analiză predictivă este esențial pentru proiecția forței expediționare.

¹o soluție în acest caz fiind folosirea de analiști aparținând aceleași culturi cu cea specifică evenimentelor evaluate/ rețelelor umane implicate; în orice situație, re-evaluarea de către un alt analist se impune ca opțiune pentru evitarea proiectării ”imaginii în oglindă”

²inabilitatea de a face distincția între subiect și părerea altora despre acesta este numită în psihologie ”fixare funcțională”

³ US Marine Corps, *Concepts and programs 2013, America's Expeditionary Force in Readiness*, <http://www.hqmc.marines.mil/Portals/142/Docs/USMCCP2013flipbook/USMC%20CP13%20Final.pdf>

Crearea unor elemente specializate (de ex. Marine Corps Intelligence Department Technology Innovation Division) permite folosirea unor metode și instrumente analitice avansate ce facilitează analiza predictivă standardizată și colaborativă.

Prin implementarea unor instrumente analitice moderne se urmărește accesul tuturor componentelor forței, dar și al partenerilor din cadrul comunității de interes, la cunoaștere, date, resurse și expertiză, exprimate prin abilitatea de ”a vedea” (asigurată prin mijloace ISR cu largă acoperire în timp și spațiu), ”a înțelege” (prin diseminarea de produse analitice bazate pe informații coroborate provenite de la întreg spectrul de discipline de culegere a informațiilor) și ”a acționa” (în baza procesului decizional sprijinit de produse Intelligence de înaltă calitate) (figura 6.3).

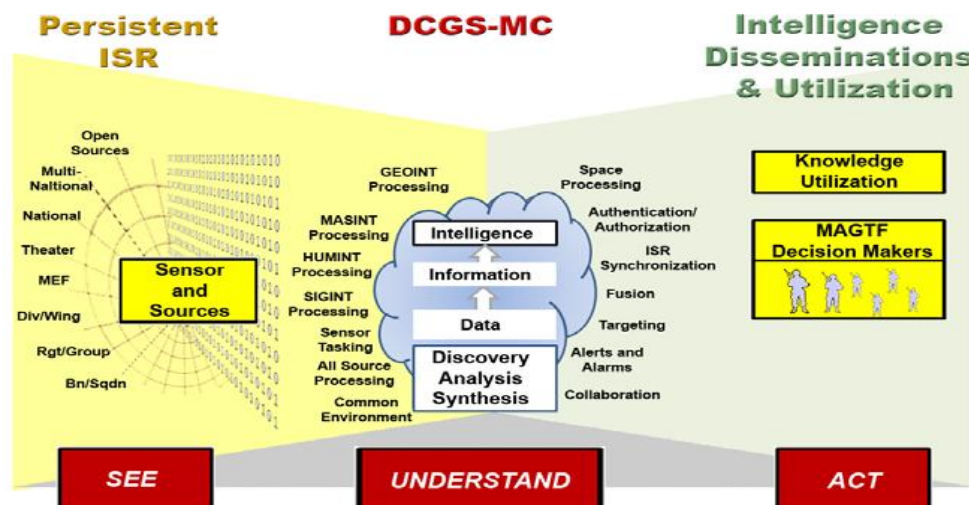


Figura 6.3 Rolul Intelligence în sprijinul operațiilor la nivel tactic¹

Conceptul ”21st Century Marine Expeditionary Intelligence Analysis (MEIA-21)”² prezintă o inițiativă formală a USMC de a restructura, standardiza și profesionaliza analiza de intelligence la nivel tactic în cadrul Corpului Maritim, în baza a șase principii fundamentale:

1. **operațiile de succes reclamă o capacitatea Intelligence viabilă la nivel tactic;**
2. **viabilitatea produselor de Intelligence la nivel tactic este asigurată prin proceduri sistematizate, adaptate misiunii;** documentul introduce acronimul SMAT (Modele, Abordări și Tehnici Structurate) ca spectru funcțional (proces și instrumente) fundamentat pe experiența practică a USMC, menit să sprijine producția de Intelligence acționabil în baza datelor primare;
3. **analiza de Intelligence orientate spre proceduri specifice acțiunilor avansate folosește procese analitice riguroase;** dincolo de abilitățile intuitive ale analiștilor în baza datelor existente, aceasta este îndreptată către tehnici obiective, validate în mod științific și supuse reactualizării permanente;
4. **produsele de Intelligence provenite din științele sociale (SOCINT³) sunt esențiale pentru procesul de analiză** în cadrul operațiilor ne-convenționale (ex. contrainsurgența, managementul situațiilor de criză, etc.), păstrând totodată o

¹ Idem, p. 125

² 21st Century Marine Expeditionary Intelligence Analysis (MEIA-21), *Modernizing Tactical Military Intelligence Analysis*, September 2011, <http://www.phibetaiota.net/2011/09/21st-century-marine-expeditionary-analysis-meia-21-modernizing-tactical-military-intelligence-analysis/>

³ Documentul folosește conceptual de *Social Science Intelligence (SSI)/ Intelligence din Științe Sociale* pentru a desemna produsele informative rezultate din analiza specifică domeniilor de interes ale științelor sociale

importanță majoră și în cadrul operațiilor militare convenționale; SOCINT permite depășirea barierelor subiectivității în analiza factorului uman în folosirea bazei unor proceduri și instrumente științifice consacrate în cadrul științelor sociale, toate acestea contribuind la mai bună înțelegere a mediului operațional;

5. **tehnologia este esențială în prelucrarea afluxului enorm de date și informații;** analiza asistată de mijloace tehnice permite stocarea, organizarea, selectarea, identificarea și prelucrarea facilă a datelor, în timp scurt și în mod obiectiv;
6. **analiza de Intelligence este o profesie în sine și trebuie structurată și tratată ca atare;** aceasta presupune o pregătire formală solidă, certificată, completată cu educația continuă, standarde performante, o metodologie de lucru validată și instrumente adecvate.

Caracteristicile amenințărilor emergente la adresa securității, indiferent de nivel – strategic, operațional sau tactic – determină adaptarea și specializarea compartimentelor funcționale la nivel de analiză. Vectorii amenințărilor internaționale, provocările la nivel operațional sau adversarii în câmpul tactic dovedesc noi valențe operaționale legate de mobilitate, acțiunea clandestină sau acoperită, accesul la resurse de orice natură, de la informații la tehnologie avansată, opțiuni de comunicare, etc.

În armata SUA, la nivelul unităților expediționare, există programe de dezvoltare a capacităților analitice la nivel tactic – necesitate izvorâtă din experiența acumulată și lecțiile învățate în teatrele de operații în ultimul deceniu. Analiza la nivel tactic – în special în operațiile în care centrul de greutate migrează către zona socială – trebuie să acopere toate elementele mediului operațional, integrate în vederea înțelegerii aspectelor umane în multidimensionalitatea lor, mediul instituțional formal și informal, logica inter-relaționării și fundamentarea rețelelor umane, stabilirea criteriilor deviaționiste de la norma locală, profilul oponentului (nevoi, percepții, reprezentări, motivații), etc.

În mod tradițional, câmpul de interes al SOCINT – din perspectivă analitică, cu acoperire sectorială (pe un anumit domeniu) sau teritorială (analiza integrată a aspectelor socio-culturale într-un sistem teritorial) – constituie apanajul științelor umane, exploatate ca atare (nu în scop de a produce Intelligence) în mediul academic. Începutul secolului a adus cu sine și recunoașterea valențelor de Intelligence ale produselor analitice ale diferitor ”think-tank”uri, adevărate exponențe ale societății informaționale, bazate pe cunoaștere. Acestea nu se limitează doar la SOCINT, ci acoperă întreg spectrul analitic, la orice nivel de referință. Bineînțeles, cartea ”independenței” funcționale pe care o îmbracă unele societăți, ca exponenți ai societății civile, trebuie asumată cu precauțiile de rigoare. Cu toate acestea, importanța industriei civile în domeniul Intelligence nu este deloc de neglijat – după cum vom arăta într-o altă temă.

Instrumentele inovatoare menite să îmbunătățească capacitatea Intelligence la nivel tactic, atât în ce privește colectarea de date și informații, cât și prelucrarea acestora la nivel tactic în vederea obținerii de Intelligence acționabil, sunt acoperite de diferite proceduri legate de: selectarea țintelor (matrici de lucru menite să sincronizeze ritmul operațional cu emergența datelor legate de mobilitatea țintelor), angajarea liderilor cheie (formate standard de raportare a datelor de interes provenite de la liderii comunităților umane), amenințările reprezentate de Dispozitivele Explosive Improvizate (DEI) (metodologii specifice de colectare și prelucrare a datelor, menite să determine un anumit nivel de predictibilitatea a gradului de risc în timp și spațiu), analiza datelor provenite din rapoartele privind angajarea forțelor inamice (în vederea determinării tehnicilor, tacticilor și procedurilor inamice și a eficienței acestora), determinarea profilurilor multidimensionale ale grupărilor insurgente (incluzând elementele de suport, capacitățile, ramificațiile intra și inter-naționale, elemente de fundamentare psiho-socială a acțiunii acestora).

Inovațiile metodologice în domeniul analitic, odată validate, trebuie preluate și integrate în vederea standardizării, atât pentru a îmbunătăți calitatea actului de procesare a informației și a asigura compatibilitatea/ interoperabilitatea, cât și pentru a evita redundanțele.

Produsele analitice sunt puse la dispoziția consumatorilor sub forma materialelor scrise (informări, sumare, actualizări, prognoze, avertizări) sau în cadrul briefingurilor de informare. În vederea asigurării utilității produselor analitice, acestea trebuie să asigure înțelegerea materialului prezentat - cerință ce reclamă din partea analistului o bună cunoaștere a mecanismelor psihologice ale cognitivității umane¹.

La final, analistul trebuie să asigure generarea unei duble perspective a cunoașterii:

- *insight* (înțelegerea cauzalității evenimentelor);
- *foresight* (identificarea-anticiparea cursurilor de acțiune viitoare).

Tehnologia în sprijinul analizei de Intelligence. IBM i2 Intelligence Analysis Platform

După cum am arătat anterior, condițiile concrete ale desfășurării activității de analiză necesită sprijinul cu tehnologie în vederea rezolvării problemelor legate de stocarea, selectarea, prelucrarea și vizualizarea materialului informativ.

IBM i2 Intelligence Analysis Platform reprezintă o interfață analitică extensibilă, scalabilă, orientată spre serviciu, destinată furnizării organizațiilor beneficiare accesul la produse de Intelligence în conformitate cu nevoile acestora². Dezvoltat de către compania I-2 Ltd. din Cambridge sub denumirea "I2 Analyst Notebook", acesta a devenit un produs IBM din 2011, odată cu cumpărarea I-2 Ltd de către gigantul informatic.

Programul permite modelarea complexă, în baza unui suport grafic expresiv, a tuturor acțiunilor și relaționării în cadrul rețelelor umane (prin colectarea, colarea și consolidarea datelor din multiple surse), în scopul asigurării vizualizării și analizei unui volum mare de date.

Instrumentele intuitive de analiză vizuală (figura 6.4) permit perspective elaborate asupra detaliilor specifice structurilor și evenimentelor analizate, contabilizând actorii în totalitatea lor și stabilind rețelele de interdependență dintre aceștia.

¹ de exemplu, pentru persoanele orientate perceptiv către receptorul vizual, reprezentarea grafică (geospațială) a datelor sprijină în mod decisiv nivelul de înțelegere

² IBM Software (2012) *IBM i2 Intelligence Analysis Platform*

Beyond Operation Chameleon - The International Network in the Trade of Reptiles and Wildlife

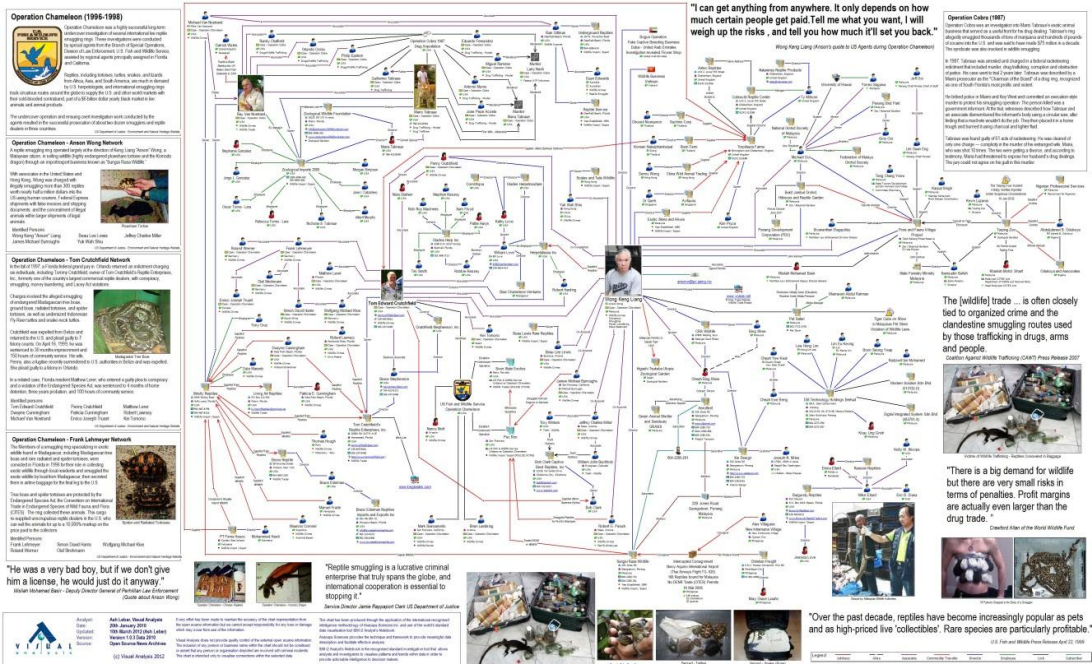


Figura 6.4 Diagramă i2 folosită în operația Cameleonul (demascarea unei rețele de traficanți de reptile)¹

Mai mult, reprezentarea geospațială a datelor și informațiilor de care se dispune (figura 6.5) sporește utilitatea acestei platforme în cadrul procesului de analiză, fiind deosebit de utilă în determinarea parametrilor calitativi ai produsului final.

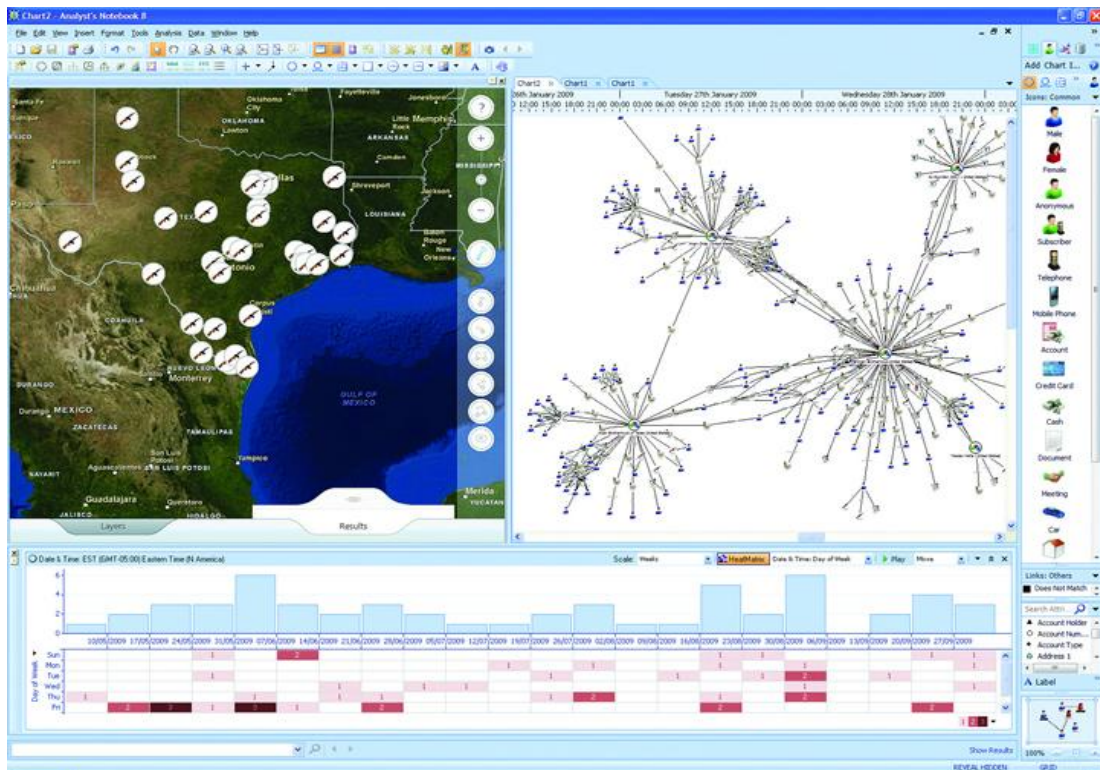


Figura 6.5 Reprezentare geospațială în i2²

¹<https://www.visualanalysis.com/Images/ANB/CHARTS/Beyond%20Operation%20Chameleon.jpg>

²<http://www-03.ibm.com/software/products/en/analysts-notebook-esri/>

Modalitatea de prezentare a datelor este multiplă, permițând reprezentări prindiarame, hărți, tabele, fotografii, etc. Cerința de asigurare a colaborării cu alte sisteme este la rândul ei îndeplinită prin capacitățile de interconectare securizată pe care programul le permite.

Concluzii

La nivel organizațional, adaptarea la schimbările dictate de realitate nu este un proces natural, care survine de la sine. Schimbarea (transformarea) capacității este un proces care trebuie bine gândit și planificat, evaluat și corectat în permanență (Frățilă, 2008), inclusiv în ce privește disciplina Intelligence.

În ce privește analiza de Intelligence, dincolo de activitățile consacrate de experiența națională și internațională în domeniu, se observă o serie de aspecte ce pot să contribuie la îmbunătățirea performanțelor în materie:

- viziunea și claritatea beneficiarilor în orientarea efortului de colectare a informațiilor (calitatea leadershipului);
- coordonarea și cooperarea intra și interinstituțională, pe plan național și internațional;
- tehnologizarea proceselor analitice;
- instruirea și motivarea personalului.

Bibliografie

1. ***, *Doctrina națională a informațiilor pentru securitate* (2004) Editura S.R.I. București, în <http://www.sri.ro/doctrina-nationala-a-informatiilor-pentru-securitate.html>
2. 21st Century Marine Expeditionary Intelligence Analysis (MEIA-21), *Modernizing Tactical Military Intelligence Analysis*, September 2011, <http://www.phibetaiota.net/2011/09/21st-century-marine-expeditionary-analysis-meia-21-modernizing-tactical-military-intelligence-analysis/>
3. BUCIUMAN, Marian (2004) *Managementul crizelor - modalitate eficientă de gestionare a surselor de instabilitate la nivel global și regional*, p. 97-107, în MOȘTOFLEI, Constantin (coordonator), *Surse de instabilitate la nivel global și regional. Implicații pentru România, A IV-a Sesiune anuală de comunicări științifice*, Editura Universității Naționale de Apărare, București
4. BUZAN, Barry (2000) *Popoarele, statele și teama. O agendă pentru studii de securitate internațională în epoca de după Războiul Rece*, Editura Cartier, Chișinău
5. FRĂȚILĂ, Ovidiu Ilie (2008) *Capacitatea de adaptare a analizei de „Intelligence” - factor determinant în condițiile evoluției actuale a mediului de securitate*, în MOȘTOFLEI, Constantin (coord.) (2008) *Politici și strategii în gestionarea conflictualității*, Editura Universității Naționale de Apărare „Carol I”
6. HEUER, Richards J. Jr. (1999) *Psychology of Intelligence Analysis. Chapter 2. Perception: Why Can't We See What Is There To Be Seen?*, History Staff, Center for the Study of Intelligence, Central Intelligence Agency, în <http://www.au.af.mil/au/awc/awcgate/psych-intel/art5.html>
7. IBM Software (2012) *IBM i2 Intelligence Analysis Platform*
8. IOAN, Marian (2008) *Bolile analizei de Intelligence*, în *Pulsul geostrategic*, Nr.37, 20 Septembrie
9. JDP 2-00 (3rd Edition) *Understanding and Intelligence in Support of Joint Operations*, capitolul 5, 2011
10. NIȚU, Ionel (coordonator) (2011) *Ghidul analistului de intelligence: compendiu pentru analiștii debutanți*, Editura Academiei Naționale de Informații „Mihai Viteazul”, București
11. PĂRLOG, Adrieian (2008) *Procesul de analiză de „intelligence”, componentă a sistemului de securitate*, în MOȘTOFLEI, Constantin (coord.) (2008) *Politici și strategii în gestionarea conflictualității*, Editura Universității Naționale de Apărare „Carol I”
12. SARCINSCHI, Alexandra (2005) *Elemente noi în studiul securității naționale și internaționale*, Editura Universității Naționale de Apărare, București, în http://cssas.unap.ro/ro/pdf_studii/elemente_noi_in_studiul_securitatii_nationale.pdf
13. ȘERBAN, Mihai (2008) *Unele aspecte referitoare la importanța analizei în mediul intelligence*, în MOȘTOFLEI, Constantin (coord.) (2008) *Politici și strategii în gestionarea conflictualității*, Editura Universității Naționale de Apărare „Carol I”
14. The Development, Concepts and Doctrine Centre, UK Ministry of Defence, *Joint Doctrine Publication 04 (JDP 04) (2010) Understanding*, Shrivenham Swindon, Wiltshire, UK
15. TULICĂ, Mircea (2009) *Intelligence și securitate* (note de curs), Iași

16. US Marine Corps, *Concepts and programs 2013*, America's Expeditionary Force in Readiness, in <http://www.hqmc.marines.mil/Portals/142/Docs/USMCCP2013flipbook/USMC%20CP13%20Final.pdf>
17. WITLIN, Lauren (2008) Of Note: Mirror-Imaging and Its Dangers (excerpt). SAIS Review (The Johns Hopkins University Press), 28 (1): 89–90. doi:10.1353/sais.2008.0024
18. <http://azizaizmargari.files.wordpress.com/2011/08/critical-thinking-image.gif>
19. <http://www.oxforddictionaries.com/definition/english/judgement>
20. <http://www-03.ibm.com/software/products/en/analysts-notebook-esri/>
21. <https://www.visualanalysis.com/Images/ANB/CHARTS/Beyond%20Operation%20Chameleon.jpg>

CAPITOLUL 7. INTELLIGENCE PRIVAT – DE LA SECURITATE LA COMPETITIVITATE PRIN INTELLIGENCE

Securitatea și mediul privat

Conexiunile dintre instituțiile din sectorul de securitate și diferiți actori ai mediului civil nu reprezintă nimic nou. Aceștia din urmă au constituit de foarte mult timp principalii parteneri în materie de dotare cu echipamente și tehnică (industria militară), furnizarea de servicii logistice (transport, mentenanță, hrană, servicii poștale și de curierat, etc.), furnizarea de soluții de comunicații și informatică sau constituirea unor forumuri de dezbatere asupra unor probleme de interes politico-militare.

Dezvoltarea paradigmei securității a dus la conștientizarea faptului că noile câmpuri de confruntare ale intereselor naționale (economia, accesul la resurse, politicile actorilor internaționali non-guvernamentali și mobilitatea financiară/investițională, mediul cibernetic, controlul informației, amenințările asimetrice, etc.) solicită guvernele dincolo de capacitățile militare de care acestea dispun (aliniate cerințelor de apărare națională). Securitatea, ca fundamentare conceptuală, acoperă toate aspectele relevante pentru funcționarea mecanismelor de dezvoltare ale statului, iar acest fapt reclamă o specializare suplimentară a capacităților de prevenire, protecție și evoluție a proceselor subsumate acestora.

Sub imperiul globalizării, apărarea și securitatea au încetat să mai fie apanajul construcției exclusive a statelor, indiferent de puterea și de disponibilitățile militare de care dispun; mai mult, cerințele specifice în materie de securitate depășesc limitele sectorului instituțional consacrat, recurgând la resurse și expertiza disponibilă pe piața liberă. Noile realități și cerințe de natură securitară au dus la o adevărată revoluție în afacerile militare/zona serviciilor de securitate, care nu este doar tehnologică și informațională, ci și una de natură filozofică și managerială, care presupune noi scopuri și obiective politice pentru acțiunea militară sau civil-militară (abordarea comprehensivă), noi concepte strategice, operative, tactice precum și noi resurse (Ungureanu, 2009). Pentru mediul militar, unul dintre aspectele de referință este externalizarea unor servicii (*"outsourcing"*), care poate să acopere un spectru larg de servicii specifice (consultanță, avertizarea timpurie, logistica, protecția forței, Intelligence, etc.).

Apariția acestor capacități private poate fi interpretată și din perspectiva reducerilor de resurse în domeniul sectorului de securitate guvernamental (ca efect al crizei economice), fapt ce a dus la dificultăți în îndeplinirea unora din sarcinile specifice, oferind astfel o nișă de oportunitate.

Privatizarea securității în accepțiunea sa actuală în cadrul pieței globale este asociată cu orientările manifestate în SUA în virtutea noii paradigme a securității și a liberalismului economic promovat de școala de la Chicago. Influența SUA în materie, cooperarea și schimbul de know-how în cadrul organizațiilor de securitate (ex. NATO) și oportunitățile deschise de globalizare au permis generalizarea practicilor de externalizare a sarcinilor de securitate.

N. Klein pune în evidență circumstanțele specifice ale implicării mediului privat în domeniul securității în SUA, depășind sfera inițial limitată la "activități neesențiale" și alunecând, treptat, spre sarcini din întreg spectrul operațiilor militare: planificarea și instruirea trupelor, operațiuni armate, culegerea de informații, interogarea deținuților, analiza de Intelligence, servicii de protecția forței, etc (Klein, 2008).

Influențele în abordarea laturii lucrative a securității se regăsesc în ambele sensuri, atunci când facem o comparație între nivelurile de capacități implicate. Pe de o parte, în mediul organizațiilor de securitate guvernamentale se observă un trend crescător către alocarea de posturi personalului civil și chiar schimbarea calității de funcționar public civil cu

statutul de entitate contractuală ("contractor"), în virtutea unor criterii de flexibilitate și eficiență în domeniul resurselor umane, fapt definit de Charles Moskos jr. ca "dezinstituționalizare a birocrăției civile militare" (în Callaghan și Kernic, 2004) – un pas adoptat ca model managerial corporatist, dar totodată o recunoașterea formală a calității private a serviciilor specifice oferite de către contractanți. Pe de altă parte, în mediul non-militar se observă o creștere a potențialului combativ (nu numai ca dotare cu tehnică și echipamente specifice, dar și ca resursă umană instruită, planificare și tehnici, tactici și proceduri de executare a activităților după model militar, etc.), ca urmare a accesibilității crescute pe piață a acestora și a transferului de know-how în condițiile unui cadru legislativ permisiv.

Privatizarea unor servicii în domeniul securității – calificată ca o adevărată "industrie" în domeniu (Han, 2009) – a dus și la conturarea unei piețe distincte, unde cererea vine din partea clienților selectați atât din mediul civil (persoane private, companii civile, etc.), cât și la nivelul organizațiilor guvernamentale - agenții naționale, organizații internaționale, forțe ale ministerelor de resort în domeniul apărării și siguranței naționale, etc.

Companiile/contractorii privați de securitate (Private Security Companies/Contractors – PSC) sunt întreprinderi ce furnizează servicii de securitate (militarizate sau nu) și expertiză clienților publici și privați (de la servicii de pază și patrulare până la prevenirea unor activități neautorizate, controlul accesului, prevenirea și detectarea furturilor). Acestea sunt relativ comune în spațiul public și diferă ca esență de companiile (firmele) private militare (PMC/PMF) (Singer, 2005, 119-132), care prestează servicii profesionale similare celor specifice forțelor militare sau de poliție guvernamentale (incluzând sarcinile de securitate), la scara pe care capacitățile de care dispun o permite.

Oferta de servicii a acestor companii de securitate este fie prezentată în mod selectiv clienților-țintă (în cadrul unor comunități de interes), ca oferte personalizate, fie ca servicii deschise publicului, fără restricții (ori o combinație între cele două variante). Pentru a-și prezenta oferta, firme private de securitate sunt prezente alături de companiile din domeniul industriei de apărare în cadrul a diferite evenimente (de ex. Counter-Terror Expo¹, Expoziția și Conferința pe tema Forțelor din Operațiunile Speciale – SOFEX/Special Operations Forces Exhibition and Conference², etc.). Conexiunile pe care liderii acestor firme le au la nivel guvernamental sau în cadrul sectorului formal de securitate (de unde majoritatea provin³) marchează o oarecare apetență a parteneriatului cu fostele entități de apartenență; oricum, orientarea spre profit a acestor "business"-uri primează în procesul de selectare a clientelei, în baza principiilor economiei de piață.

Serviciile oferite de aceste companii acoperă o largă plajă de referință, pornind de la protecție, recuperarea de bunuri, extracția din zone de risc, căutare și recuperare, negociere în situații critice, servicii de instruire pentru operațiuni defensive și ofensive, consiliere și mentorat, servicii de intelligence (culegere de informații, analiză), investigații și contrainformații, securitatea informațiilor, sprijin cu tehnică specifică, etc., replicând practic – în versiune privată – spectrul de activități și funcțiuni specifice ale organelor de stat din domeniul securității. PMC au fost solicitate în vederea securizării zonele de exploatare a resurselor naturale și a facilităților de prelucrare, a căilor de transport a hidrocarburilor, protecția vaselor comerciale împotriva pirateriei, protejarea contractorilor civili în cadrul proiectelor de reconstrucție în zone de criză, protecția oficialilor guvernamentali, pilotarea

¹ <http://www.counterterrorexp.com/>

² <http://www.sofexjordan.com/what.shtm>

³ Aria de recrutare a personalului ce încadrează astfel de companii vizează foști profesioniști în operațiuni speciale, apărare, spionaj, instituții de aplicare a legii, oameni cu experiență practică, abilități și capacități excepționale în diferite domenii de interes

avioanelor de recunoașteri, mentenanța aparaturii speciale, dezvoltarea de software pentru monitorizarea Internetului, etc.¹

Cu toate acestea, implicarea PMC în executarea unor funcțiuni cu caracter militar – de multe ori un compromis menit să asigure o preluare de riscuri politice și diplomatice pe care guvernele, la nivel strategic, nu și le permit, ori pur și simplu o suplimentare a capabilităților trupelor dislocate într-o zonă de criză – a fost, în general, aspru criticată datorită abuzurilor, activității în zona gri a legalității, lipsei unui control real și a responsabilității²; în multe situații, personalul acestor firme private a fost calificat ca fiind, în fapt, mercenarii lumii de azi (Făinaru, 2008).

PMC sunt mult mai subtile când vine vorba de statutul angajaților. Practic, două companii - Executive Outcomes și Sandline - sunt singurele PMC cunoscute ca fiind implicate în lupta efectivă (Blain); în mod general, PMC își protejează afacerile prin asigurarea legitimității acțiunilor pe care le întreprind și complianța angajaților cu coduri etice stricte, care să elimine posibilitatea oricărui abuz la adresa drepturilor omului³. Acest fapt nu constituie o piedică în calea derapajelor (a se vedea incidentele legate de Blackwater în Irak – Scahill, 2009) sau a accidentelor nefericite.

O scurtă revedere a semnificației termenului de ”mercenar” este utilă pentru a face o judecată de valoare în ce privește statutul personalului firmelor private din domeniul securității. Convenția internațională împotriva recrutării, folosirii, finanțării și instruirii mercenarilor (rezoluția ONU nr. 44/34 din 4 decembrie 1989) definește condițiile pe care o persoană trebuie să le întrunească pentru a fi considerată mercenar⁴:

- a. este în mod special recrutată local sau în afara țării cu scopul de a lupta într-un conflict armat;
- b. este motivată în a lua parte la ostilități eminamente de câștigul personal și, în fapt, i se promite de către o parte la conflict sau în numele acesteia, o compensație materială excesiv mai mare decât cea promisă sau plătită combatanților de grad și funcție similară în forțele armate ale respectivei părți;
- c. nu este de naționalitatea unei părți la conflict și nici rezidentă a teritoriului controlat de către o parte la conflict;
- d. nu este membru al forțelor armate ale unei părți la conflict;
- e. nu este trimis de un stat care nu este parte la conflict în funcție oficială ca membru al forțelor sale armate.

De asemenea, Convenția asimilează mercenarilor orice persoană care, în orice altă situație:

- a. este în mod special recrutată local sau în afara țării cu scopul de a participa în acte de violență concertate cu scopul:
 - de a răsturna un guvern sau să submineze ordinea constituțională a unui stat;
 - de a submina integritatea teritorială a unui stat;
- b. este motivată în a lua parte în mod esențial prin dorința unui câștig personal semnificativ, ca urmare a promisiunii sau plății compensației materiale;
- c. nu este de naționalitatea și nici rezidentă a Statului împotriva căruia un astfel de act este direcționat;

¹<http://www.colectivodeabogados.org/PRIVATE-SECURITY-TRANSNATIONAL>

²a se vede scandalul Blackwater în Irak (Scahill, 2009)

³Un rol important în coordonarea activităților de lobby la nivel internațional pentru implicarea firmelor militare private în acțiuni de menținere a păcii, îl are asociația comercială a acestor firme, I.P.O.A. (Asociația Internațională pentru Operațiuni de Pace). I.P.O.A. se prezintă ca o organizație alcătuită din „cele mai profesionale companii”, care își desfășoară activitatea în baza unui cod de comportament redactat „cu ajutorul a zeci de organizații internaționale și non-guvernamentale, avocați ai drepturilor omului și oameni de știință” și care acționează în „industria de pace și stabilitate” (Scahill, 2009, 374).

⁴<http://www.un.org/documents/ga/res/44/a44r034.htm>

- d. nu este trimis de un stat în funcție oficială;
- e. nu este membru al forțelor armate ale Statului pe teritoriul căruia are loc actul.

Disensiunile legate de interpretarea Convenției și problemele determinate de activitățile militarizate ale firmelor private în diferite zone de criză a determinat stabilirea unui Grup de lucru al UNHCR, în 2005, în vederea reglementării folosirii mercenarilor. Acesta a stabilit faptul că anumite companii private de securitate ce operează în zone de conflict armat sunt angajate în "noi forme de mercenariat"¹ (cu referire la PMC în Irak și Afganistan), solicitând comunității internaționale măsuri în vederea reglementării activității acestora.

Grupul a elaborat un proiect pentru o nouă Convenție Internațională privind Reglementarea, Răspunderea și Monitorizarea Companiilor Militare sau de Securitate private², a treia întrunire a acestuia fiind programată în iulie 2014³. Draftul Convenției limitează atribuțiile și responsabilitățile PMC/PSC, prevăzând că statele trebuie să păstreze monopolul în ce privește uzul forței, fiind responsabile atât pentru activitățile forțelor armate naționale, cât și pentru grupările armate private ce operează cu licența sau în baza unui contract cu statul respectiv. Printre activitățile prohibite ca serviciu atribuitabil contractorilor privați, denumite generic "funcțiuni fundamentale ale statului", alături de uzul forței, operațiile militare, luarea de prizonieri, activitatea normativă și forțele de poliție, se regăsesc: spionajul, Intelligence și exercitarea puterii de arestare și detenție (incluzând interogarea persoanelor reținute)⁴.

Firmele private militare/de securitate și prestările de servicii în spectrul Intelligence

Prima PMC în accepțiune modernă este considerată Watch Guard International, fondată în 1965 de veteranul forțelor SAS (Special Air Service) britanice, sir David Stirling și John Woodhouse (Crowel și alții, 2011) și care a operat în Zambia și Sierra Leone, furnizând echipe de instruire și consultanță în materie de securitate.

DynCorp a fost fondată în 1946 ca furnizor de tehnologie și sprijin logistic pentru armata SUA, ulterior dezvoltându-și spectrul de servicii care includ, la momentul actual, și soluții pentru Intelligence⁵:

- educarea, instruirea și certificarea profesioniștilor în Intelligence;
- îmbunătățirea activităților de colectare și analiză în vederea elaborării de produse de Intelligence în sprijinul proceselor decizionale;
- oferirea de asistență în domeniul Intelligence prin servicii asigurate "la orice locație și în orice condiții".

Din 2010, odată cu achiziționarea de către companie a Phoenix Consulting Group, DynCorp International oferă prin Centrul de Instruire Phoenix un bogat pachet de cursuri specifice domeniului informațiilor militare și al contrainformațiilor, parte din ele certificate de Departamentul Apărării al SUA⁶. Acestea acoperă aspecte privitoare la: tehnici de obținere a informațiilor de la surse umane, metodologia operațiilor cu surse, sprijinul analitic pentru HUMINT, validarea surselor, aspecte de bază în domeniul contrainformațiilor, debriefing la nivel strategic, elicitare, interogare, tehnici de stabilire a profilului psihologic, managementul surselor, detectarea supravegherii, etc.

¹ Comunicat de presă al ONU, *Private Security Companies Engaging In New Forms of Mercenary Activity*, UN Working Group (6 Nov. 2007)

²<http://mgimo.ru/files/121626/draft.pdf>

³<http://www.ohchr.org/EN/HRBodies/HRC/WGMilitary/Pages/OEIWGMilitaryIndex.aspx>

⁴<http://mgimo.ru/files/121626/draft.pdf>

⁵<http://www.dyn-intl.com/what-we-do/intelligence-and-security/>

⁶http://www.dyn-intl.com/media/phoenix_training_center_catalog_2013.pdf

Michael Smith definește agențiile private din domeniul Intelligence ca organizații dedicate colectării și analizei informațiilor, cel mai adesea prin evaluarea surselor publice și prin cooperarea cu alte instituții (Smith, 2008). Produsele acestora sunt fie sectoriale (acoperind probleme din domenii de interes la nivelul diferitelor servicii guvernamentale sau din domeniul privat), fie concentrate asupra analizei comprehensive a sistemelor teritoriale regionale sau chiar la nivel global.

SUA și Marea Britanie sunt în topul statelor în care își desfășoară activitatea astfel de companii, dintre care menționăm doar câteva: Kroll Inc., Smith Brandon International, Inc., Stratfor, Booz Allen Hamilton, AEGIS, Control Risks Group, GK Sierra, Hakluyt & Company, precum și ASI Group, Global Strategies Group, Global Source, iJET, International Regional Security Agency, Jane's Information Group, NC4, Olive Group, Secure Solutions International SIASS - Specialist Intelligence and Security Services, The Steele Foundation, TranSecur, World-Check, SITE (Michaletos, 2009) etc.

Informațiile publice despre aceste companii variază, cele oferite pe websiteurile oficiale fiind deseori limitate la datele de contact; oportunități suplimentare de informare le oferă presa de investigație, care citează cazuri (de regulă scandaluri) în care astfel de firme sunt implicate.

De exemplu, Holdingham Group este compania mamă a unui grup de firme care își desfășoară activitatea în domeniul consultanței și a informațiilor de interes strategic, la nivel global – Hakluyt¹ și Pelorus². Dacă Hakluyt (cunoscută ca fiind dedicată) se limitează în a furniza doar datele de contact ale sediului central din Londra și ale subsidiarelor din SUA, Japonia și Singapore. În schimb, Pelorus face public obiectul de activitate – consultanța în domeniul afacerilor/ managementului, în sprijinul deciziilor investiționale – și selectivitatea în alegerea clientelei, în condiții de complianță cu reglementările internaționale specifice.

Alte companii sunt mult mai generoase în a oferi detalii despre activitatea pe care o desfășoară, în vederea asigurării unei selecții facile de către clienții potențiali a gamei de servicii căutate.

Control Risks Group³ este o companie ce activează în domeniul controlului riscurilor politice, de securitate și integritate (furnizând servicii de consultanță, audit anti-corupție, instruire specifică, căutare de date pe platforme on-line, analiză de risc, sprijin de securitate și gestionarea situațiilor de risc, rezolvarea litigiilor internaționale, răspunsul în caz de incident, etc).

Aegis Defence Services⁴ este o companie de anvergură în domeniul securității și managementului situațiilor de risc, care are în portofoliul de clienți guverne, agenții internaționale și firme corporatiste. În vederea asigurării sarcinilor specifice de securitate, compania dispune de contacte în mediile de interes, precum și de echipe tactice de analiză, în măsură să furnizeze informații care să fie incluse în materialele privind avertizarea situațională sau evaluările zonelor de interes, facilitând totodată schimbul de informații cu alte agenții.

Booz Allen Hamilton Inc.⁵ este una dintre cele mai vechi companii de pe glob în domeniul consultanței de management; aceasta și-a dezvoltat în timp oferta de produse, furnizând și servicii de securitate și tehnologie agențiilor guvernamentale în domeniul securității și al apărării/ Intelligence. Notorietatea firmei a devenit publică odată cu scandalul Snowden - angajat al Booz Allen Hamilton Inc. – care a divulgat date secrete privind

¹<http://www.hakluyt.co.uk/>

²<http://www.pelorus-research.com/about>

³<http://www.controlrisks.com/>

⁴<http://www.aegisworld.com/>

⁵<http://www.boozallen.com/>

programul clandestin al Agenției Naționale de Securitate a SUA folosit pentru supravegherea în masă

Stratfor (Strategic Forecasting, Inc.)¹, think-tank creat și condus de George Friedman, pune la dispoziția publicului larg și a clienților² săi produse analitice și prognoze geopolitice la nivel strategic, în măsură să asigure o mai bună înțelegere a dinamicii fenomenului securității internaționale și să sprijine identificarea oportunităților de acțiune. Resursele de care firma dispune în acest sens, pe lângă procesarea OSINT, sunt reprezentate de o rețea globală de contacte/ experți regionali, parteneriate cu peste 500 de companii, institute, ONGuri etc., analiști geopolitici de valoare recunoscută și o metodologie de lucru menită să asigure calitatea produselor, dincolo de orice agendă politică sau influență națională.

Smith Brandon International³ este o firmă specializată în investigații și consultanță de risc ce oferă, în condiții de confidențialitate, servicii de analiză politică, investigații de afaceri la nivel global, investigații corporatiste, evaluarea și reducerea nivelului de risc, intelligence de afaceri. Aceste servicii se bazează pe o rețea de comunități din mediul diplomatic, al afacerilor și de Intelligence cu extindere pe continentele americane, Orientul Mijlociu, Asia și Africa.

Cu obiect de activitate asemănător, serviciile oferite de compania Kroll⁴ acoperă: investigații financiare, investigații tranzacționale, Intelligence de afaceri, recuperarea de date, evaluarea amenințărilor și a vulnerabilităților, securitatea fizică, planificarea securității, dezvoltarea de politici și proceduri, studii de procesare, etc.

Compania israeliană Terrogence⁵ este ceva mai explicită în ce privește metodologia folosită în elaborarea serviciilor și produselor sale, explorând capacități de pionierat în ce privește culegerea de informații din surse umane prin intermediul platformelor online (Virtual HUMINT™), Intelligence rezultat în urma exploatarea oportunităților pasive și active oferite de rețele (Web Intelligence/WEBINT Services&Technology) și OSINT, cu precădere în sprijinul eforturilor de luptă împotriva dispozitivelor explozive improvizate (la nivel tactic), contrainformațiilor în domeniul cibernetic, diplomației în mediul digital, etc.

”Virtual HUMINT™” este o metodologie patentată de Terrogence, care presupune cultivarea și operarea de identități virtuale în spațiul cibernetic, active în platforme de socializare, unde urmăresc câștigarea încrederii persoanelor de interes, formarea rețelei de surse și colectarea de informații prin diferite tehnici.

Detalii interesante despre activitatea firmelor private din domeniul securității, dar și alte aspecte din domeniul larg al securității, de interes personal, sunt disponibile în revista dedicată acestora, ”The Circuit”, on-line la <http://www.circuit-magazine.com/>.

Analiza mediului de securitate și avertizarea timpurie

Înțelegerea mediului de securitate în complexitatea sa reprezintă o necesitate absolută pentru factorii de decizie politici și militari. Dimensiunile acestuia, fenomenologia specifică și manifestările de stare reprezintă cadrul de configurarea sistemului strategic global, care se reflectă și se condiționează reciproc cu strategiile regionale și naționale, acestea din urmă asigurând instrumentele teoretice, practice și metodologice politicilor naționale, pentru realizarea obiectivelor propuse.

Avertizarea timpurie este un proces sistematic ce evaluează și măsoară în timp oportun situațiile de risc în vederea facilitării acțiunilor preemptive menite să minimizeze impactul

¹<http://www.stratfor.com/>

²Subscriși online sau contractanți ai serviciilor de consultanță

³<http://www.smithbrandon.com/>

⁴www.kroll.com

⁵<http://www.terrogence.com/>

hazardelor asupra securității. De aici, un sistem de avertizare timpurie reprezintă un lanț de sisteme de comunicare a informației, cuprinzând subsisteme de receptare, detectare, decizie și selectare, în măsură să anticipeze și să semnaleze perturbări ce afectează în mod negativ stabilitatea în materie de securitate, în condiții în care să asigure suficient timp sistemelor de răspuns pentru a-și pregăti resursele și acțiunile de răspuns în vederea minimizării impactului acțiunilor/evenimentelor/fenomenelor destabilizatoare (după Waidyanatha, 2010).

Un sistem de avertizare timpurie focalizat asupra comunităților umane trebuie să cuprindă patru elemente cheie¹:

- cunoașterea riscurilor;
- monitorizarea (ce presupune existența raportorilor din teren), analiza (cantitativă și calitativă, în baza unor surse de informare multiple, incluzând sursele deschise) și anticiparea hazardelor;
- comunicarea și diseminarea alertei și avertizărilor (rapoarte regulate și actualizate);
- capacități locale de răspuns la avertizări și/sau legături consolidate cu mecanisme adecvate de răspuns.

După A. Schmid, sistemele de avertizare timpurie presupun colectarea organizată, regulată și sistematizată și analiza informațiilor provenind din zonele de criză în scopul:

- a) anticipării escaladării unui conflict violent,
- b) dezvoltării de răspunsuri strategice la crizele respective și
- c) prezentării opțiunilor actorilor critici în scop decizional (Schmid, 1998).

Un istoric al evoluției sistemelor de avertizare timpurie este făcut de R. Ștefănescu, care scoate în evidență o serie de repere ce au stat la baza unor astfel de inițiative în plan interguvernamental (ex. Oficiul pentru Cercetarea și Colectarea de Informații – ORCI la ONU, inițiativele UNOCHA – Biroul Națiunilor Unite pentru Coordonarea Problemelor Umanitare, etc.), la nivel academic (ex. *”The Minorities at Risk Data Generation and Management Project”*) sau în cadul societății civile, la nivel de ONG (primul de acest fel fiind International Alert, în 1985) (Ștefănescu, 2009)². Cercetătoarea distinge 3 generații de sisteme de avertizare timpurie:

- generația anilor ‘90, categorie ce își desfășoară activitatea de analiză la sediu, exclusiv în baza analizei datelor din surse deschise (OSINT), fără mecanisme de răspuns timpuriu (ex. GEDS – Global Events Data System, sistemul german BMZ³, sistemul de indicatori utilizat de Comisia Europeană);
- sistemele inițiate în perioada anului 2000, ce folosesc, pe lângă OSINT, resurse de monitorizare în zonele de criză potențială, executând activitatea de analiză la sediu, de asemenea fără mecanisme de răspuns timpuriu (ex. ICG - International Crisis Group, EAWARN - Network for the Ethnological Monitoring and Early Warning of Conflict, FAST international - inițiativă a Swisspeace⁴);
- sistemele de generația a treia, cu sediul în zona de conflict, unde se desfășoară atât monitorizarea cât și analiza; activitatea de colectare a datelor implică societatea civilă și administrația regională și au legături cu mecanisme instituționale de răspuns (ex.

¹<http://www.preventionweb.net/english/professional/terminology/v.php?id=478>

²R. Ștefănescu menționează ca repere de debut ale conceptualizării EW: Liniile Directoare ale OECD – DAC (Organization for Economic Cooperation and Development - Development Assistance Committee) pentru Conflict, Pace, Dezvoltare și Cooperare (1997); Raportul final al Comisiei Carnegie pentru Prevenirea Conflictelor Mortale (1997); Raportul Brahimi (2000); Declarația de la Khartoum la nivel sub-regional a șefilor de state IGAD (Autoritatea Interguvernamentală pentru Dezvoltare) unde se pun bazele CEWARN (Conflict Early Warning and Response Mechanism); Raportul Secretarului General ONU referitor la prevenirea conflictelor armate (2001); Comunicarea din 2001 a Comisiei Europene cu privire la prevenirea conflictelor (Ștefănescu, 2009).

³Bundesministerium für wirtschaftliche Zusammenarbeit (Ministerul Federal pentru Cooperare Economică)

⁴<http://www.swisspeace.ch/etc/archive/previous-projects/fast-international/about.html>

PHSC - Sri Lanka, FEWER - Eurasia, ECOWARN - Rețeaua de avertizare timpurie și răspuns rapid a Comunității Economice a Statelor din Vestul Africii, ECOWAS/ Economic Community of West African States și CEWARN/ Conflict Early Warning and Response Mechanism);

căroră li se adaugă platforme de generația a patra, ce permit raportarea individuală a incidentelor din proximitate, prin intermediul telefoniei/ internetului (Ștefănescu, 2009).

În paralel cu evoluția semnificativă a instrumentelor analitice la nivelul organizațiilor internaționale, menite să monitorizeze diferite aspecte funcționale de interes pe linia de specialitate (financiară, economică, alimentație, dezastre naturale, etc.), apariția și consolidarea think-tankurilor a dus la o adevărată explozie a aplecării asupra unor studii și cercetări concretizate în analize și indecși/ indicatori meniți să furnizeze elemente de avertizare timpurie în baza a diferite sisteme de referință. Un exemplu în acest sens îl constituie Topul Statelor Eșuate, un produs al think-tankului Fund for Peace (studiat într-o temă anterioară), căruia i se adaugă multe altele: Indexul Fragilității Statale, CFIP (Country Indicators for Foreign Policy Project), Indexul Statelor Slabe (al Brookings Institution), etc. (Kis, 2012). Un exemplu concret legat de indicatorii folosiți și metodologia de lucru este disponibil și în lucrarea lui Frederick Barton – Avertizarea timpurie – o revedere a modelelor și sistemelor de prevedere a conflictelor (Barton și alții, 2008).

Bineînțeles, suportul științific sau, dimpotrivă, cel ideologic/ programatic al unor astfel de avertizări provenite în special din mediul calificat ca "independent" trebuie abordat cu precauțiile de rigoare. După cum observă R.C. Blitt, ONGurile active în domeniul avertizării timpurii privitor la drepturile omului – și așa generaliza aici pentru toate organizațiile societății civile implicate în avertizarea timpurie, indiferent de domeniul de interes – trebuie să accepte depășirea formelor de control informal privind calitatea și etica procedurală, ce pot conduce la critici legate de relevanța și obiectivitatea produselor lor. Asumarea rolului de agent al schimbării trebuie asociată cu credibilitatea și legitimitatea, iar acestea sunt condiționate de transparență și responsabilitate în procesele reglatoare și metodologiile de lucru (Blitt, 2005).

Intelligence în competiția economică (*Competitive Intelligence*)

Dezvoltarea unui mediu de afaceri concurențial și performant este o preocupare constantă în orice societate bazată pe economia de piață și competiția între agenții economici.

Dincolo de mijloacele de producție și know-how, informația este un activ de înaltă valoare în mediul economic. Pentru atingerea obiectivelor la nivelul managementului companiilor, informațiile despre furnizori, piața de desfacere a produselor și serviciilor și competitori sunt esențiale, fiind în măsură să asigure un avantaj competitiv în fața concurenței. Acestea nu sunt decât parțial cuprinse în documente cu caracter public, accesibile compartimentelor de analiză și prognoză, aprovizionare, marketing, desfacere, etc.

Pe de altă parte, firmele au niveluri de dezvoltare variabile, resursele dedicate activității de analiză a mediului economic în sprijinul deciziilor manageriale fiind ajustate în mod corespunzător. Situații specifice (tranzacții, listarea la bursă, nișe de piață, oportunități de dezvoltare, preferințele neexploatare ale clienților, etc.) pot solicita un volum mult mai mare de informații, cu un nivel ridicat de confidențialitate, de unde și necesitatea unor servicii specializate de descoperire, colectare și prelucrare a acestor date.

Activitatea de Intelligence în afaceri (*Bussiness Intelligence*) reprezintă un set de teorii, metodologii, arhitecturi și tehnologii ce facilitează transformarea datelor brute în informații utile pentru desfășurarea afacerilor (Rud, 2009), focalizate cu precădere asupra studierii și analizei activităților interne. Acest fapt determină diferența între Intelligence în afaceri și Intelligence competitivă, acesta din urmă constând în culegerea, analiza și diseminarea de informații cu privire la produse, tehnologii, clienți, competitori economici sau

mediul de afaceri, fiind definit ca ”proces hibrid de cercetare de marketing și analiză strategică ce poate oferi companiilor avantaj competițional”¹.

Bazele activității de Intelligence competitiv modern se consideră a fi puse de Michael Porter, în 1980, odată cu publicarea studiului *Competitive-Strategy: Techniques for Analyzing Industries and Competitors*, cunoștințele în materie fiind ulterior dezvoltate de CraigFleisher², Babette Bensoussan³, Leonard Fuld⁴ și alți autori. În 1988, Ben și Tamar Gilad au publicat primul model organizațional al unei funcțiuni de Intelligence competițional la nivel corporatist, care a fost adoptat pe scară largă în SUA, ulterior și în Europa⁵.

Crearea în 1986 a Societății Profesioniștilor în Intelligence Competițional, devenită ulterior asociația Profesioniștilor în Intelligence Strategic și Competițional (The Strategic and Competitive Intelligence Professionals - SCIP⁶), se leagă de numele lui Leonard Fuld și Kight. Organizația furnizează servicii de dezvoltare a cunoașterii și oportunități de relaționare între specialiștii în domeniul Intelligence competițional, cu accent pe aspectele legale și etice a culegerii și analizei de informații privind capacitățile, vulnerabilitățile și intențiile competitorilor în afaceri, reprezentând cadrul organizat al manifestării comunității profesioniștilor în Intelligence competițional. În 1996, Ben Gilad și Jan Herring au fondat Academia de Intelligence Competițional; acestora li s-a alăturat, din 1999, Leonard Fuld, urmând înființarea primei forme acreditate de instruire în domeniu⁷, recunoscută de SCIP.

Activitatea de Intelligence competițional nu trebuie confundată cu spionajul industrial, definit de Oxford Dictionary ca formă de spionaj îndreptată către descoperirea secretelor unui competitor în producția de bunuri sau către alte companii industriale⁸.

Spionajul industrial/ economic este practicat cu scopul obținerii unor avantaje comerciale în competiția economică internațională. În SUA, legea privind actul de spionaj economic, promulgată în 1996, încriminează: 1) însușirea frauduloasă a secretelor comerciale (informația comercială, neclasificată, sau informații privind apărarea națională, incluzând conspirația de însușire în mod fraudulos a secretelor comerciale sau achiziționarea secretelor comerciale obținute în mod fraudulos) având la cunoștință sau cu intenția ca beneficiul acțiunii să fie în favoarea unei puteri străine; 2) însușirea frauduloasă a secretelor comerciale legate de, sau incluse într-un produs care este destinat comerțului interstatal (inclusiv internațional), având la cunoștință sau cu intenția ca actul să prejudicieze proprietarul secretului comercial.⁹

În România, protecția, menținerea și stimularea concurenței și a mediului concurențial normal, este reglementată de legea nr. 11/1991 privind combaterea concurenței neloiale, cu modificările și completările ulterioare. Colectarea sistematică și analiza în condiții legale a datelor despre activitatea firmelor – în cadrul definit de Intelligence competițional – având ca surse ziarele, publicațiile privind ramura industrială de interes, statistici, înregistrări publice ale proceselor, formulare publice, prezentări la întâlniri industriale, contactul personalului cu clienții, furnizorii și competiția sunt considerate legale dacă nu se folosesc metode ne-etice de colectare a acestora, precum:¹⁰

¹ <https://www.boundless.com/marketing/consumer-marketing/technology-to-assist-market-research/competitive-intelligence/>

² <http://competitiveintelligence.ning.com/profile/CraigSFleisher>

³ <http://www.babettebensoussan.com/>

⁴ <http://www.leadingauthorities.com/speakers/leonard-fuld.html>

⁵ http://www.academyci.com/ftse/About_Competitive_Intelligence.html

⁶ www.scip.org

⁷ <http://www.academyci.com/ResourceCenter/>

⁸ <http://www.oxforddictionaries.com/definition/english/industrial-espionage>

⁹ http://www.businesshistory.com/mgt_compet_intelligence.php

¹⁰ <http://www.cciagl.ro/en/Newsletter%2010.pdf>

- furtul sau primirea de informații oferite voluntar (de exemplu, din partea unui angajat care vrea să se răzbune pe companie, sau care vrea o poziție mai bună într-o altă firmă);
- reprezentarea falsă (angajați care se dau drept clienți pentru a obține informații de la concurență, sau caută informații sub pretextul realizării unui studiu la nivelul ramurii);
- influențare ilegală (de exemplu, dare de mită);
- urmărirea ascunsă a concurentului (prin instrumente high-tech).

Diferența între actul de spionaj economic și specificul activității de Intelligence competițional este o preocupare permanentă în cadrul comunității de interes a profesioniștilor în Intelligence competițional (Horowitz, 1999); valorile etice la care SCIP face referire în acest sens sunt relevante:¹

- asigurarea recunoașterii și respectului acestei profesii;
- conformitatea cu legislația națională și internațională aplicabilă;
- asigurarea transparenței prin prezentarea tuturor informațiilor relevante (identitatea operatorului și al organizației de apartenență) în cadrul interviurilor;
- evitarea conflictelor de interes în îndeplinirea sarcinilor profesionale;
- furnizarea de recomandări și concluzii oneste și realiste în exercitarea activităților specifice;
- promovarea codului etic al SCIP în cadrul propriilor organizații, a sub-contractorilor și în cadrul profesiei, în general;
- aderarea cu fidelitate și conformarea la politicile, obiectivele și îndrumările companiei.

Spionajul economic atrage după sine și necesitatea protecției împotriva acestor acțiuni, care poate fi orientată de la împiedicarea ascultării telefoanelor mobile și a intruziunii clandestine în rețelele de date confidențiale ale firmelor, până la modalități de protecție fizică în asigurarea secretului comercial² și a securității activității firmelor.

Exploatarea oportunităților oferite de Intelligence competițional este realizată la nivelul companiilor atât prin resurse proprii (compartimente specializate), cât și prin contractarea ocazională a furnizorilor privați de astfel de servicii, fiind direct dependentă de aspectele interne (cultura organizațională, leadership) sau externe (deschiderea de piață, realitatea concurențială) ale organizației.

O evidență a firmelor ce au ca obiect de activitate Intelligence competițional trebuie să excludă companiile implicate în activități ce desfășoară studii de piață generale, studii de strategii generale, agenții ce desfășoară activități de Intelligence/ managementul riscului în mediul economic în baza unor proceduri neconforme cu cele promovate de SCIP (cum sunt Hakluyt sau Kroll) sau specialiștii independenți în informații – afacere ce acoperă un spectru larg de interese comerciale care desfășoară activități de Intelligence competițional ca preocupare secundară³.

La nivelul prestațiilor profesionale în Intelligence competițional sunt reclamate abilități specifice pentru sub-domenii ale Intelligence, precum OSINT sau HUMINT, combinate cu cunoștințe specifice domeniului economic și al unor discipline conexe –

¹www.scip.org

² constituie secret comercial informația care, în totalitate sau în conexarea exactă a elementelor acesteia, nu este în general cunoscută sau nu este ușor accesibilă persoanelor din mediul care se ocupă în mod obișnuit cu acest gen de informație și care dobândește o valoare comercială prin faptul că este secretă, iar deținătorul a luat măsuri rezonabile, ținând seama de circumstanțe, pentru a fi menținută în regim de secret; protecția secretului comercial operează atâta timp cât condițiile enunțate anterior sunt îndeplinite (Legea nr.11 din 29 ianuarie 1991 privind combaterea concurenței neloiale)

³http://aiip.org/sites/default/files/Getting_Started_IIP_2ed_2013.pdf

management, marketing, piața financiară, psihologia pieței, management comparat, operații bursiere, etc.

Activitatea de Intelligence competițional este o practică recunoscută, legală și esențială pentru asigurarea succesului managerial în anumite circumstanțe de piață, sporind beneficiile directe ale companiei.

Concluzii

Controversele în jurul contractelor cu furnizorii privați de servicii în domeniul Intelligence se leagă de prezența lor crescândă în cadrul comunităților de interes ale statului, atribuirea de funcțiuni considerate până de curând ca exclusive pentru sectorul de Intelligence guvernamental (cum ar fi culegerea de informații sau analiza, interogarea persoanelor capturate, culegerea de informații din surse umane, etc.), loialitatea chestionabilă (datoria față de angajator, și nu față de stat), cheltuielile bugetare reclamate de relațiile contractuale. Controlul contractorilor în zonele de conflict, în sensul atribuirii responsabilităților și în condițiile unor reglementări internaționale vagi, rămâne de asemenea o problemă.

Motivele ce determină conlucrarea comunităților guvernamentale de Intelligence cu entitățile private ce activează în domeniu sunt multiple; dintre acestea amintim:

- capacitățile tehnice/ tehnologice ale unor firme private, utile în domeniul dezvoltării unor sisteme din spectrul ISR;
- personal calificat și expertiză (abilități culturale, militare, lingvistice, IT, etc., traduse în activități de consultanță, protecție ș.a.m.d.);
- flexibilitatea locului de muncă/ disponibilitatea imediată;
- eficiența acțională asigurată de o structură organizatorică flexibilă, adaptată nevoilor efective ale companiei, cu o capacitate decizională rapidă, necondiționată de constrângeri birocratice.
- pentru decidenții politici, avantajul utilizării contractorilor privați rezidă în primul rând în reducerea costurilor politice, sociale și psihologice ale intervențiilor externe, disponibilitatea imediată a pârgurilor de acțiune și discreția/ confidențialitatea acțiunii.

Evoluția mediului de securitate relevă o serie de tendințe ce își pun amprenta asupra relevanței companiilor private în acest domeniu: lărgirea nișelor de piață (de ex. securitatea în domeniul cibernetic, extinderea zonelor de interes a marilor corporații în domeniul exploatării resurselor naturale, etc.) asociată cu expansiunea în materie de oferte de servicii specifice, monopolizarea domeniului consultanței de securitate (în condițiile în care, la nivel de politici publice, aceste aspecte sunt strict limitate), competiția economică și informațională între state și actorii nonstatali (Han, 2009), cărora le adăugăm multiplicarea spectrului de amenințări transnaționale, dar și creșterea în complexitate a manifestărilor societății civile, mediu propice pentru acțiuni ale grupărilor extremiste de diferite inspirații, adeseori asociate cu acte de violență.

De asemenea, reținem că analiza industriei private de securitate trebuie să aibă în vedere o serie de repere esențiale pentru înțelegerea tuturor resorturilor ce definesc activitatea companiilor din acest sector:

- tradiția istorică a mercenariatului ca întreprindere privată;
- cadrul legal de desfășurare a întregului spectru de activități din domeniul securității private;
- modul de finanțare;
- interesele firmelor private de securitate;
- cadrul contractual de prestare a unor servicii; sub-contractarea;
- selecția personalului;
- cultura organizațională;

- fundamentarea teoretică a activității;
- modalitatea de executare a serviciilor (în mod deschis, discret, acoperit sau clandestin);
- tehnicile, tacticile și procedurile folosite;
- resursele/ mijloacele de care dispun;
- responsabilitatea;
- comanda și controlul;
- etica în activitate;
- sensibilitatea culturală;
- comunicarea publică;
- relația/coordonarea cu alte entități a căror activitate interferează cu cea a firmei private de securitate.

Rosenbach și Peritz prevăd folosirea tot mai intensă, în viitor, a firmelor private în domeniul Intelligence, subliniind nevoia unor adaptări legislative care să rezolve toate incertitudinile legate de funcționarea acestora în condiții de transparență și răspundere (Rosenbach și Peritz, 2014). Pe de altă parte, creșterea dependenței de contractorii privați în domeniul Intelligence poate determina conflicte de interese atunci când spațiul de separare dintre interesele guvernamentele și cele ale actorilor privați tinde să se îngusteze.

În acest context, apare în mod justificat dilema privitoare la coabitarea în viitor, în condițiile mediului concurențial, a organizațiilor și agențiilor guvernamentale de Intelligence cu cele private, precum și modalitatea în care această relație se va reflecta asupra parametrilor reali și tangibili ai securității atât la nivel național, cât și regional sau chiar global.

Un prim comentariu este legat de competența profesională și expertiza personalului agențiilor guvernamentale din domeniu, care trebuie menținute la standarde înalte, cel puțin comparabile cu cele ale organizațiilor private. Aici intervin capacitatea managerială și politicile de personal în sectorul public în ceea ce privește educația și instruirea, motivarea personalului (pentru a preveni migrarea către mediul privat, mai promițător ca perspective¹), valorificarea oportunităților de practică, asigurarea resurselor necesare proceselor specifice în condițiile extinderii și multiplicării activităților necesare pentru a face față noilor forme de manifestare a amenințărilor la adresa securității.

Totodată, este de interes urmărirea evoluției aspectelor conceptuale, doctrinare și legale privind activitatea în domeniul securității, prin prisma multitudinii de actori implicați și a lobby-ului susținut pe care unele companii private din domeniul securității îl finanțează la nivel de guverne și organizații internaționale.

Toate aceste aspecte sunt de natură să influențeze capacitatea de menținere și dezvoltare a standardelor operaționale și a culturii organizaționale în domeniul activității de Intelligence la nivelul structurilor naționale specializate, necesitând acțiuni concrete de asigurare a unor modalități optime de conjugare a activității sectorului guvernamental cu cel privat.

Bibliografie

1. BARTON, Frederick; Von HIPPEL, Karin; SEQUEIRA, Sabina; IRVINE, Mark (2008) *Early Warning? A review of Conflict Prediction Models and Systems*, Center for Strategic and International Studies, în https://csis.org/files/publication/080201_early_warning.pdf

¹ Ion Duvac militează pentru un demers transparent de reconversie profesională pentru viitorii rezerviști din structurile cu atribuții informative și experții din domeniul securității naționale, în cadrul unor programe guvernamentale, propunând și soluții de optimizare a formării culturii de intelligence a decidenților politici prin implicarea nemijlocită a Comunității Naționale de Informații (Duvac, 2007)

2. BLAIN, Bruce, *The Role of Private & Mercenary Armies in International Conflict*, în <http://www.informationclearinghouse.info/article3396.htm>
3. BLITT, Robert Charles (2005) *Who will watch the watchdogs? Human Rights Nongovernmental Organizations and the case for regulation*, în Buffalo Human Rights Law Review Vol. 10, <http://www.ngo-monitor.org/data/images/File/SSRN-id753487.pdf>
4. CALLAGHAN, Jean și KERNIC, Franz (coord.) (2004) *Securitatea internațională și forțele armate*, Editura Tritonic, București
5. Comunicat de presă al ONU, *Private Security Companies Engaging In New Forms of Mercenary Activity*, UN Working Group (6 Nov. 2007)
6. CROWELL, William P, CONTOS, Brian T, DeRODEFF, Colby, DUNKEL, Dan (2011) *Physical and Logical Security Convergence: Powered By Enterprise Security Management: Powered By Enterprise Security Management*, Syngress
7. CUCU, Cornel (2008) *Transformări ale securității și relațiilor internaționale în contextul globalizării*, în Coordonator: dr. Constantin MOȘTOFLEI, *Politici și strategii în gestionarea conflictualității* (Sesiunea anuală de comunicări științifice cu participare internațională a Centrului de Studii Strategice de Apărare și Securitate, 20-21 noiembrie 2008, București - vol. 5 *Despre orizontala și verticala securității*), Editura Universității Naționale de Apărare „Carol I”, București
8. DUVAC, Ion (2007) *Suport de curs Intelligence – aplicații*, Facultatea de Sociologie și Asistență Socială, Universitatea din București, București
9. FAINARU, Steve (2008) *Legea celor puternici. Lupta mercenarilor din Irak*, Editura Litera Internațional, București
10. HAN, Laurențiu S. (2009) *Noi actori și tendințe pe piața securității*, în MOȘTOFLEI, Constantin (coord.), *Perspective ale securității și apărării în Europa*, Editura Universității Naționale de Apărare „Carol I”, București
11. HIRCH, Michael (2007) *Blackwater and the Bush Legacy*, în Newsweek, ed. Septembrie
12. HOROWITZ, Richard (1999) *Competitive Intelligence and the Economic Espionage Act*, a Policy Analysis adopted by the Society of Competitive Intelligence Professionals (SCIP) Board of Directors
13. KIS, Alexandru (2012) *NATO și securitatea umană*, Editura Universității din Oradea
14. KLEIN, Naomi (2008) *Doctrina șocului: nașterea capitalismului dezastrelor*, Editura Vellant, București
15. Legea nr.11 din 29 ianuarie 1991 privind combaterea concurenței neloiale
16. MICHALETOS, Ioannis (2009) *The era of the private intelligence agencies*, în <http://www.worldsecuritynetwork.com/Other/ioannis-michaletos-1/The-era-of-the-private-intelligence-agencies>
17. PETRACHE, Costinel (2009) *Războiul cald – războiul rece – războiul global. Pacea în armura terorii*, în MOȘTOFLEI, Constantin (coord.), *Perspective ale securității și apărării în Europa*, Editura Universității Naționale de Apărare „Carol I”, București
18. PORTER, Michael (1980) *Competitive-Strategy: Techniques for Analyzing Industries and Competitors*, First Free Press Edition, New York, în <http://www.vnseameo.org/ndbmai/CS.pdf>
19. ROSENBAACH, Eric și PERITZ, Aki J.(2014) *The Role of Private Corporations in the Intelligence Community*, în *Confrontation or Collaboration? Congress and the Intelligence Community*
20. RUD, Olivia (2009) *Business Intelligence Success Factors: Tools for Aligning Your Business in the Global Economy*, Hoboken, N.J: Wiley & Sons
21. SCAHILL, Jeremy (2009) *Blackwater – ascensiunea celei mai puternice armate private din lume*, Editura Litera Internațional, București
22. SCHMID, Alex (1998) *Thesaurus and Glossary of Early Warning and Conflict Prevention Terms*, Forum on Early Warning and Early Response (FEWER), în <http://reliefweb.int/sites/reliefweb.int/files/resources/82548F38DF3D1E73C1256C4D00368CA9-fewer-glossary-may98.pdf>
23. SINGER, P.W. (2005) *Outsourcing War*, în Foreign Affairs 84 (2) Ed. Martie/Aprilie
24. SMITH, Michael (2008) *Private Intelligence Companies*, în http://www.michaelsmithwriter.com/pdf/intelligence_companies.pdf
25. ȘTEFĂNESCU, Roxana (2009) *Sisteme, indicatori și platforme OSINT pentru avertizare timpurie, monitorizare și analiză*, în MOȘTOFLEI, Constantin (coord.), *Perspective ale securității și apărării în Europa*, Editura Universității Naționale de Apărare „Carol I”, București
26. UNGUREANU, Adriana (2009) *Revoluția în afacerile militare, sursă de securitate în zonele cu potențial conflictual*, în MOȘTOFLEI, Constantin (coord.), *Perspective ale securității și apărării în Europa*, Editura Universității Naționale de Apărare „Carol I”, București
27. WAIDYANATHA, Nuwan (2010) *Towards a typology of integrated functional early warning systems*, în International Journal of Critical Infrastructures. No 1 6: 31–51

28. http://aiip.org/sites/default/files/Getting_Started_IIP_2ed_2013.pdf
29. <http://competitiveintelligence.ning.com/profile/CraigSFleisher>
30. <http://mgimo.ru/files/121626/draft.pdf>
31. http://www.academyci.com/ftse/About_Competitive_Intelligence.html
32. <http://www.academyci.com/ResourceCenter/>
33. <http://www.aegisworld.com/>
34. <http://www.aqute.com/blog/building-a-list-of-competitive-intelligence-companies>
35. <http://www.babettebensoussan.com/>
36. <http://www.boozallen.com/>
37. http://www.businesshistory.com/mgt_compet_intelligence.php
38. <http://www.cciagl.ro/en/Newsletter%2010.pdf>
39. <http://www.colectivodeabogados.org/PRIVATE-SECURITY-TRANSNATIONAL>
40. <http://www.controlrisks.com/>
41. <http://www.counterterrorexp.com/>
42. http://www.dyn-intl.com/media/phoenix_training_center_catalog_2013.pdf
43. <http://www.dyn-intl.com/what-we-do/intelligence-and-security/>
44. <http://www.hakluyt.co.uk/>
45. <http://www.leadingauthorities.com/speakers/leonard-fuld.html>
46. <http://www.ohchr.org/EN/HRBodies/HRC/WGMilitary/Pages/OEIWGMilitaryIndex.aspx>
47. <http://www.oxforddictionaries.com/definition/english/industrial-espionage>
48. <http://www.pelorus-research.com/about>
49. <http://www.preventionweb.net/english/professional/terminology/v.php?id=478>
50. <http://www.smithbrandon.com/>
51. <http://www.sofexjordan.com/what.shtm>
52. <http://www.stratfor.com/>
53. <http://www.swisspeace.ch/etc/archive/previous-projects/fast-international/about.html>
54. <http://www.terrogen.com/>
55. <http://www.un.org/documents/ga/res/44/a44r034.htm>
56. <http://www.boundless.com/marketing/consumer-marketing/technology-to-assist-market-research/competitive-intelligence/>
57. www.kroll.com
58. www.scip.org

CAPITOLUL 8. CONTRAINFORMAȚIILE ȘI SPECTRUL AMENINȚĂRILOR LA ADRESA SECURITĂȚII

Counterintelligence/ contrainformații – delimitări conceptuale

Subiectul reprezentat de *counterintelligence* pornește, în mod necesar, de la clarificarea acestei noțiuni și a termenilor asociați. În acest sens, vom folosi în continuare termenul *contrainformații* ca traducere directă a noțiunii *counterintelligence*, abreviat ca CI.

Dicționarul WEBSTER definește conceptul contrainformațiilor ca *activitate organizată a unui serviciu de informații desfășurată cu scopul de a bloca sursele de informații ale inamicului, de a îl induce în eroare, a preveni sabotajele și a culege informații politice și militare*.¹

Definirea termenului ”contrainformații” în spațiul noțional al limbii române este legată de noțiunea de ”contraspionaj”; astfel, DEX 98 definește contrainformația (contrainformații) ca *serviciu de stat însărcinat cu urmărirea și combaterea spionajului și contraspionajul ca activitate de urmărire și de contracarare a actelor de spionaj și de descoperire și prindere a spionilor (dar și ca serviciu special care desfășoară activitatea de contraspionaj)*.²

În SUA, contrainformațiile se referă la *informațiile colectate și activitățile desfășurate în vederea protejării împotriva spionajului, a altor activități din spectrul intelligence, a sabotajelor sau asasinatelor executate de - sau în numele unei - puteri străine, organizații sau persoane, ori activități de terorism internațional, fără a include programe de securitate și protecție fizică a persoanelor, documentelor sau comunicațiilor*.³

Contraspionajul este văzut în doctrina militară SUA (JP 1-02 și JP 2-01.2, CI & HUMINT in Joint Operations, 11 Mar 2011) ca subset al CI, strict focalizat asupra *dectării, distrugerii, neutralizării, exploatării sau prevenirii activităților de spionaj prin identificarea, penetrarea, manipularea, înșelarea și reprimarea indivizilor, grupurilor sau organizațiilor implicate sau suspectate a fi implicate în activități de spionaj*.

Raportul Comisiei Church prezentat în senatul SUA consideră contraspionajul ca parte ofensivă⁴ a CI (acțiunea ofensivă a CI fiind detaliată într-un glosar de specialitate SUA din 2006 ca penetrare a grupurilor adverse și inducerea în eroare a acestora⁵, exclusiv orientat împotriva spionilor/ surselor umane ale acestora și având ca scop afectarea eficienței lor prin manipulare sau disruperea operațiilor de spionaj⁶).

În completare, același glosar clasifică CI *defensiv* ca totalitatea acțiunilor menite să protejeze informațiile vitale privind securitatea națională împotriva intrării în posesia lor sau a manipulării acestora de către organizațiile/ operațiile de intelligence adverse, fiind reprezentat

¹ <http://www.merriam-webster.com/dictionary/counterintelligence>

² <http://www.webdex.ro/online/dictionar/67115/contrainformatii>

³ ***, The provisions of Executive Order 12333 of Dec. 4, 1981, in 46 FR 59941, 3 CFR, 1981 Comp., p. 200, <http://www.archives.gov/federal-register/codification/executive-order/12333.html>

⁴ Senate Report # 94-755, aka Church Committee Report (1976) p. 166, citat în Office of Counterintelligence (DXC), Defense CI & HUMINT Center, Defense Intelligence Agency (2011), *Glossary (unclassified) Terms & Definitions of Interest for DoD Counterintelligence Professionals*, <http://fas.org/irp/eprint/ci-glossary.pdf>

⁵ NIPF (2006) *Intelligence Topic Definitions and Information Needs (unclassified)*, citat în Office of Counterintelligence (DXC), Defense CI & HUMINT Center, Defense Intelligence Agency (2011), *Glossary (unclassified) Terms & Definitions of Interest for DoD Counterintelligence Professionals*, <http://fas.org/irp/eprint/ci-glossary.pdf>

⁶ Lowenthal descrie acțiunea ofensivă ca manipulare fie prin transformarea agentului străin în agent dublu, fie prin ”intoxicarea” cu informații false a acestora (Lowenthal, 2003) – ambele variante vizând inducerea în eroare a serviciilor adversare.

la nivel acțional de destructurarea rețelelor clandestine și prevenirea (ca măsură a succesului) a atacurilor teroriste, cibernetice, etc.

Directiva Departamentului Canadian pentru Apărare Națională distinge tot două categorii funcționale ale disciplinei CI¹:

- pe de o parte *contrainformații* ("counter-intelligence/ contre-ingérence"²), focalizate asupra identificării și contracarării amenințărilor din partea serviciilor secrete ostile, a indivizilor sau organizațiilor ostile angajate în spectrul activităților TESSOC³ la adresa personalului, proprietății și informației forțelor proprii;
- pe de altă parte *informații pentru securitate* ("security intelligence/ renseignement de sécurité"), constând în colectarea și prelucrarea de date și informații privind identitatea, capacitățile și intențiile serviciilor de intelligence ostile angajate în activități din spectrul TESSOC (furnizând intelligence ca fază pregătitoare a CI ofensiv).

Definiția NATO dată CI face trimitere la activitățile care urmăresc identificarea și contracararea amenințărilor la adresa securității reprezentate de serviciile de informații, organizațiile sau indivizii ostili angajați în acțiuni de spionaj, sabotaj, subversiune sau terorism (AAP-6, 2-C-16, 2014). Această definiție introduce acronimul "TESS" (*Terrorism, Espionage, Sabotage, Subversion*) ca indicator al domeniilor de interes din perspectiva CI în NATO, aspecte care le vom aborda ulterior.

Contrainformații – contraspionaj; activități specifice mediului militar

Serviciile de CI sunt, de regulă, distinct organizate în cadrul comunităților de intelligence. Structuri specializate de contrainformații se regăsesc la nivelul tuturor entităților implicate în activitatea de garantare a securității naționale, în primul rând datorită expunerii acestora la activitatea de spionaj a structurilor adverse, interesate de resursele și potențialul de acțiune al acestora. Aceste structuri interne funcționează atât la nivel național, cât și în cadrul operațiilor externe ale entităților pe care le deservesc. Exemple de servicii centrale cu atribuțiuni de contrainformații sunt Biroul Federal de Investigații (FBI) în SUA, Serviciul de Securitate (MI5) în Marea Britanie, Serviciul Federal de Securitate (FSB) al Federației Ruse, iar în România – Serviciul Român de Informații (SRI).

CI trebuie abordate la toate nivelurile de referință – strategic, operațional și tactic. La nivel strategic-operațional, această disciplină facilitează asigurarea protecției intereselor guvernamentale (de stat) – indiferent de domeniul de manifestare a acestora (influență politică, economie și bunăstare, putere militară, etc.).

În NATO, instituția ce servește interesele strategice de protecție contrainformativă este Comandamentul Aliat pentru Contrainformații (Allied Command Counter Intelligence – ACCI), reprezentat la nivelul structurilor de comandă ale NATO, precum și în comandamentele operațiilor Alianței. La nivel operațional – tactic, atribuțiile specifice sunt coordonate de către structura de Intelligence din cadrul statului major al operației, prin intermediul secțiunii cunoscută ca "2X", responsabilă de coordonarea HUMINT, CI⁴ și, într-o

¹ DAOD 8002-2, Canadian Forces National Counter-Intelligence Unit, 2003, <http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-8000/8002-2.page>

² traducerea exactă din limba franceză interpretând CI ca și "[acțiune] împotriva ingerinței [adverse]"

³ Acronim consacrat în comunitățile de intelligence, semnificând "Terrorism, Espionage, Sabotage, Subversion, Organized Crime" (terrorism, spionaj, sabotaj, subversiune, crimă organizată)

⁴ Măsurile de protecție a forței (personal și instalații – securitatea fizică; operații – OPSEC; informații – INFOSEC) sunt sprijinite de operațiile CI cu surse umane – HUMINT, însă direcționate în mod exclusiv către aspecte de interes contrainformativ, având ca finalitate furnizarea de indicatori și avertismente.

măsură variabilă, a aspectelor legate de securitate¹, urmărind ca finalitate obiective de protecția forței.

Structurile militare naționale beneficiază de capacități CI (organice sau în sprijin) reprezentate de diferite structuri, în funcție de eșalonul de referință.

În mediul militar, responsabilitatea în domeniul contrainformațiilor se adresează atât elementelor specializate, cât și tuturor celorlalte structuri; dincolo de o cultură de securitate puternică, acestea trebuie să beneficieze de o minimă instruire în vederea depistării/ identificării structurilor de intelligence ale forțelor adverse și activitățile acestora.

Acțiunile de contracarare a structurilor de Intelligence ale adversarului îmbracă diferite forme – CI fiind o funcțiune multidisciplinară și nu un apanaj exclusiv al acțiunii agenților speciali (cum este de cele mai multe ori înțeleasă).

La acest nivel, acțiunile CI sunt legate de capacitățile de lovire a sistemelor tehnice de colectare a informațiilor, pe platforme terestre și aeriene (SIGINT, IMINT, MASINT, etc.), procedurile/ programele informatice de contracarare a spionajului cibernetic sau acțiunea forțelor și mijloacelor special desemnate să nimicească mijloacele de cercetare/ supraveghere ale forțelor adverse.

În succesiunea etapelor și fazelor operațiilor militare, funcțiunile Intelligence se traduc în următoarele sarcini de bază (FM 34-60, 1995):

- a. furnizarea de indicatori și avertizări;
- b. sprijinirea pregătirii informative a mediului operațional întrunit;
- c. sprijinirea producției de scenarii de dezvoltare situațională;
- d. sprijinirea activității de achiziționare a țintelor;
- e. dezvoltarea de intelligence pentru protecția forței;
- f. executarea de evaluări ale rezultatelor operațiilor/ acțiunilor/ loviturilor (BDA).

În acest cadru (după manualul Armatei SUA pentru CI, FM 34-60, ediția 1995, figura 1-1), funcțiunile CI variază în funcție de eșalon și de tipul operației desfășurate, cuprinzând activități din spectrul:

- **investigațiilor** (privind securitatea personalului, cazuri de trădare, spionaj, subversiune, revoltă, sabotaj direcționat de servicii străine, terorism, asasinat, dezertare, detenție, absență nejustificată, violări deliberate ale politicilor de securitate, suicid sau tentativă de suicid, penetrări de natură tehnică);
- **sprijinul operațiilor și protecția forței** (prin operații speciale CI, protecția forței în diferite faze și etape ale operației, protecția forței în operațiile cu surse, asistență și consiliere, legătură, sprijin tehnic, verificări ale respectării acordurilor/ tratatelor, contracararea acțiunilor ISR inamice, simularea acțiunilor adversarului – ”red cell”, acțiuni de acoperire a agenților, etc.);
- **colectarea de date și informații** (identificarea și validarea cerințelor, colectarea de date, debriefing și interogare, etc.);
- **analiză, sinteză, producție** (dezvoltarea și gestionarea de baze de date privind forțele proprii și amenințările, evaluări privind vulnerabilitățile și amenințările, identificarea prezenței și acțiunilor entităților ISR adverse, formularea de recomandări privind contramăsurile de securitate, evaluarea contramăsurilor, etc.).

Acestora, Manualul pentru Intelligence al Forțelor Terestre ale SUA (Army FM 2-0, Intelligence, 2010), adaugă în spectrul activităților specifice CI și serviciile funcționale și tehnice specifice.

¹ <https://rdl.train.army.mil/catalog/view/100.ATSC/10492372-71C5-4DA5-8E6E-649C85E1A280-1300688170771/2-22.3/chap2.htm>

Logica de funcționare a CI este strâns legată de procedurile de securitate existente la nivelul structurilor proprii, aplicate la nivelul securității personalului, a informațiilor, securitatea fizică, securitatea operațiilor și a informațiilor.

TESS – terorismul, spionajul, sabotajul și subversiunea ca subiecte de interes pentru serviciile de contrainformații militare

Terorismul

Terorismul a apărut ca subiect politic la nivelul Ligii Națiunilor din 1934, însă fără să fi întrunit până azi consensul în ce privește definirea unitară, comprehensivă, ancorată în principii de legalitate și urmărind prosecutiona faptelor de terorism, în ciuda multiplelor instrumente legale sectoriale elaborate începând cu 1963 pentru amendarea și prevenirea acestora.¹ În accepțiunea ONU, terorismul este descris ca reprezentând "acte criminale ce intenționează sau sunt calculate să provoace stare de teroare în cadrul publicului general, a unui grup de persoane sau la adresa persoanelor private (...) indiferent de considerațiile politice, filozofice, ideologice, rasiale, etnice, religioase sau de orice altă natură care sunt invocate în justificarea acestora"²

În NATO, terorismul este definit ca "folosirea sau amenințarea cu folosirea forței sau a violenței în mod ilegal împotriva indivizilor sau a proprietății în încercarea de a presa sau intimida guverne sau societăți în vederea atingerii unor obiective de natură politică, religioasă sau ideologică" (AAP-6, 2-T-5, 2014)

Legat de acesta, Alianța Nord-Atlantică a dezvoltat conceptul de apărare împotriva terorismului (aprobat la summitul de la Praga din 21 noiembrie 2002), sub impulsul atacurilor teroriste din 11 septembrie 2001 din SUA și a dezvoltărilor ulterioare ale fenomenului.

Interesul din perspectiva informațiilor militare în ce privește terorismul se leagă atât de rolurile identificate ale apărării împotriva acestui flagel (măsurile defensive antiteroriste, managementul consecințelor și reducerea efectelor actelor teroriste, măsurile ofensive contrateroriste și cooperarea militară)³, cât și de o funcțiune consacrată tuturor operațiilor militare – protecția forței⁴ – care, în contextul apărării împotriva terorismului, se confruntă cu un spectru de amenințări mult mai nuanțat și imprevizibil.

În funcție de caracteristicile mediului operațional, tipurile de amenințări teroriste la adresa forței și instalațiilor proprii (când ne adresăm mediului militar), probabilitatea de producere și impactul acestora sunt variabile în timp și spațiu, solicitând eforturi deosebite la nivel de colectare a datelor și informațiilor relevante (indicatori și avertizări privind ținta, momentul acțiunii, modul de operare, efectele scontate, etc.), precum și în palierul de analiză CI, angrenând totodată schimbul de informații cu alte agenții/ structuri.

Spionajul

Este de notat faptul că logica funcționării activității de spionaj se concentrează asupra accesării (directe sau prin intermediul unor interpuși, persoane cu acces corespunzător la informațiile de interes) a unor date și informații secrete de ordin politic, militar, de securitate, tehnologic sau economic. Obiectivul final al acestei activități vizează *alterarea sau*

¹ <http://www.un.org/en/terrorism/>

² UN General Assembly resolution 49/60 "Measures to Eliminate International Terrorism" (1994), *United Nations Declaration on Measures to Eliminate International Terrorism* (annex), December 9, în <http://www.un.org/documents/ga/res/49/a49r060.htm>

³ http://www.nato.int/cps/en/natohq/topics_69482.htm

⁴ În terminologia NATO, protecția forței semnifică totalitatea măsurilor și mijloacelor mobilizate pentru minimizarea vulnerabilității personalului, a facilităților, echipamentelor și operațiilor față de orice amenințare, în orice situație, pentru prezervarea libertății de acțiune și a eficienței operaționale a forțelor proprii

*influențarea unei decizii strategice, promovarea ilegală a intereselor proprii în detrimentul celor ale statului și ale partenerilor săi sau provocarea de agresiuni informaționale.*¹

Serviciul britanic MI-5 definește spionajul în mod bivalent, ca *proces ce implică folosirea de surse umane (agenți) sau mijloace tehnice pentru obținerea de informații ce nu sunt, în mod normal, publice, alături de influențarea factorilor de decizie și a formatorilor de opinie în beneficiul intereselor unei puteri străine.*² Acest al doilea aspect îl reprezintă tocmai finalitatea activității de spionaj; informațiile secrete vin în completarea celor disponibile din surse deschise - a căror culegere și prelucrare reprezintă o activitate de rutină pentru o serie de funcționari (diplomați, atașați militari sau economici, etc.) însărcinați cu monitorizarea diferitor aspecte ale vieții socio-economice, politice, ș.a.m.d. - și sprijină luarea deciziilor la nivel guvernamental, menite să contureze politica externă și relațiile internaționale, sau să asigure anumite avantaje (competiționale) în domeniile de interes.

Informațiile clasificate dețin acest caracter datorită importanței pe care o au pentru securitatea națională și care, datorită nivelurilor de importanță și consecințelor care s-ar produce ca urmare a dezvăluirii sau diseminării neautorizate, trebuie să fie protejate. În baza evaluării informației raportat la aceste două criterii, statele sau organizațiile internaționale își stabilesc taxonomii specifice, în cadrul cărora se reglementează și cerințele specifice de securitate aplicabile.

În România, Legea nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate³ prevede o serie de standarde naționale obligatorii, în concordanță cu criteriile și recomandările NATO în acest domeniu. Conform acestei legi (art. 15), *clasele de secretizare* a datelor și informațiilor sunt: **secrete de stat** (care privesc securitatea națională, prin a căror divulgare se pot prejudicia siguranța națională și apărarea țării) și **secrete de serviciu** (informațiile a căror divulgare este de natură să determine prejudicii unei persoane juridice de drept public sau privat). În continuare, *nivelurile de secretizare* sunt atribuite informațiilor clasificate din clasa secrete de stat, distingând categoriile (Legea 182/2002, art.15, litera "f"):

- **strict secret de importanță deosebită** - informațiile a căror divulgare neautorizată este de natură să producă daune de o gravitate excepțională securității naționale;
- **strict secret** - informațiile a căror divulgare neautorizată este de natură să producă daune grave securității naționale;
- **secret** - informațiile a căror divulgare neautorizată este de natură să producă daune securității naționale.

În NATO sunt considerate patru niveluri de clasificare a securității:^{4 5}

- a) COSMIC TOP SECRET (CTS), pentru informații a căror divulgare neautorizată ar cauza organizației pagube excepțional de grave;
- b) NATO SECRET (NS), pentru informații a căror divulgare neautorizată ar cauza pagube serioase organizației;
- c) NATO CONFIDENTIAL (NC), pentru informații a căror divulgare neautorizată ar afecta interesele organizației;

¹ <https://www.sri.ro/contraspionaj.html>

² <https://www.mi5.gov.uk/home/the-threats/espionage/what-is-espionage.html>

³ <http://www.orniss.ro/ro/182.html>

⁴ Marcarea documentelor ca NATO UNCLASSIFIED (NU) nu reprezintă o clasificare de securitate în sensul secretizării, ci a proprietății documentului – care nu poate fi făcut public fără permisiunea organizației. Diseminarea către public este însoțită de marcarea informației ca fiind NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC.

⁵ Marine Corps Installations Command East, *NATO Security Briefing*, în <http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=0CEIOFjAF&url=http%3A%2F%2Fwww.secnav.navy.mil%2Fdnsp%2FSecurity%2FInformation%2FDocuments%2Fintro-natosecuritybrief.pdf&ei=WKzrVLFiDOvXyQOruIKgBw&usq=AFQjCNFzhNqveDeZwKRY8wgWcUJqkrfILg&bvm=bv.86475890,d.bGQ>

d) NATO RESTRICTED (NR), pentru informații a căror divulgare neautorizată ar fi dezavantajoasă intereselor organizației.

Revenind la tema spionajului, putem identifica o serie de priorități în ce privește informațiile secrete vizate de către serviciile de spionaj, începând cu cele din domeniul militar și politic, precum și secretele industriale. Art. 17 din Legea nr. 182/2002 prezintă succint elementele de interes din categoria informațiilor secrete de stat.

Raportat la modalitățile de operare ale spionilor, acestea sunt direct determinate de cele două categorii de persoane implicate în acte de spionaj:

- membrii (militari sau civili) ai serviciilor de intelligence adversare, cu o pregătire corespunzătoare în ce privește tehnicile de spionaj și lucrul cu agenții, acționând sub acoperire (cu sau fără protecție diplomatică)¹;
- agenții² - surse umane ce acționează în mod acoperit și furnizează, în mod clandestin, în baza poziției lor și a relațiilor de încredere prestabilite, informații către ofițerii de intelligence; agenții au o instruire de bază în tehnici de spionaj și pot avea diferite motivații personale (inclusiv pecuniare) pentru desfășurarea acestei activități.

Culegerea informațiilor secrete se poate face printr-o largă varietate de metode, făcând apel la tehnologii de ultimă oră din domeniul comunicațiilor (mijloace de interceptare, transmitere de date, înregistrare optică, acustică, sau a altor semnale, etc.) și exploatarea vulnerabilităților de securitate ale organizațiilor/ entităților spionate. Dezvoltarea spațiului cibernetic oferă, din acest punct de vedere, oportunități extraordinare.

Sabotajul

În sens larg, sabotajul este definit ca fiind distrugerea, avarierea sau obstrucționarea deliberată a unui sistem (instalații și echipamente, activități, lucrări de infrastructură, servicii, etc.), în special pentru obținerea unui avantaj politic sau militar³, ca urmare a finalității reprezentate de împiedicarea bunului mers (eficienței) al unei activități, în special frânarea desfășurării normale a unui proces de producție⁴.

Acțiunea de sabotaj cade în sarcina celor numiți, generic, sabotori – persoane de interes pentru structurile CI, atât timp cât acestea servesc interese ostile iar identitatea lor este, de regulă, ascunsă (ca urmare a consecințelor actelor de care se fac responsabile). Dincolo de distrugerea fizică – ca metodă de acțiune pe care o implică sabotajul, obiectivul urmărit poate fi obținut de sabotor și prin exploatarea așa numitului ”element uman”: oportunităților de luare a unor decizii greșite (care să disrupă activitatea lucrativă – ex. promovarea incompetențelor în posturi cheie, fragmentarea activității prin convocarea de ședințe în momente critice, etc.) și convingerea altora de a le urma, sau adoptarea unor atitudini necooperante (ex. inflamarea situației la locul de muncă cu efecte directe asupra productivității).⁵

Un exemplu de act de sabotaj, comis prin intermediul virusului STUXNET, este distrugerea unei părți din echipamentul industrial al complexului nuclear iranian de la Natanz (Langner, 2013); alte exemple recente pot fi enumerate, comune situațiilor de criză sau război, cum ar fi: pasivitatea și neglijența forțelor de ordine ucrainene pe timpul revoltelor din orașul

¹ Acțiunea în acest sens ce presupune asumarea unei false identități fiind practică, dar ilegală și pedepsită de către statul gazdă

² Anumite națiuni folosesc termenul de ”agent” pentru a desemna ofițerii de intelligence, în timp ce sursele umane acoperite ale acestora sunt denumite ”informatori” (<https://www.mi5.gov.uk>)

³ <http://www.oxforddictionaries.com>

⁴ <http://dexonline.ro>

⁵ Office of Strategic Services (1944) Simple Sabotage Field Manual, Strategic Services (Provisional) No. 3, Washington, D. C, p. 5, în http://www.gutenberg.org/ebooks/26184?msg=welcome_stranger

Harkov (Ucraina), în aprilie 2014¹ sau distrugerea parțială prin acte de sabotaj a unor poduri de cale ferată în Ucraina, în martie 2015². Sabotajul face parte din arsenalul de proceduri asimetrice ce pot fi utilizate în cazul unui război hibrid, după cum o arată acțiunile Rusiei în estul Ucrainei.

Subversiunea

NATO definește subversiunea³ ca acțiune având ca scop slăbirea forței militare, a puterii economice sau voinței politice a unei țări⁴ prin subminarea moralului, a loialității cetățenilor săi sau a încrederii care li se poate acorda acestora (AAP-6, 3-S-7, 2014), sumă de aspecte ce pot fi subsumate conceptului ordinii de stat (Marcu, 2000).

La nivelul unei structuri de forță militară, regulamentele de specialitate ale armatei SUA menționează în spectrul subversiunii și acțiunea de încurajare activă a personalului militar sau civil în ce privește violarea legilor, nerespectarea ordinelor sau reglementărilor legale sau disruperea activităților militare cu intenția expresă de a interfera cu (sau a afecta) loialitatea, moralul sau disciplina forței (US CI Glossary, p. GL-82, 2011). În acest sens, toate actele ce contravin intereselor structurilor autorității și nu se încadrează în categoriile: trădare, incitare la revoltă, sabotaj sau spionaj sunt considerate activitate subversivă (JP 1-02).

Avantajele oferite de acțiunile subversive sunt legate de riscul, costurile și dificultatea relativ scăzută raportat la efectele urmărite; cu toate acestea, strategiile ce stau la baza acțiunilor subversive necesită rețele umane și conexiuni bine stabilite în organizațiile/societățile țintă, precum și o evaluare complexă a aspectelor sociale, politice, economice, culturale, religioase, etnice, istorice, etc. caracteristice acestora. Acțiunea propriu-zisă poate fi realizată prin pârgii de putere politică (infiltrarea și manipularea partidelor), manipulare prin mass-media, infiltrarea instituțiilor și structurilor din domeniul securității și al apărării – de unde și interesul pe care îl suscită pentru contrainformațiile militare.

Alte subiecte de interes pentru disciplina contrainformațiilor militare

Crima organizată

În România⁵, Legea 39/ 2003 privind prevenirea și combaterea criminalității organizate, publicată în Monitorul Oficial nr. 50 din 29.01.2003⁶ (având ca bază Convenția ONU împotriva criminalității transnaționale organizate⁷), definește în capitolul I, art. 2, **grupul infracțional organizat** ca fiind grupul structurat, format din trei sau mai multe persoane, care există pentru o perioadă și acționează în mod coordonat în scopul comiterii

¹ <http://www.ziare.com/international/ucraina/concedieri-in-masa-in-ucraina-o-treime-din-politistii-din-harkov-demisi-pentru-sabotaj-1292857>

² <http://www.mediafax.ro/externe/criza-din-ucraina-trei-poduri-feroviare-vizate-de-acte-de-sabotaj-in-estul-tarii-12903703>

³ Dicționarul explicativ al limbii române (ediția a II-a revăzută și adăugită), ed. 2009, prezintă subversiunea ca având același înțeles cu subminarea (a ataca, a lovi (indirect, pe ascuns) pentru a slăbi, a compromite, a zădărnici sau a nimici o acțiune, o realizare (a unui adversar))

⁴ Date fiind nivelurile diferite de referință care pot fi abordate, o abordare mai precisă ar trebui să facă referire la structuri ale autorității, incluzând statele

⁵ Alte interpretări la nivel european sunt disponibile în IACOB Adrian (2009) *Conceptul de criminalitate organizată în dreptul european*, în <http://www.legaladviser.ro/article/6082/Conceptul-de-criminalitate-organizata-in-dreptul-european>

⁶ <http://legeaz.net/legea-39-2003-actualizata>

⁷ Organizația Națiunilor Unite, *Convenție a națiunilor unite împotriva criminalității transnaționale organizate* (traducere), din 15/11/2000, publicată în Monitorul Oficial, Partea I nr. 813 din 08/11/2002, www.just.ro

uneia sau mai multor **infracțiuni grave**¹, pentru a obține direct sau indirect un beneficiu financiar sau alt beneficiu material (totodată, nu constituie grup infracțional organizat grupul format ocazional în scopul comiterii imediate a uneia sau mai multor infracțiuni și care nu are continuitate sau o structură determinată ori roluri prestabilite pentru membrii săi în cadrul grupului).

Infracțiunile grave, în contextul acțiunii structurate, capătă un interes deosebit din punct de vedere al securității din cauza impactului pe care acțiunile respective îl au la nivelul societății, prin penetrarea unor domenii esențiale funcționării statului (ex. crearea de riscuri sistemice prin fraudare masivă, asociată cu coruperea reprezentanților puterii) și dezvoltarea lor la dimensiuni și grade de complexitate comparabile cu cele corporatiste², într-o multitudine de modele acționale (Miclea, 2004).

În mediul militar, acțiunile complexe pe care criminalitatea organizată le presupune, coordonarea și relațiile dintre membrii rețelelor criminale (naționale sau transnaționale), obiectivele lor, precum și conexiunile membrilor forțelor proprii cu elemente de crimă organizată (percepute ca vulnerabilități) devin subiecte de interes pentru serviciile de contrainformații.

Amenințările din interior ("insider threat")

Capabilitatea și activitatea de Intelligence nu este vulnerabilă doar în fața unor factori externi, ci și a amenințărilor venite din interior – contabilizate la nivel de vulnerabilități exploatate prin activități ca subversiunea, trădarea, scurgerile de informații secrete, infiltrarea elementelor ostile.

Pericolul din interior ("*insider threat*") este reprezentat de indivizi aparținând organizației – actuali sau foști angajați, contractori, asociați – cu acces la zone sensibile și informații secrete pe care le exploatează în interes personal sau al unei terțe entități (organizații sau chiar țări), afectând interesele proprii organizației sau chiar securitatea națională (de la furtul unor date privind proprietatea intelectuală/ spionaj economic până la sabotaj și crimă).

În acest caz, efortul contrainformativ este focalizat asupra unor aspecte privind:³

- *factorii personali* (motive sau situații ce determină o astfel de acțiune îndreptată împotriva propriei organizații – cum ar fi: nevoia de bani, dorința de răzbunare, frustrarea la locul de muncă, conflictul ideologic sau de loialitate, spiritul de aventură, vulnerabilitatea la șantaj, comportament compulsiv etc.), asociați unor *indicatori de comportament* de natură să trezească suspiciuni cu privire la activitatea suspectului (accesarea unor documente care nu țin de necesitatea profesională; prezența (neaprobată) la lucru în afara programului normal; nerespectarea politicilor de

¹ **infracțiunea gravă** este infracțiunea care face parte din una dintre următoarele categorii: omor, omor calificat, omor deosebit de grav; lipsire de libertate în mod ilegal; sclavie; șantaj; infracțiuni contra patrimoniului, care au produs consecințe deosebit de grave; infracțiuni privitoare la nerespectarea regimului armelor și munițiilor, materiilor explozive, materialelor nucleare sau al altor materii radioactive; falsificare de monede sau de alte valori; divulgarea secretului economic, concurența neloială, nerespectarea dispozițiilor privind operații de import sau export, deturnarea de fonduri, nerespectarea dispozițiilor privind importul de deșeuri și reziduuri; proxenetismul; infracțiuni privind jocurile de noroc; infracțiuni privind traficul de droguri sau precursori; infracțiuni privind traficul de persoane și infracțiuni în legătură cu traficul de persoane; traficul de migranți; spălarea banilor; infracțiuni de corupție, infracțiunile asimilate acestora, precum și infracțiunile în legătură directă cu infracțiunile de corupție; contrabanda, evaziunea fiscală, alte infracțiuni financiare; bancruta frauduloasă; infracțiuni săvârșite prin intermediul sistemelor și rețelelor informatice sau de comunicații; traficul de țesuturi sau organe umane; orice altă infracțiune pentru care legea prevede pedeapsa închisorii, al cărei minim special este de cel puțin 5 ani (în România). (Legea 39/ 2003)

² <https://studiidesecuritate.wordpress.com/2011/02/19/crima-organizata-in-america-latina/>

³ <http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat>

- securitate ale organizației; contacte cu străini care nu sunt raportate; călătorii scurte și dese în afara țării, fără o motivație credibilă; afișarea unei bunăstări nejustificate de câștigurile materiale; interes deosebit în ce privește alți colegi; manifestarea îngrijorării cu privire la posibilitatea de a fi supravegheați, etc.);
- *factorii organizaționali* (percepția relaxată asupra riscurilor și vulnerabilităților; deficiențe privind politicile de securitate, managementul informațiilor, instruirea angajaților; practici de lucru neadevurate, care duc la o presiune a timpului asupra angajaților și la eludarea unor aspecte privind securitatea, etc.).

Noțiunile ”*insider threat*” sau ”*green on blue*” sunt în mod comun folosite în operațiile militare (NATO) pentru a desemna militari ai țării gazdă, aflați în relații de cooperare cu forțele proprii, care – la un moment dat – se întorc împotriva acestora din urmă (incluzând în rândul victimelor colegi loiali din cadrul propriilor structuri) (figura 1.8).

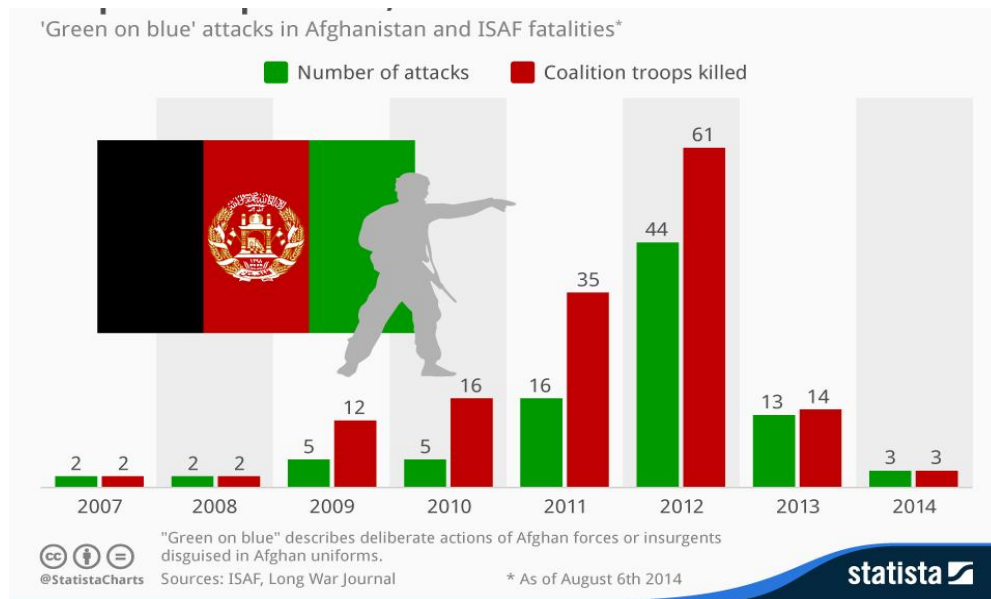


Figura 1.8 Evoluția incidentelor de tip ”*green on blue*” (atacuri ale militarilor afgani asupra militarilor din cadrul coaliției) în misiunea ISAF. Numărul de atacuri este reprezentat pe coloanele verzi, iar numărul de victime pe coloanele roșii.¹

Dincolo de spectrul de amenințări TESSOC, acest tip de atacuri sunt de o importanță deosebită pentru protecția (și moralul) forței, reclamând acțiuni complexe de prevenire.²

Amenințările cibernetice

Interesul tot mai mare al CI pentru acțiunile în mediul cibernetic este legitimat de o creștere exponențială a dependenței funcționale a sistemelor de securitate organizaționale/naționale de suportul informatic, asociat creșterii progresive a numărului de atacuri cibernetice sau utilizare a spațiului cibernetic în sprijinul unor acțiuni din spectrul TESSOC.

¹ <http://www.statista.com/chart/2537/green-on-blue-attacks/>

² https://www.google.ro/url?url=https://ronna.apan.org/CAAT/Coin%2520Common%2520Sense/20130220_NIU_REL_Public_COIN_Common_Sense_Insider_Threat_Special_Edition.pdf&rct=j&frm=1&q=&esrc=s&sa=U&ei=JJIIVdegAer7ygPbooHABQ&ved=0CBsQFjAB&usq=AFQjCNGNuG1z_1dsst-BPev0XROzU3jNag

Avantajele acțiunii în mediul cibernetic țin de costurile relativ scăzute raportat la volumul de date accesibil (și valoarea acestora)/ impactul acțiunii ostile, în condiții de siguranță fizică și posibilitatea de acțiune cu identitatea disimulată a operatorului, indiferent dacă acționează în interes personal, în numele unui grup (activist/ criminal/ terorist) sau al unui stat.

Acțiunile ostile în mediul cibernetic pot reprezenta un risc la adresa securității statului, a sistemului socio-economic, a bunei funcționări a unor organizații din domenii vitale, etc., de aceea eforturile CI sunt îndreptate spre identificarea atacatorului, stabilirea procedurilor folosite, contracararea acțiunilor de spionaj cibernetic, determinarea structurilor implicate (componenta operațională), ș.a.m.d. – alunecând către o supraspecializare ce face acest domeniu distinct în spectrul capacităților structurilor de securitate (a se vedea capitolul referitor la Intelligence în mediul cibernetic).

Concluzii

Este important de subliniat faptul că activitatea CI se desfășoară într-un cadru normat, legitim; în general, obiectivul de securitate al activităților CI vizează protecția a trei elemente fundamentale la nivel de organizație: personalul, instalațiile și operațiile proprii.

Parte din atributele ”pasive” ale disciplinei CI se leagă atât de documentarea și cunoașterea amenințărilor și a elementelor legate de acestea – surse posibile (organizații, indivizi), locații, etc., precum și de sensibilizarea și educarea personalului structurilor protejate cu privire la riscurile de securitate la care pot fi expuși. În partea acțională, monitorizarea persoanelor cu vulnerabilități în ce privește spectrul TESSOC urmărește aspecte legate de fundamentarea motivațională a deciziei acestora de implicare în astfel de acțiuni¹.

Contracararea mijloacelor tehnice ce pot fi utilizate în rețele de spionaj (senzori SIGINT, IMINT, MASINT) se bazează pe identificarea vulnerabilităților propriilor sisteme/elemente, furnizarea de soluții de securitate (inclusiv măsuri de mascare pasivă și activă) și monitorizarea acestora.

Pentru asigurarea protecției corespunzătoare în domeniul surselor deschise, cenzurarea informației (pusă în balanță de libertatea de exprimare specifică societăților democratice) reprezintă o măsură de prevenire a scurgerii de date și informații de valoare. Clasificarea documentelor în funcție de valoarea datelor și informațiilor pe care le conțin și a impactului pe care publicarea acestora l-ar avea asupra capacităților proprii reprezintă o practică aproape universală, parte a măsurilor generale de protecție a informației – INFOSEC.

Bibliografie

1. ***, *The provisions of Executive Order 12333 of Dec. 4, 1981*, in 46 FR 59941, 3 CFR, 1981 Comp., p. 200, <http://www.archives.gov/federal-register/codification/executive-order/12333.html>
2. DAOD 8002-2, *Canadian Forces National Counter-Intelligence Unit*, 2003, <http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-8000/8002-2.page>
3. ***, *Dicționarul explicativ al limbii române* (ediția a II-a revăzută și adăugită), ed. 2009
4. FM2-22.3 (2006) în <https://rdl.train.army.mil/catalog-ws/view/100.ATSC/10492372-71C5-4DA5-8E6E-649C85E1A280-1300688170771/2-22.3/toc.htm#toc>

¹ În general, comunitatea de Intelligence face referință în acest sens la: **bani** (câștig financiar, dificultăți financiare, adicția la cumpărături luxoase sau jocuri de noroc), **ideologie** (vederi extremiste, patriotism, credință religioasă, opinii politice, fundament cultural), **compromis/ coerciție** (șantaj, amenințări la adresa securității personale sau a familiei) sau **ego/ importanța de sine** (lipsa de toleranță la critică sau nevoia exacerbată de aprobare, mândria, aroganța, promisiunile de sprijin privind evoluția în carieră). Acestora li se adaugă și alte elemente favorizante, ca: starea de excitație (adrenalina) provocată de această activitate, legăturile de familie/ amoroase, seducția, situațiile conflictuale și dorința de răzbunare, etc.

5. Headquarters, Department of the Army (1995) *FM 34-60 Counterintelligence*, Washington, DC, 3 October, în http://fas.org/irp/doddir/army/fm34-60/f34-60_1.htm
6. <http://dexonline.ro>
7. <http://legeaz.net/legea-39-2003-actualizata>
8. <http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat>
9. <http://www.mediafax.ro/externe/criza-din-ucraina-trei-poduri-feroviare-vizate-de-acte-de-sabotaj-in-estul-tarii-12903703>
10. <http://www.merriam-webster.com/dictionary/counterintelligence>
11. http://www.nato.int/cps/en/natohq/topics_69482.htm
12. <http://www.orniss.ro/ro/182.html>
13. <http://www.oxforddictionaries.com>
14. <http://www.statista.com/chart/2537/green-on-blue-attacks/>
15. <http://www.un.org/en/terrorism/>
16. <http://www.webdex.ro/online/dictionar/67115/contrainformatii>
17. <http://www.ziare.com/international/ucraina/concedieri-in-masa-in-ucraina-o-treime-din-politistii-din-harkov-demisi-pentru-sabotaj-1292857>
18. <https://rdl.train.army.mil/catalog/view/100.ATSC/10492372-71C5-4DA5-8E6E-649C85E1A280-1300688170771/2-22.3/chap2.htm>
19. <https://studiidesecuritate.wordpress.com/2011/02/19/crima-organizata-in-america-latina/>
20. https://www.google.ro/url?url=https://ronna.apan.org/CAAT/Coin%2520Common%2520Sense/20130220_NIU_REL_Public_COIN_Common_Sense_Insider_Threat_Special_Edition.pdf&ret=j&frm=1&q=&esrc=s&sa=U&ei=JJIVdegAer7ygPbooHABQ&ved=0CBsQFjAB&usg=AFQjCNGNuG1z_1dsst-BPey0XROzU3jNag
21. <https://www.mi5.gov.uk>
22. <https://www.sri.ro>
23. IACOB, Adrian (2009) *Conceptul de criminalitate organizată în dreptul european*, în <http://www.legaladviser.ro/article/6082/Conceptul-de-criminalitate-organizata-in-dreptul-european>
24. JP 1-02 and JP 2-01.2, *CI & HUMINT in Joint Operations*, 11 Mar 2011
25. LANGNER, Ralph (2013) *To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve*, The Langner Group, Arlington-Hamburg-Munich
26. Legea nr. 39 din 2003 privind prevenirea și combaterea criminalității organizate
27. Legea nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate
28. LOWENTHAL, M. (2003) *Intelligence: From secrets to policy*, Washington, DC, CQ Press
29. MARCU, Florin (2000) *Marele dicționar de neologisme*, Editura Saeculum
30. Marine Corps Installations Command East, *NATO Security Briefing*, în <http://www.google.com/url?sa=t&ret=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=0CEIQFjAF&url=http%3A%2F%2Fwww.secnav.navy.mil%2Fdnsp%2FSecurity%2FInformation%2FDocuments%2Fintro-natosecuritybrief.pdf&ei=WKzrVLf1DOvXyQOruIKgBw&usg=AFQjCNFzhNqyeDeZwKRY8wgWcUJqkrfILg&bvm=bv.86475890.d.bGQ>
31. MICLEA Damian (2004) *Combaterea crimei organizate – evoluție, tipologii, legislație, particularități*, Editura Ministerului Administrației și Internelor, București
32. North Atlantic Treaty Organization, NATO Standardization Agency (2014) *AAP-6 - NATO Glossary of Terms and definitions (English and French)*
33. Office of Counterintelligence (DXC), Defense CI & HUMINT Center, Defense Intelligence Agency (2011), *Glossary (unclassified) Terms & Definitions of Interest for DoD Counterintelligence Professionals*, în <http://fas.org/irp/eprint/ci-glossary.pdf>
34. Office of Strategic Services (1944) *Simple Sabotage Field Manual*, Strategic Services (Provisional) No. 3, Washington, D. C, p. 5, în www.gutenberg.org/ebooks/26184?msg=welcome_stranger
35. Organizația Națiunilor Unite, *Convenție a națiunilor unite împotriva criminalității transnaționale organizate* (traducere), din 15/11/2000, publicată în Monitorul Oficial, Partea I nr. 813 din 08/11/2002, www.just.ro
36. UN General Assembly resolution 49/60 "Measures to Eliminate International Terrorism" (1994), United Nations Declaration on Measures to Eliminate International Terrorism (annex), December 9, în <http://www.un.org/documents/ga/res/49/a49r060.htm>
37. US Army Field Manual 2-0, *Intelligence*, 23 Martie 2010

CAPITOLUL 9. SITUAȚIILE DE CRIZĂ ȘI EȘUAREA STATALĂ – O PROVOCARE PENTRU ANALIZA DE INTELLIGENCE

Introducere

Conceptul de statalitate a suferit schimbări majore în ultima decadă. Noi tipuri și noi ierarhii ale statelor definesc imaginea unei lumi în continuă schimbare, în care principiile dreptului internațional sunt aplicate selectiv, puterea militară intrând în competiție cu alți factori de putere (economici, financiari, societatea civilă, etc.) statali, sub- sau supra-statali.

În acest context, începând cu 2005, think-tankul american “Fund for Peace” (Fondul pentru Pace¹), în colaborare cu revista „Foreign Policy”, publică un index anual denumit „The Failed States Index” (Topul statelor eșuate), în care stabilește (fără pretenții de exhaustivitate, dar de o manieră tot mai complexă în timp) ierarhia statelor ce alunecă spre colaps structural. Lista face referință exclusivă la state suverane, determinate de apartenența la ONU.

Admițând scopul științific al unui astfel de demers, trebuie să arătăm că există, în mod general, opinii contradictorii legate de credibilitatea think-tankurilor, considerentele legate de acestea variind de la a fi privite ca actori politici principali în societățile democratice, asigurând un proces de analiză, cercetare, proces decizional și evaluare politică pluralist și cuantificabil (Nakamura, 2002), până la minimalizarea credibilității lor în lumina servituții unor scopuri dictate de sponsori². În mod evident, există o aliniere (mai mult sau mai puțin declarată) a acestor instituții politice la anumite perspective ideologice sau la promovarea unor interese private, fapt ce poate altera demersul științific prin: promovarea sau publicarea selectivă a rezultatelor, distorsionarea acestora, constituirea think – tankului ca instrument de propagandă, asigurarea de lobby pentru formarea de opinii favorabile unor interese private, etc.

Întorcându-ne la subiectul analizei, dezvoltarea termenilor de „stat bandit”, „stat eșuat” sau „pseudo-stat” – ca expresie a unei stări alterate a puterii de stat – și promovarea lor în limbajul politic internațional este o abordare ce lasă loc criticilor. Elementul cel mai sensibil este faptul că includerea unui stat în această categorie permite construirea de argumente ce justifică un anumit tip de negociere a suveranității naționale a acestuia (facem referire în acest sens la promovarea conceptului ”responsabilității de a proteja”, asociat cu ingerința în problemele interne ale unui stat sub motivația salvagădării securității umane).

Cazul Libiei, unde perspectiva unui dezastru umanitar a generat intervenția militară a comunității internaționale, nu a găsit aceeași rezonanță într-o situație de criză similară³ (a se vedea situația Siriei, în cazul căreia o rezoluție a Consiliului de Securitate al ONU a fost blocat în repetate ori de Rusia și China). Mai mult, intervenționismul a fost împins la extrem prin ocuparea și anexarea Crimeei de către Rusia sub pretextul protejării populației rusofone din această regiune a Ucrainei.

Pe de altă parte, indexarea unei entități statale în baza unor repere de orice natură, atât de către organizații internaționale (ex. Fondul Monetar Internațional – indexul privind starea economică⁴ sau stabilitatea financiară⁵, Banca Mondială⁶ - în domenii ca: dezvoltarea urbană și rurală, infrastructură, economie și creștere economică, mediu, datorii externe, Programul

¹ http://en.wikipedia.org/wiki/Fund_for_Peace

² http://www.sourcewatch.org/index.php?title=Think_tanks&oldid=283573

³ făcând referire la punerea în aplicare a rezoluțiilor ONU care reclamă intervenția militară de către organizații regionale cu relevanță militară – cum e cazul NATO

⁴ <http://www.imf.org/external/pubs/ft/weo/2014/update/01/>

⁵ <http://www.imf.org/external/pubs/ft/gfsr/about.htm>

⁶ <http://data.worldbank.org/topic>

pentru Dezvoltare al ONU – Indicatorii de dezvoltare umană¹, etc.) cât și la nivel informal, de către organizații neguvernamentale (ex. Fitch – în domeniul financiar și al asigurărilor², fundația Heritage – cu Indexul Libertății Economice³, ș.a.m.d.) reprezintă semnale importante pentru mediul investițional, sensibil la orice trend sau risc emergent menit să afecteze echilibrul sau perspectiva de câștig financiar a respectivelor grupuri de interes.

Dincolo de interpretări de orice natură, existența entităților statale nefuncționale este un fapt cert și considerăm de interes a observa cum funcționează balanța dintre factorii de dezechilibru interni și externi în procesul manifestării evoluției lor spațio-temporale.

Deși central pentru subiectul dezbătut, conceptul de stat „eșuat” este doar o inovație lingvistică și stilistică relativ recentă, cu toate că aceste state au existat pe tot parcursul secolului trecut (și al istoriei statalității, în ansamblul ei); faptul că această realitate a devenit un subiect de interes mondial îl constituie mutațiile suferite de capacitățile puse în slujba amenințărilor, care s-au modificat radical.

Fragilitatea nu constituie un pericol doar pentru statul în cauză, ci reprezintă o amenințare pentru progresul și stabilitatea altor state, care depind într-un fel sau altul de aceste entități sau se găsesc în situații care suferă comparații, mai ales în condițiile lumii globalizate. Sunt ilustrative, în acest sens, ecourile pe care două situații de actualitate, cu potențial destabilizator – criza din Ucraina (cu concursul larg al Rusiei) și situația financiară și politică a Greciei – le au la nivelul Uniunii Europene.

Delimitări conceptuale

Aprofundând subiectul eșuării statale, apare necesitatea determinării plajei conceptuale a mai multe atribute, relativ asemănătoare ca inducție și sugestie, care definesc state sau guverne prezentând simptome ale unei existențe ce nu se încadrează în uzanțele general acceptate și după care un stat se manifestă sau ființează în cadrul comunității internaționale ca: „eșuat” (*failed state*), „în colaps” (*collapsed state*), „escroc” sau „bandit” (*rogue state*), „pseudo-stat” (*pseudo-state*) sau chiar „stat terorist”.

Definirea conceptului de stat eșuat comportă mai multe sisteme de referință (Thürer, 1999):

Abordarea din punct de vedere politic și legal se concretizează în trei elemente: aspectul geografic și teritorial (criza ca implozie, asociată cu probleme interne, dar incluzând și impactul extern incidental), aspectul politic (colapsul intern al legii și ordinii datorat prăbușirii structurilor responsabile – mai degrabă decât cel generat de acțiunile unor facțiuni care urmăresc întărirea propriei poziții sau chiar uzurparea celei de stat) și aspectul funcțional (absența structurilor capabile să reprezinte statul la nivel internațional și, pe de altă parte, să recepteze influențele lumii exterioare).

Tributar contextului istoric și de dezvoltare, observăm că statele considerate ca „eșuate” aparțin eminent lumii a treia și au fost afectate de trei factori geopolitici: sfârșitul Războiului Rece (și implicit al suportului masiv primit de regimurile ideologice artificiale ținute în funcție de către superputerile lumii; absența sponsorizărilor acestora a permis întărirea puterii facțiunilor rivale, iar statele au început să își piardă legitimitatea și autoritatea, reducându-se la valoarea de alt grup în conflict cu celelalte), moștenirea regimurilor colonialiste (care au durat suficient de mult pentru a distruge structurile sociale tradiționale, dar nu suficient de mult pentru a le înlocui cu structurile constituționale occidentale și a le da identitatea unui nou stat – de aici autoritate bazată pe dominanța economică sau militară/

¹ <http://hdr.undp.org/en/data>

² <https://www.fitchratings.com/web/en/dynamic/fitch-home.jsp#>

³ <http://www.heritage.org/index/>

polițienească și nu pe legitimitate, loialitatea redusă a populației și divizarea acesteia¹) și procesele generale de modernizare care au încurajat mobilitatea socială și geografică, dar fără a fi contrabalansată de procese de construcție națională capabile să plaseze statul pe un fundament solid, oferindu-i capabilitatea de a gestiona integrarea pieței și schimbul și fluxul liber de capital. În viziune critică neo-imperialistă (Liu, 2005), aceasta se traduce în transformarea statelor client slăbite, cu drepturi de suveranitate restricționate, în capete de pod ale pieței statului puternic în expansiunea sa generală, detașând securitatea economică de funcțiunile statului legitim.

În al treilea rând, perspectiva sociologică face trimitere la două fenomene tributare ideii că, dacă disoluția se manifestă acut doar în anumite state, rămâne latentă oriunde în lume. Aceste fenomene sunt: colapsul esenței guvernării (inexistența sau inabilitatea de exercițiu a organelor de lege și ordine) și brutalitatea și intensitatea violenței folosite (a se vedea situația din Liberia).

Subsumând, observăm mai mulți indicatori care determină catalogarea unui stat ca fiind „eșuat”, printre aceștia regăsindu-se:

- un stat al cărui guvern central este atât de slab sau inefficient încât deține un control efectiv redus asupra celei mai mari părți a teritoriului său, după cum vom arăta în cadrul acestui capitol, și varianta în care – în condițiile păstrării controlului – supune structura statală intereselor private, în serviciul unei clientele bogate ce își trage avantajele din sistemul erodat (Liu, 2005);
- autoritatea legitimă de a lua decizii colective a fost compromisă;
- nu este în măsură să asigure servicii publice la un nivel rezonabil (absența unui sistem universal de protecție a sănătății; sistem de învățământ primar public rezervat copiilor săraci disfuncțional);
- corupție și criminalitate larg răspândite;
- existența refugiaților și a dislocărilor involuntare de populație;
- declin economic accentuat în condițiile unei infrastructuri economice care clachează în a asigura venituri și bunăstare în mod echitabil și merge până la foamete și lipsa de hrană pentru populația săracă în timp ce în economie persistă surplusuri de hrană;
- interacțiuni inexistente sau ratate cu alte state.

Putem considera că un stat supraviețuiește atâta timp cât își menține monopolul asupra uzului legitim al violenței în cadrul propriilor frontiere. Când acest fapt nu mai este efectiv (în fața prezenței „lorzilor războiului”, a milițiilor rebele sau elementelor teroriste), existența propriu zisă a statului devine îndoielnică iar acesta întrunește premisele încadrării în categoria statelor eșuate.

Dificultatea în a determina gradul de menținere a unui astfel de monopol asupra uzului legitim al forței (care include și problema definirii legitimității) nu este clar conturată. Pornind de la premiza că doar un stat deține mijloacele de producție necesare asigurării instrumentelor violenței fizice, nu se pune problema legitimității în ce privește obținerea monopolului asupra acestor mijloace (de facto), dar este important a fi luată în considerare în momentul folosirii lor (de jure). De aici, aparent paradoxal, unele curente avansează ideea conform căreia statele eșuate nu sunt întotdeauna state slabe, incluzând în această categorie state puternice (Liu, 2005) care aplică în mod voluntar anumite politici în baza unor ideologii sau permit uzurparea

¹ Procesul de acumulare a puterii centralizate în aceste state a constat într-o serie de strategii de subordonare și asimilare care tind să maximizeze resentimentele grupurilor submise – etnic, religios, etc. Rezultatul final îl constituie o profundă polarizare, bazată pe deziluzie și insatisfacții legate de stat atât din partea populației, cât și a elitelor locale. A se vedea pe larg în: The African Studies Centre (Leiden), The Transnational Institute (Amsterdam), The Center of Social Studies/ Coimbra University, The Peace Research Center CIP-FUHEM (Madrid), *Failed and collapsed states in the international system*, December 2003, în <http://www.globalpolicy.org/nations/sovereign/failed/2003/12failedcollapsedstates.pdf>

unor astfel de funcțiuni de către grupuri de interes special. Această categorie de state dețin o putere militară/ polițienească dezvoltată și promovează interesele economice înguste ale unei mici clase de cetățeni, în timp ce sacrifică marea masă a populației ca victime ale unei piețe esuate.

Termenul de „stat eşuat” este de asemenea folosit în sensul în care un stat se dovedește a fi ineficient, incapabil să aplice în mod uniform legea din cauza unei rate înalte a criminalității, corupției politice extreme, pieței negre supradimensionate, birocrăției impenetrabile, ineficienței juridice, interferențelor militare în politică, împrejurărilor culturale în care lideri tradiționali reclamă mai multă putere decât cea statală asupra unei anumite zone, dar nu intră în competiție cu statul.

Centrul de Cercetare a Crizelor Statale¹ definește „statul eşuat” ca o variantă a „colapsului statal” - stat care nu mai este în măsură să își exercite securitatea de bază și funcțiunile de dezvoltare și nu deține un control efectiv asupra teritoriilor și frontierelor sale. Un stat eşuat nu mai este în măsură să asigure condițiile propriei existențe. Această idee este utilizată în modalități contradictorii în comunitatea politică, existând o tendință de a eticheta un stat cu slabe performanțe ca fiind „eșuat”, atitudine pe care Centrul de Cercetare a Crizelor Statale o respinge.

Spre deosebire de conceptul de „stat eşuat” sau „în colaps”, cel de „stat bandit” sau „escroc” pare în esență să fie arbitrar, contestabil și încărcat din punct de vedere ideologic. Conceptul își găsește originea în adoptarea sa de către britanici în India, pe timpul perioadei coloniale. În anii '60 – '70, mai mulți autori au utilizat termeni similari pentru a descrie anumite state cu comportament neconform cu normele internaționale. În accepțiunea sa de azi, conceptul de „stat bandit” se conturează în anii '80, când se vorbea și de „state teroriste” și „în afara legii”. În 1986, președintele american Ronald Reagan promova ideea izolării totale a statelor teroriste, vizând înainte de toate regimul „în afara legii” a colonelului libian Moamer Ghadafi.

Până în 1994, conceptul suscită puțin interes. La acea vreme, Anthony Lake, consilierul președintelui american Bill Clinton, publica un articol în care folosea termenul de „stat bandit”. Acesta era punctul de plecare a unei noi ideologii care permitea orientarea politicii externe americane în contextul sfârșitului războiului rece. Folosirea conceptului s-a răspândit rapid în sânul Congresului și în media americană. Pe lista statelor bandit se regăseau: Coreea de Nord, Siria, Libia, Iranul, Irakul, Sudanul și Cuba. În contextul multiplicării criticilor legate de folosirea acestui termen, a fost retras de către administrația Clinton din discursul său oficial și înlocuit cu cel de «*state of concerns*» (state care provoacă îngrijorări), revenind în planul discuțiilor după evenimentele din 11 septembrie 2001.

O altă sintagmă folosită este noțiunea de pseudo-stat, definită ca acea entitate care nu este fondată decât pe legături personale, de clan sau tribale și pentru care, în viziunea S.U.A., Convențiile de la Geneva nu se justifică a fi aplicate². Acesta este cazul Afganistanului, unde prizonierii făcuți de forțele americane nu s-au bucurat de statutul de prizonieri de război, determinând apariția unei noi categorii de deținuți, cu regim special – cei „suspecți de terorism”.

Topul statelor eşuate; premisele colapsului și metodologia de cercetare aplicată

Nu vom insista asupra realităților particulare care au determinat prezența în partea superioară a clasamentului a anumitor state; există o vastă disponibilitate de informații relevante în acest sens. Din perspectiva analizei de securitate, ne vom focaliza efortul asupra

¹ http://en.wikipedia.org/wiki/Crisis_States_Research_Centre

² ***, *Un parfum de Guerre froide*, 2005, în <http://www.voltairenet.org/article16092.html>

metodologiei folosite pentru a putea determina scorurile și a stabili clasamentul statelor în topul susceptibilității de eșuare.

Instrumentul de lucru a fost denumit „Conflict Assessment System Tool” (CAST) – Complex de Sisteme de Evaluare a Conflictului. Pe lângă notarea a 12 indicatori¹ sociali, economici și politico – militari pe care îi vom detalia în cadrul acestui capitol, alte etape cuprind evaluarea capacităților a cinci instituții de stat considerate esențiale pentru sustenabilitatea securității, identificarea factorilor idiosincratice și a surprizelor, precum și plasarea țărilor pe o hartă a conflictelor care să arate istoricul riscurilor la care acestea sunt supuse.

Notarea este bazată pe un scor obținut în urma analizei indicatorilor de vulnerabilitate a statelor: patru în domeniul social, doi economici și șase politici, cu un rating cuprins de la 0 la 10, 10 semnificând „cel mai puțin stabil”. Indicatorii nu sunt concepuți să prezică momentul în care statele analizate riscă să se confrunte cu violențe sau să intre în colaps; în schimb, sunt capabili să măsoare vulnerabilitatea unui stat la colaps sau conflict.

a. Indicatori sociali

1). Presiuni demografice: include presiunile derivate din densitatea mare a populației relativ la posibilitățile de asigurare cu hrană și alte resurse vitale. Presiunea izvorâtă din patternurile sociale și delimitările fizice, incluzând disputele de frontieră, deținerea sau ocuparea de terenuri, acces la căile de transport, controlul locațiilor cu semnificație religioasă sau istorică și riscul producerii unor pericole ambientale.

2. Deplasări masive de refugiați sau de persoane dislocate: împrăștierea forțată a largi comunități ca rezultat al violențelor directe, a represiunilor, lipsei hranei, bolilor, lipsei apei potabile, competiției pentru terenuri și tulburărilor care pot să le antreneze în spirala unor mari probleme umanitare și de securitate, atât în cadrul propriei țări cât și între state.

3. Neajunsul reprezentat de perpetuarea grupărilor care caută răzbunare în virtutea unor nedreptăți recente sau mai vechi, chiar datând secole în urmă, incluzând atrocități, persecuții sau represiuni trăite de marea masă sau de grupuri particulare în relația cu statul sau cu alte grupări dominante. Aceste atitudini revanșarde pot să aibă la origini și excluderea politică instituționalizată, putând căpăta forme de responsabilizare publică în cadrul retoricii politice naționaliste lansate în critici aduse grupărilor considerate a fi responsabile.

4. Emigrare cronică și susținută: atât exodul creierelor, alimentat de emigrația profesioniștilor, intelectualilor și dizidenților politici, cât și emigrația voluntară a reprezentanților clasei mijlocii. Creșterea comunităților în exil/ expatriate sunt de asemenea folosite ca parte ale acestui indicator.

b. Indicatori economici

5. Dezvoltarea economică inegală determinată de inegalitățile de grup ori de inechitățile percepute în educație, muncă și statut economic. De asemenea, include măsurile nivelurilor sărăciei la nivel de grup, rata de mortalitate infantilă, nivelurile de educație.

6. Declinul economic accentuat/ sever, care este măsurat ca progresie a declinului economic al societății ca întreg (folosindu-se în acest sens: venitul brut per capita, PIB, datoriile, rata de mortalitate a copiilor, nivelurile de sărăcie, eșecurile în afaceri) și vizează în egală măsură evoluția prețurilor, schimburile, investiții străine sau plata datoriilor. Este urmărit colapsul sau devalizarea monedei naționale și creșterile pe care le înregistrează economia subterană, incluzând traficul de droguri, armament, minerale rare, precum și expedierile de capital. Un alt reper îl constituie neplata de către stat a salariilor către funcționarii publici, către forțele armate sau a altor obligații financiare către proprii cetățeni, cum ar fi plata pensiilor.

¹ Apud http://en.wikipedia.org/wiki/Failed_state

c. Indicatori politici interni

7. Criminalizarea și/ sau delegitimarea statului: corupție și profitorism al elitelor conducătoare, rezistență la transparență, politica financiară, reprezentarea politică. Reperul include orice pierdere a încrederii populației pe scară largă în procesele și instituțiile statului.

8. Deteriorarea progresivă a serviciilor publice: o dispariție a funcțiilor de bază ale statului care serveau populației, incluzând lipsa protecției acesteia față de terorism și violență și asigurarea serviciilor esențiale în domeniile: sănătate, educație, igienă, transport public. De asemenea, folosirea aparatului de stat în folosul agențiilor subordonate elitelor conducătoare, cum ar fi forțele de securitate, stafful prezidențial, banca centrală, serviciul diplomatic, vămile și agențiile de colectare a taxelor și impozitelor.

9. Violarea pe scară largă a drepturilor omului: emergența unor reguli autoritariste, dictatoriale sau militare în care instituțiile și procesele constituționale și democratice sunt suspendate sau manipulate. Mai sunt cuantificate: izbucniri ale violenței de inspirație politică împotriva civililor nevinovați; un număr crescut de prizonieri politici sau dizidenți cărora li se refuză un proces echitabil, în concordanță cu practicile și normele internaționale; orice abuz asupra drepturilor legale, politice și sociale, incluzându-le pe cele ale indivizilor, grupurilor sau instituțiilor culturale.

10. Aparatul de securitate ca „stat în stat”: emergența elitelor sau a „gărzilor pretoriene” care operează fără a fi supuse pedepsei; emergența milițiilor private sponsorizate sau sprijinite de stat în vederea terorizării oponentilor politici, a celor suspectați ca fiind „inamici” sau a civililor care simpatizează opoziția; o „armată în cadrul armatei”, care servește interesele unei clici militare sau politice dominante; emergența milițiilor rivale, forțelor de gherilă sau armatelor private în acțiuni armate sau campanii violente împotriva forțelor de securitate a statului.

11. Ridicarea elitelor fașionalizate, focalizându-se asupra fragmentării elitelor conducătoare și a instituțiilor statului pe linia intereselor de grup. Este urmărit orice uz al retoricii politice naționaliste de către elitele conducătoare, adeseori în termeni iredentiști sau de solidaritate comunitară.

Nu numai realitățile politice interne sau factori indigeni de altă natură sunt responsabili pentru problemele cu care unele state se confruntă.

Factorii externi, chiar dacă nu sunt întotdeauna vizibili, au o importanță care nu poate fi neglijată. Fund for Peace a identificat o serie de astfel de factori de natură externă, pe care îi evaluează în vederea stabilirii scorului de risc, dar fără a evidenția o metodologie în acest sens (similară CAST):

- angajări militare sau paramilitare în afacerile interne ale statului aflat în situație de risc;
- acțiuni ale unor armate externe, state, grupuri de identitate sau entități care afectează balanța internă a puterii ori rezoluția unui conflict;
- intervenții ale unor donori (în mod special dacă există o tendință către dependența exclusivă de sprijin străin¹) sau existența unor misiuni în sprijinul păcii care se derulează pe teritoriul lor.

Dincolo de acestea, în contextul actual al evoluțiilor din economie, contabilizând și efectele schimbărilor climatice, se conturează pericolul limitării accesului la resursele vitale și al înfometării¹.

¹ Ajutorul internațional nu reușește să depășească etapa de „control al pagubelor”, rezumându-se la peticirea rapidă a crizelor umanitare, transformându-se cu greu în proiecte viabile pe termen lung. „Ajută-i să se ajute singuri” este o formulă aplicată de comunitatea internațională în Afganistan, iar perioada de după ISAF va fi relevantă pentru sustenabilitatea acestora.

Observăm că metodologia CAST, permanent revizuită și perfecționată cu concursul unor experți și agenții din toate sectoarele de interes, prezentând garanția folosirii surselor alternative de informare, se constituie într-un instrument complex și viabil de analiză a stării generale a unui stat².

În sprijinul acestei afirmații vine faptul că această metodologie este folosită de guverne, printre alte instrumente de analiză, pentru a obține avertizări timpurii și a dezvolta strategiile de asistență economică ce pot reduce potențialul pentru conflict și să promoveze dezvoltarea în statele fragile.

Uzul militar al CAST se regăsește în consolidarea avertizărilor punctuale, perfecționarea gradului de pregătire și aplicarea de strategii de evaluare a succesului în operațiuni de gestionare a situațiilor de criză.

Sectorul privat folosește această metodologie pentru a calcula riscurile politice pentru oportunitățile de investiții. Organizațiile multinaționale găsesc acest instrument util pentru modelare și simularea de scenarii, managementul organizațiilor complexe și pentru evaluarea riscurilor conflictuale.

Specialiștii din mediul academic îl folosesc pentru a antrena studenții în analiza problemelor aferente stărilor de război, criză sau pe timp de pace prin mixarea tehnicilor specifice tehnologiei informațiilor cu științele sociale (un reper de luat în seamă pentru fundamentarea metodologiei SOCINT).

Finalmente, țările implicate în testare folosesc CAST pentru autoevaluarea în baza unor criterii obiective, în cautarea reperelor propriei stabilități și performanțe.

Considerații privind topul statelor eșuate din perspectiva analizei SWOT³

Observăm din cele prezentate că afișarea consistentă a grijilor legate de statele eșuate au apărut în politica internațională după 1990, odată cu aplicarea principiului Westfalian al suveranității⁴ în funcție de alte criterii decât cele consacrate până atunci. Promotorul acestei noi terminologii - diplomația americană – s-a lansat în paralel în găsirea de soluții pentru nou identificatele provocări la adresa dinamicii de securitate globală.

În 1994, vicepreședintele SUA Al Gore stabilea instituția “State Failure Task Force” (Stohl și Stohl, 2001), compusă dintr-un grup de distinși academicieni care aveau ca sarcină, în cooperare cu agențiile guvernamentale, să analizeze factorii care duc la colapsul statal și să dezvolte scheme de acțiune pentru contracararea acestora. Ulterior, politica președintelui Clinton față de aceste state s-a bazat pe trei componente: acțiunea asupra cauzelor destabilizatoare din statele eșuate, promovarea securității colective și a capacității de reacție corelate cu nevoile (bazată pe ONU și NATO) și angajarea în diplomația preventivă.

¹ Datele în acest sens sunt îngrijorătoare: 73 milioane de persoane din 78 de țări depind de sprijinul acordat de United Nations World Food Programme (UNWFP) (<http://english.aljazeera.net/NR/exeres/958CC5D2-638C-428E-AF84-91041B355EF0.htm>); criza alimentelor afectează în prezent 37 țări și își are originile în: cererea tot mai mare de alimente (în special în țările beneficiare ale boom-ului economic, China și India), folosirea biocombustibililor, nivelul tot mai scăzut al stocurilor mondiale de hrană, speculațiile de pe piață, creșterea prețurilor la combustibili și a cheltuielilor de producție agricolă, modificările climatice și restricțiile de export (Pomeroy, f.a.). Șeful FMI a avertizat că înfometarea în masă poate duce la război și dezechilibre macroeconomice care să afecteze națiunile dezvoltate, dincolo de aspectul umanitar pe care îl implică efortul de rezolvare a crizei actuale. (*World Bank tackles food emergency*, <http://news.bbc.co.uk/2/hi/business/7344892.stm>)

² Anexa 3 prezintă câteva elemente de vizualizare dezvoltate în cadrul CAST pentru fiecare stat analizat – în acest caz, Afganistanul

³ Strengths, weaknesses, opportunities, threats/ puncte tari, puncte slabe, oportunități, amenințări

⁴ Sistemul interstatal, simbolizat de către tratatul de la Westfalia din 1648, a fost fondat pe principiul teritorialității și suveranității statelor. În interiorul frontierelor, ordinea este de apanajul autorităților statale, deținătoare ale monopolului violenței legitime, în timp ce viața internațională este caracterizată de anarhie.

În aprilie 2000, Comisia de Securitate Națională a S.U.A. (cunoscută și sub denumirea Hart – Rudman, de la numele componentilor) a elaborat un raport ce sublinia șase obiective-cheie de securitate națională a S.U.A. pentru primul sfert al secolului XXI. Comisia recomanda ca primă reacție în relația cu entități statale eșuate folosirea diplomației preventive, incluzând apelul la inițiative politice și economice. În caz de insucces, SUA trebuiau să fie pregătite să acționeze militar în cooperare cu alte națiuni în situații caracterizate de următoarele criterii (Stohl și Stohl, 2001):

- când state aliate/ prietene ale SUA erau în pericol;
- când apărea pericolul folosirii de arme de distrugere în masă care să afecteze populația civilă;
- când accesul sistemului economic global la resurse critice este pus în pericol;
- când un regim își demonstrează intenția de a aduce atingeri serioase intereselor SUA;
- în caz de genocid.

Comisia a considerat că existența premizelor unui singur factor din cei amintiți este suficient pentru a justifica o intervenție militară. În consecință, pe lângă statele care într-adevar suferă de tare politice, sociale, economice ce le deviază de la cursul normal al existenței, adâncindu-le în crize care duc, inevitabil, la catastrofe umanitare, există și state puse în poziția ori de a nu fi suficient de puternice (sau hotărâte) în a-și gestiona problemele interne – și de aici a risca neacceptarea lor ca fiind suverane de către alte state, fie să fie etichetate ca state eșuate pentru violarea drepturilor omului în încercarea lor de a-și menține securitatea internă. Această postură a războiului care nu se naște din puterea statului, ci din slăbiciunea sa (Pouligny, 2000), poate justifica intervențiile peste frontiere din motive legate de drepturile omului sau din rațiuni economice, în special când opțiunea intervenției aparține exclusiv statelor puternice care, în baza forței lor militare, își arogă privilegiul de a defini standardele drepturilor omului și echității economice (Liu, 2005).

În virtutea acestor considerente, deși algoritmul și logica analizei CAST sunt îmbietoare ca demers științific¹, ideea în sine de a realiza un „top” al statelor eșuate forțează etica relațiilor internaționale și stigmatizează oarecum întregul pe care statul îl reprezintă. Nu se pune problema aici de formalism și curtoazie proprii limbajului diplomatic. A spune despre un stat că este eșuat induce ideea de ireversibilitate a fenomenului și conferă o senzație de întrunire a tuturor tarelor abordate în cadrul sistemelor de referință anterior trecute în revistă.

Comentariile legate de acest subiect vădesc o stare de confuzie; accesând forumurile de discuții pe Internet având acest topic, observăm – pe lângă frustrarea unor participanți, cetățeni ai unor state listate în partea superioară a clasamentului, intervenții care demonstrează scoaterea din context a unor indicatori, nuanțarea unor abordări, apelul la evenimente mai mult sau mai puțin relevante, și – peste toate acestea – tendința de a compara.

Acest aspect îl considerăm important din următorul considerent: nimeni nu neagă problemele cu care o entitate statală se poate confrunta într-o anumită perioadă a existenței

¹ După cum evidențiază cercetătorii din cadrul celor două think-tankuri americane, metodologia CAST, permanent revizuită și perfecționată cu concursul unor experți și agenții din toate sectoarele de interes, prezentând garanția folosirii surselor alternative de informare, se constituie, în principiu, într-un instrument complex și viabil de analiză a stării generale a unui stat. În sprijinul acestei afirmații vine faptul că această metodologie este folosită de guverne ale mai multor state, printr-alte instrumente de analiză, pentru a obține avertizări timpurii și a desemna strategiile de asistență economică care pot reduce potențialul pentru conflict și să promoveze dezvoltarea în statele fragile. Uzul militar al CAST se regăsește în întărirea avertizărilor punctuale, perfecționarea gradului de pregătire și aplicarea de strategii de evaluare a succesului în operațiuni de stabilitate și pace. Sectorul privat folosește această metodologie pentru a calcula riscurile politice pentru oportunitățile de investiții. Organizațiile multinaționale și un segment al altor entități găsesc acest instrument util pentru modelarea și simularea de scenarii, managementul organizațiilor complexe și pentru evaluarea riscurilor conflictuale. Educatorii îl folosesc pentru a antrena studenții în analiza problemelor aferente stărilor de război și pace prin mixarea tehnicilor specifice tehnologiei informațiilor cu științele sociale. Finalmente, țările implicate în testare folosesc CAST pentru autoevaluare cu criterii obiective în căutarea reperelor proprii stabilități și performanțe.

sale istorice, este însă forțat a supune aceluiași complex de sisteme de referință state cu fundamente istorice și culturale radical diferite. Acest fapt poate alimenta șovinismul și se constituie în argumente ce justifică intervenționismul.

În plus, apare întrebarea privind independența de opinie și neutralitatea instituțiilor care au întocmit acest index¹. Legat de aceasta, fragilitatea credibilității unui astfel de top se învârtă în posibilitatea influențării scorului în sensul dictat de anumite interese. În virtutea rațiunilor anterior amintite, unele state pot „aluneca” pe o pantă care să justifice măsuri radicale favorabile jucătorului din umbră, în timp ce state care prezintă mari neajunsuri raportat la criteriile așa zis „generale” ale eșuării pot fi recompensate cu o poziție favorabilă pe listă în funcție de atitudinea pe care o au față de superputere și de serviciile pe care le aduc acestea.

Cu rezerva acestor obiecții considerăm, totuși, că rezultatul acestui demers se constituie într-un instrument analitic util pentru diagnosticarea slăbiciunilor sistemelor statale, primul pas în conturarea strategiilor pentru întărirea statelor aflate în declin, un excelent reper pentru dezvoltarea unor studii aprofundate punctuale, având ca finalitate definirea complexă a situației unui anumit stat, mai ales în condițiile în care se apelează la corelarea datelor statistice cu informații valide legate de specificul evoluției istorice și a valențelor culturale care definesc profilul respectivei entități.

Cu cât factorii de decizie avizați pot anticipa, monitoriza și măsura problemele, cu atât mai mult pot fi prevenite căderi violente, proteja civilii aflați în zone de conflict și promova refacerea și recuperarea. În același timp, politicienii trebuie să se concentreze în construirea capacității instituționale a statului slăbit, în principal a celor cinci instituții de bază: cea militară, poliția, serviciile civile, sistemul de justiție și conducerea. Politicile în acest sens trebuie ajustate nevoilor concrete ale statului, monitorizate și evaluate permanent, ajustate în funcție de necesități, toate acestea între reperele unei tot mai necesare științe a reclădirii statale.

În ce privește termenul de “stat eșuat”, sugestivitatea sa l-a consacrat în limbajul profan, dar și cel științific. În mod firesc, datorită încărcăturii sale aparte, acesta nu poate fi în nici un caz folosit în limbajul diplomatic.

Dincolo de abordarea critică a problematicii topului statelor eșuate, dorim să atragem atenția asupra realităților de strictă actualitate care zugrăvesc spectacolul sumbru al scenelor de violență din anumite zone fierbinți ale globului, precum și perspectivele oferite de consecințele unor decizii politice. Toate acestea sunt însoțite de indicatori și avertizări ce intră în sfera de interes a entităților specializate în prognozarea și modelarea evoluției unor astfel de situații.













Bibliografie

¹ Din propria prezentare, Fund for Peace este o instituție specializată în diagnoza și evoluția conflictelor asociate statelor slăbite și a reacțiilor de politică externă la astfel de fenomene, organizația asumându-și rolul de a promova conceptul de securitate sustenabilă și a cultiva abilitatea societăților de a-și rezolva problemele în mod pașnic, fără o prezență militară sau administrativă străină (<http://www.fundforpeace.org/publications/annual/ar2006.pdf>). "Foreign Policy" este o revistă de politică, economie și relații internaționale care a fost lansată în 1970 în S.U.A. și este editată de think-tankul The Carnegie Endowment for International Peace (CEIP), în mod formal o organizație non-profit privată, care își asumă non-partizananul, în practică puternic asociată cu United States Department of State, mulți dintre președinții SUA, numeroase grupuri de afaceri străine private și liderii partidelor politice mari din SUA (http://en.wikipedia.org/wiki/Carnegie_Endowment_for_International_Peace). A se vedea în acest sens și lista cu sponsorii care finanțează think – tankul, disponibilă pe websiteul acestuia (<http://www.carnegieendowment.org/about/index.cfm?fa=funding>), unde pot fi regăsite nume proeminente din diferite domenii de interes. CEIP se autodefineste ca promotoare a unui angajament global activ al S.U.A. și caută să contureze formule de exercitare a unui leadership pozitiv și constructiv al acestora la nivel global.

1. BĂHNĂREANU, Cristian (2005) *Puterea militară în secolul XXI. Modalități de realizare și manifestare a puterii militare în societatea democratică românească*, Editura Universității Naționale de Apărare, București
2. CHOMSKY, Noam (2006) *Failed States: The Abuse of Power and the Assault on Democracy* în http://www.democracynow.org/2006/3/31/exclusive_noam_chomsky_on_failed_states
3. FRUNZETI, Teodor; ZODIAN, Vladimir, (2007) *Lumea 2007: enciclopedie politico – militara; studii strategice și de securitate*, Editura Centrului Tehnic – Editorial al Armatei, București
4. LIU, Henry C. K., (2005) *The failed-state cancer*, in http://www.atimes.com/atimes/Front_Page/GD28Aa02.html
5. MUNTARBHORN, Vitit (2006) *Fragile Countries and United Nations Reform*, *Bangkok Post*, February 23, în <http://www.globalpolicy.org/nations/sovereign/failedindex.htm>
6. NAKAMURA, Madoka (2002) Center for Policy Research Information, National Institute for Research Advancement – Introduction, <http://www.nira.go.jp/ice/nwdtt/2005/intro/intro2002.html>
7. POMEROY, Robin (2008) *Warning of food riots as world cereal prices hit record highs*, în <http://news.scotsman.com/world/Warning-of-food-riots-.3975494.jp>
8. POULIGNY, Béatrice (2000) *Un seul monde, un monde pour tous ? Interventions militaires et régulation des conflits*, in <http://www.ceras-projet.com/index.php?id=2062>
9. PRADOS, Alfred B. (2001) *Middle East: Attitudes toward the United States (CRS Report for Congress)*, Congressional Research Service, the Library of Congress
10. RANCOURT, Jean-François (2005) « *Rogue States* », *un concept incompatible avec la politique étrangère canadienne*, Chaire de recherche du Canada en politiques étrangère et de défense, Vol. 6, no 1 (19 janvier 2005), in <http://www.er.uqam.ca/nobel/cepes>
11. STOHL, Rachel; STOHL, Michael (2001) *Fatally Flawed? U.S. Policy Toward Failed States*, în *The Defense Monitor*, Volume XXX, no. 8
12. The African Studies Centre (Leiden), The Transnational Institute (Amsterdam), The Center of Social Studies/ Coimbra University, The Peace Research Center CIP-FUHEM (Madrid) (2003) *Failed and collapsed states in the international system*, în <http://www.globalpolicy.org/nations/sovereign/failed/2003/12failedcollapsedstates.pdf>
13. THÜRER, Daniel (1999) *The "Failed State" And International Law*, *International Committee Of The Red Cross*, December 31, în <http://www.globalpolicy.org/nations/sovereign/failedindex.htm>
14. *** (2005) *Un parfum de Guerre froide*, în <http://www.voltairenet.org/article16092.html>
15. *** (2008) *World Bank tackles food emergency*, în <http://news.bbc.co.uk/2/hi/business/7344892.stm>
16. <http://commons.wikimedia.org/wiki>
17. <http://data.worldbank.org/topic>
18. http://en.wikipedia.org/wiki/Carnegie_Endowment_for_International_Peace
19. http://en.wikipedia.org/wiki/Crisis_States_Research_Centre
20. http://en.wikipedia.org/wiki/Fund_for_Peace
21. http://en.wikipedia.org/wiki/List_of_countries_by_Failed_States_Index
22. <http://english.aljazeera.net/NR/exeres/958CC5D2-638C-428E-AF84-91041B355EF0.htm>
23. <http://ffp.statesindex.org/afghanistan>
24. <http://ffp.statesindex.org/rankings-2013-sortable>
25. <http://hdr.undp.org/en/data>
26. <http://www.carnegieendowment.org/about/index.cfm?fa=funding>
27. <http://www.fundforpeace.org/publications/annual/ar2006.pdf>
28. <http://www.fundforpeace.org/thefund/president.php>
29. <http://www.heritage.org/index/>
30. <http://www.imf.org/external/pubs/ft/gfsr/about.htm>
31. <http://www.imf.org/external/pubs/ft/weo/2014/update/01/>
32. http://www.sourcewatch.org/index.php?title=Think_tanks&oldid=283573
33. <https://www.fitchratings.com/web/en/dynamic/fitch-home.jsp#>

ANEXE

ANEXA NR. 1 – TOPUL STATELOR EȘUATE 2013¹

Rank	Country													Total
1	Somalia	9.5	10.0	9.3	8.9	8.4	9.4	9.5	9.8	10.0	9.7	10.0	9.4	113.9
2	Congo (D. R.)	10.0	10.0	9.4	7.1	8.8	8.5	9.6	9.5	9.8	10.0	9.5	9.7	111.9
3	Sudan	8.8	10.0	10.0	8.4	8.5	7.8	9.6	8.8	9.3	9.8	10.0	10.0	111.0
4	South Sudan	8.9	10.0	10.0	6.5	8.9	8.6	9.1	9.8	9.3	9.6	9.8	10.0	110.6
5	Chad	9.5	9.7	8.8	8.0	8.9	8.0	9.7	9.9	9.8	9.4	9.5	7.9	109.0
6	Yemen	9.3	9.2	9.0	7.4	8.1	9.2	9.3	8.7	8.7	9.8	9.5	8.7	107.0
7	Afghanistan	9.3	9.2	9.2	7.2	7.8	8.2	9.4	8.8	8.4	9.9	9.4	10.0	106.7
8	Haiti	9.6	8.6	7.0	9.1	9.1	9.7	8.8	9.6	7.6	7.9	9.0	9.9	105.8
9	Central African Republic	8.6	9.8	8.5	6.1	9.2	7.7	9.0	9.5	8.6	9.7	9.1	9.4	105.3
10	Zimbabwe	9.2	8.7	8.4	8.6	8.6	8.6	9.2	9.1	8.9	8.4	9.7	7.8	105.2
11	Iraq	8.3	8.8	10.0	8.3	8.4	7.3	8.6	7.6	8.6	10.0	9.6	8.5	103.9
12	Cote d'Ivoire	7.8	9.3	9.0	7.3	7.8	7.7	9.3	8.5	8.6	9.1	9.4	9.7	103.5
13	Pakistan	8.9	9.1	9.7	6.9	7.9	7.5	8.4	7.3	8.7	9.8	9.2	9.6	102.9
14	Guinea	8.4	8.2	7.6	7.7	8.2	9.2	9.8	8.9	8.4	9.1	8.9	7.0	101.3
15	Guinea Bissau	8.4	7.8	5.7	8.0	8.1	8.7	9.7	8.8	7.6	9.5	9.7	9.0	101.1
16	Nigeria	8.5	6.6	9.8	7.3	9.2	7.5	8.8	9.3	8.6	9.5	9.4	6.3	100.7
17	Kenya	9.1	8.7	9.0	7.8	8.3	7.6	8.3	8.1	7.1	8.1	9.0	8.5	99.6
18	Niger	9.8	7.9	7.8	6.3	7.9	8.4	8.1	9.5	7.6	8.3	8.9	8.5	99.0
19	Ethiopia	9.7	8.7	8.6	6.7	7.6	7.7	7.3	8.7	8.7	8.4	8.7	8.1	98.9
20	Burundi	8.9	8.8	8.1	6.2	7.6	9.1	8.4	8.3	7.9	7.7	7.9	8.7	97.6
21	Syria	5.6	9.5	9.3	6.2	7.2	6.4	9.6	7.0	9.5	9.8	9.2	8.1	97.4
22	Uganda	9.1	8.4	8.0	6.7	7.8	7.4	8.1	8.3	7.9	8.2	8.6	8.2	96.6
23	North Korea	8.0	5.0	6.6	4.4	8.3	9.3	9.8	9.5	9.7	8.4	7.7	8.4	95.1
23	Liberia	8.8	9.2	6.5	7.0	8.0	8.3	6.6	9.1	6.4	7.1	8.3	9.8	95.1
25	Eritrea	8.7	7.4	6.1	7.3	6.9	8.3	8.7	8.4	9.1	7.5	8.1	8.6	95.0
26	Myanmar	7.6	8.5	9.0	5.4	8.4	7.3	9.0	8.1	8.3	7.8	8.6	6.6	94.6
27	Cameroon	8.3	7.3	7.8	7.2	7.8	6.1	8.5	8.4	8.1	8.0	9.2	6.8	93.5
28	Sri Lanka	6.8	8.4	9.5	7.3	7.8	5.9	8.2	5.5	9.0	8.5	9.3	6.8	92.9
29	Bangladesh	8.1	7.3	8.6	7.5	7.8	7.3	8.3	8.0	7.3	7.7	8.9	5.8	92.5

¹ <http://ffp.statesindex.org/rankings-2013-sortable>

30	Nepal	7.6	7.7	9.0	5.9	8.1	7.3	8.1	7.3	7.9	7.6	8.2	7.1	91.8
31	Mauritania	8.5	8.3	7.2	5.7	6.5	8.0	7.7	8.4	7.4	7.8	8.2	7.9	91.7
32	Timor-Leste	8.7	7.4	6.8	6.4	6.7	7.9	8.0	8.5	6.0	8.3	8.3	8.5	91.5
33	Sierra Leone	9.0	8.1	5.9	8.0	8.5	8.6	7.3	9.0	6.1	5.4	7.9	7.4	91.2
34	Egypt	7.2	6.5	8.5	5.4	7.1	8.2	8.9	5.6	9.6	7.3	8.7	7.7	90.6
35	Burkina Faso	9.4	7.4	5.3	6.3	8.4	7.7	7.7	8.7	6.8	7.2	7.3	8.0	90.2
36	Congo (Republic)	8.2	8.0	6.0	6.2	8.2	7.0	8.7	8.7	7.5	6.7	6.7	8.2	90.0
37	Iran	5.5	7.3	8.8	6.1	6.7	6.5	8.9	5.0	9.4	8.6	9.4	7.5	89.7
38	Mali	9.3	7.6	7.6	7.8	6.8	8.1	6.0	8.5	6.5	8.1	5.0	8.0	89.3
38	Rwanda	8.4	7.9	8.2	6.9	7.7	6.7	6.5	7.6	7.7	5.5	8.2	8.0	89.3
40	Malawi	8.9	6.5	5.7	8.1	8.0	8.4	7.5	8.2	6.8	5.0	7.6	8.4	89.2
41	Cambodia	7.2	6.2	7.0	7.4	7.3	6.4	8.3	8.1	7.8	6.2	8.0	8.0	88.0
42	Togo	8.2	7.1	4.8	6.8	7.6	7.4	8.3	8.3	7.8	7.4	7.5	6.5	87.8
43	Angola	8.9	7.2	6.8	5.9	9.4	5.1	8.6	8.4	7.3	6.1	7.3	6.1	87.1
44	Uzbekistan	6.7	6.0	7.5	6.3	7.6	7.2	9.0	5.4	9.2	7.9	8.7	5.4	86.9
45	Zambia	9.3	7.4	6.0	7.4	8.0	8.3	8.0	7.6	6.7	5.0	5.7	7.2	86.6
46	Lebanon	6.3	8.5	8.5	6.0	6.2	5.3	7.2	5.6	6.8	8.5	9.2	8.2	86.3
47	Equatorial Guinea	8.3	3.3	6.6	6.6	9.1	4.5	9.6	7.6	9.4	7.5	8.2	5.5	86.1
48	Kyrgyzstan	6.2	5.6	8.4	6.4	7.0	7.6	8.4	5.9	7.6	7.4	8.0	7.3	85.7
49	Swaziland	9.0	4.9	3.6	6.3	7.5	8.9	8.7	7.8	8.3	6.0	7.0	7.5	85.6
50	Djibouti	8.3	7.2	6.2	5.2	7.3	6.9	7.8	7.4	7.0	6.6	7.5	8.1	85.5
51	Tajikistan	7.4	5.3	6.7	5.9	6.2	8.0	9.1	6.3	8.2	7.4	8.3	6.4	85.2
51	Solomon Islands	7.7	4.9	6.8	5.7	8.3	7.8	7.3	8.0	5.9	6.7	8.0	8.2	85.2
53	Papua New Guinea	7.6	5.0	6.6	7.5	9.1	6.9	7.1	8.9	6.2	6.6	7.1	6.3	84.9
54	Libya	5.5	5.4	7.4	4.2	6.7	5.0	8.4	7.3	9.0	8.9	8.0	8.8	84.5
55	Georgia	5.2	7.5	8.0	5.2	6.3	6.4	8.6	5.4	6.4	7.9	9.4	7.9	84.2
56	Comoros	7.4	4.5	5.3	7.2	6.4	8.2	7.4	7.9	6.6	7.5	7.5	8.1	84.0
57	Colombia	6.5	8.3	7.5	7.3	8.1	3.8	7.3	6.1	7.3	6.8	7.7	7.1	83.8
58	Laos	7.5	5.8	6.1	6.8	6.1	5.7	8.6	7.3	8.3	6.6	8.3	6.6	83.7
59	Mozambique	9.2	4.6	4.9	7.2	8.0	8.0	7.0	8.5	6.4	6.5	5.6	6.8	82.8
59	Philippines	7.1	6.5	7.9	6.2	6.5	5.6	7.6	6.4	6.7	8.7	8.0	5.5	82.8
61	Madagascar	8.1	4.3	4.9	5.5	7.9	8.2	7.2	8.6	5.9	7.0	7.5	7.7	82.7
62	Gambia	7.7	6.4	3.7	7.1	6.8	7.8	7.6	7.5	8.0	5.5	6.8	6.9	81.8
62	Bhutan	6.4	6.9	7.3	6.8	7.5	6.3	6.0	6.9	7.3	5.6	7.5	7.3	81.8
64	Senegal	8.3	7.0	6.3	6.8	6.8	7.2	5.9	7.8	6.2	6.2	6.6	6.3	81.4

65	Tanzania	8.6	6.8	6.0	6.4	6.4	6.8	6.2	8.8	6.2	5.5	5.7	7.7	81.1
66	China	8.1	6.1	8.3	5.0	8.0	3.6	8.1	6.8	9.4	6.5	7.2	3.8	80.9
67	Israel/West Bank	6.2	7.4	9.8	3.2	7.5	3.7	6.7	5.9	7.6	7.1	8.1	7.7	80.8
67	Fiji	5.2	3.8	7.3	7.0	7.4	7.3	8.8	4.9	7.3	7.0	7.9	6.9	80.8
67	Bolivia	6.9	4.0	7.1	6.4	8.9	6.2	7.2	6.8	6.3	6.7	8.0	6.3	80.8
70	Guatemala	7.3	6.0	7.3	7.1	8.1	6.1	6.9	6.9	6.6	7.0	6.0	5.4	80.7
71	Lesotho	8.8	4.9	4.7	6.8	6.7	8.5	6.0	8.2	5.4	5.2	7.0	7.2	79.4
72	Nicaragua	6.6	4.8	5.9	7.8	7.9	6.8	7.5	6.8	5.4	5.6	6.8	7.3	79.2
73	Algeria	5.8	7.0	7.8	5.1	6.2	5.8	7.4	5.9	7.7	7.4	7.3	5.2	78.7
74	Ecuador	5.8	5.7	7.2	6.8	7.4	5.6	7.2	6.9	4.9	6.7	8.2	6.2	78.6
75	Honduras	7.0	3.9	5.8	6.6	8.1	6.9	6.9	6.8	6.3	6.8	6.3	6.9	78.3
76	Azerbaijan	5.3	7.9	6.9	4.7	6.1	4.7	8.2	5.1	7.6	6.9	7.8	6.9	78.2
76	Indonesia	7.5	6.0	7.3	6.3	6.9	5.5	6.4	6.1	6.5	6.8	7.0	5.9	78.2
78	Benin	8.3	6.5	3.6	6.2	7.2	7.1	6.0	8.6	5.1	5.8	6.1	7.3	77.9
79	India	7.5	5.2	8.2	5.4	8.1	5.4	5.2	6.7	5.9	7.8	6.8	5.2	77.5
80	Russia	5.7	5.3	8.2	5.1	7.0	3.5	8.1	5.1	8.6	8.5	8.0	4.0	77.1
81	Turkmenistan	5.9	3.9	6.7	4.9	6.5	5.4	9.3	6.1	8.7	7.1	7.7	4.6	76.7
81	Belarus	5.7	3.6	6.8	3.9	5.7	6.2	9.0	5.2	8.3	6.3	8.3	7.6	76.7
83	Bosnia	4.4	6.8	7.7	5.6	6.2	5.2	6.7	4.4	6.4	6.4	8.7	8.0	76.5
83	Moldova	5.9	5.0	6.0	6.9	5.9	6.4	6.9	5.7	6.0	7.2	7.7	6.9	76.5
83	Tunisia	4.9	4.2	7.8	5.0	6.0	6.0	7.9	5.0	8.4	7.2	7.8	6.3	76.5
86	Turkey	5.7	7.4	9.0	3.9	6.8	5.3	5.9	5.5	5.5	7.9	7.3	5.6	75.9
87	Jordan	6.7	7.8	7.1	4.2	6.5	6.5	6.5	4.3	7.4	5.8	6.8	6.2	75.7
88	Maldives	5.4	5.3	4.9	6.2	4.4	6.5	8.3	6.7	7.6	5.8	8.0	6.4	75.4
89	Venezuela	5.4	4.8	6.4	5.8	6.9	5.4	7.6	6.5	7.7	6.5	7.3	4.9	75.3
90	Thailand	7.9	6.4	8.1	3.5	6.4	3.5	6.2	4.6	7.3	7.8	8.8	4.6	75.1
91	Sao Tome	6.6	4.3	4.8	7.9	6.3	7.9	6.6	6.4	4.3	5.8	6.3	7.3	74.6
92	Serbia	4.7	6.6	8.0	4.7	5.9	6.5	6.3	4.7	5.5	6.5	8.0	7.0	74.4
93	Morocco	5.8	5.9	6.5	7.0	6.9	5.3	6.7	5.9	6.6	6.3	6.6	4.9	74.3
94	Cape Verde	6.7	4.1	4.2	8.3	6.9	6.1	6.3	6.5	5.1	5.7	5.5	8.2	73.7
95	Dominican Republic	6.4	5.5	6.1	7.9	6.9	5.5	5.4	6.2	5.7	5.2	6.5	5.9	73.2
95	El Salvador	7.4	5.5	5.7	6.9	7.0	6.5	5.9	6.5	6.1	6.4	4.3	5.1	73.2
97	Mexico	6.5	4.0	6.1	5.9	7.2	5.2	6.1	6.6	6.3	7.9	5.2	6.1	73.1
97	Vietnam	5.9	4.7	5.7	5.7	5.8	6.2	7.8	5.8	7.5	5.4	6.9	5.6	73.1
99	Micronesia	7.1	3.1	4.2	8.4	8.0	7.5	6.3	6.3	3.1	5.4	5.6	7.9	72.9

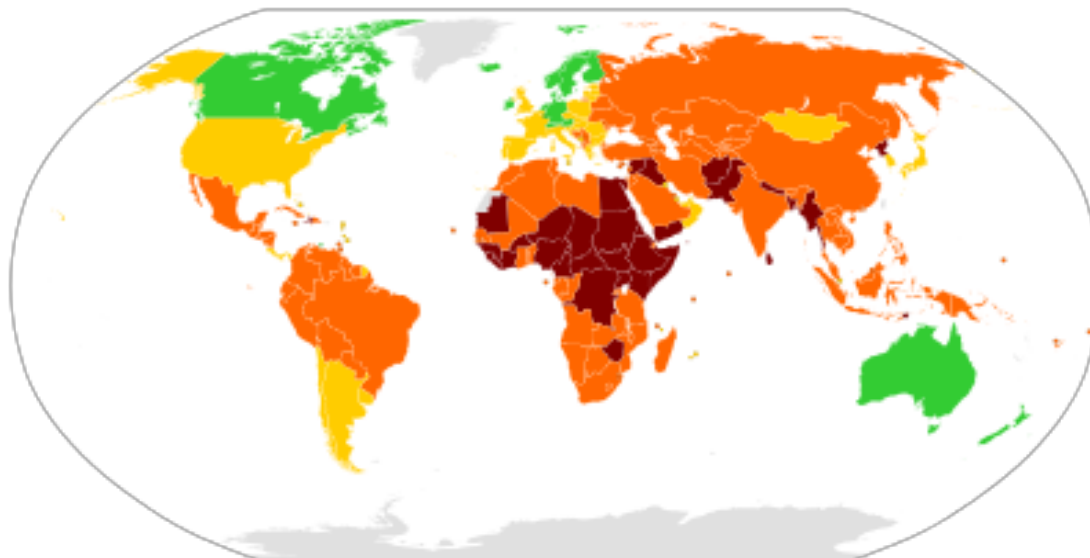
99	Gabon	6.8	5.6	3.3	5.5	7.3	5.2	7.6	7.0	6.8	5.4	7.1	5.4	72.9
101	Cuba	6.6	5.3	4.8	6.3	5.9	5.2	6.5	4.7	7.5	6.3	6.9	6.7	72.8
102	Saudi Arabia	5.5	5.2	7.4	3.1	6.4	3.6	7.8	4.0	8.9	7.2	8.0	5.6	72.7
103	Peru	5.9	4.7	7.0	6.1	7.8	4.1	7.1	6.4	5.0	7.0	6.7	4.5	72.3
104	Paraguay	6.1	2.4	6.5	4.9	8.6	5.1	7.9	6.1	6.1	6.1	7.9	4.2	71.8
105	Armenia	4.9	7.0	5.7	6.0	5.6	5.9	6.6	4.4	6.8	5.3	7.0	6.2	71.3
106	Suriname	5.7	3.0	6.1	7.6	7.0	7.1	6.1	5.3	5.4	5.8	5.8	6.3	71.2
107	Guyana	5.8	3.8	5.9	8.5	6.8	6.6	6.2	6.0	4.4	5.8	5.1	5.9	70.8
108	Namibia	6.9	5.6	5.3	6.5	8.7	6.7	4.1	6.7	4.9	4.9	3.5	6.5	70.4
109	Kazakhstan	5.3	3.8	6.2	3.6	5.3	6.2	7.8	5.1	7.1	6.4	7.7	5.3	69.8
110	Ghana	6.7	5.5	4.9	7.3	6.5	6.1	5.1	7.6	4.7	3.8	5.0	6.0	69.1
111	Samoa	6.8	2.5	4.8	8.8	6.0	5.9	6.0	4.8	4.5	5.5	5.1	8.0	68.7
112	Macedonia	3.9	5.2	7.8	6.1	6.2	5.9	6.1	3.9	4.3	6.0	7.0	5.6	68.0
113	South Africa	7.8	6.5	5.7	4.3	8.0	5.9	5.3	6.3	4.2	5.1	5.6	2.9	67.6
114	Belize	6.5	4.9	4.4	7.1	6.6	5.5	6.0	6.0	4.1	5.5	4.3	6.3	67.2
115	Cyprus	4.0	4.4	7.3	4.8	7.0	5.8	5.5	3.0	3.3	5.0	7.9	9.0	67.0
116	Malaysia	5.6	4.6	6.1	4.8	5.9	4.1	6.2	4.5	7.1	6.0	6.8	4.4	66.1
117	Ukraine	4.7	3.2	5.9	5.7	5.3	5.4	7.8	3.6	5.7	4.4	8.0	6.2	65.9
118	Jamaica	5.6	3.4	4.0	7.2	5.9	6.6	6.1	5.7	5.0	6.3	3.7	6.3	65.6
119	Albania	4.7	3.1	4.8	6.6	4.8	5.3	7.0	4.8	6.0	5.5	6.3	6.3	65.2
120	Grenada	5.2	3.2	3.9	8.5	5.9	5.8	6.2	3.6	3.7	5.3	5.6	7.7	64.6
121	Seychelles	5.2	3.3	4.8	4.9	6.6	5.2	6.3	3.5	5.2	6.4	5.7	6.9	64.0
121	Botswana	8.3	5.8	4.8	5.0	7.5	6.1	4.4	6.0	4.4	3.5	3.3	4.8	64.0
123	Brunei	4.5	3.3	6.2	4.6	7.8	2.8	7.4	2.6	6.9	5.6	7.4	4.1	63.2
124	Bahrain	4.6	2.5	7.3	3.3	5.7	3.2	7.6	2.4	7.5	6.1	7.1	5.6	62.9
125	Trinidad	5.3	3.0	4.4	7.8	6.1	4.6	5.6	5.2	5.2	5.7	5.6	4.2	62.6
126	Brazil	7.0	3.6	5.9	3.9	8.3	3.3	5.3	5.4	5.3	5.9	4.9	3.3	62.1
127	Kuwait	5.1	3.8	4.6	3.7	5.3	3.4	7.6	2.6	6.8	4.4	7.9	4.4	59.6
128	Antigua & Barbuda	4.6	3.0	4.1	7.6	5.6	4.5	5.8	4.0	4.4	4.9	3.7	5.8	58.0
129	Mongolia	5.5	2.2	3.7	2.5	6.3	4.7	5.3	5.7	5.4	4.4	5.5	6.5	57.8
130	Romania	4.3	2.7	6.3	4.7	5.3	5.7	6.4	4.3	3.9	4.1	5.2	4.6	57.4
131	Panama	5.9	3.7	5.0	4.5	7.9	3.8	4.7	5.0	4.4	5.1	2.5	3.3	55.8
132	Bulgaria	4.4	3.1	4.6	4.9	5.1	5.0	4.8	4.4	3.7	4.7	5.3	5.0	55.0
133	Bahamas	6.6	2.8	4.4	5.6	5.6	4.5	4.9	4.4	2.8	4.3	4.5	4.3	54.7
134	Montenegro	3.9	4.5	6.5	3.0	3.5	4.6	4.2	3.6	4.4	4.6	6.2	5.3	54.4

135	Croatia	3.7	5.5	5.3	4.4	4.4	5.1	3.9	2.9	4.7	4.8	4.4	5.0	54.1
136	Oman	5.0	2.0	2.7	1.8	3.6	4.5	6.1	4.4	7.5	5.3	6.6	2.4	52.0
137	Barbados	3.8	2.7	4.4	6.2	5.7	5.8	3.6	2.7	2.5	4.2	4.2	5.0	50.8
138	Greece	4.3	2.0	4.8	4.4	4.3	6.4	5.4	3.9	3.0	3.9	3.0	5.1	50.6
139	Costa Rica	4.9	4.1	4.1	3.5	6.1	4.3	3.5	4.6	2.4	2.5	3.8	4.9	48.7
140	Latvia	3.6	3.3	5.4	4.2	4.9	4.0	4.5	3.4	3.2	3.3	4.3	3.8	47.9
141	Hungary	2.5	2.9	4.1	3.9	4.9	6.0	5.9	3.1	3.4	2.3	4.8	3.8	47.6
142	United Arab Emirates	3.9	2.5	4.3	2.4	4.8	3.5	6.5	2.9	6.4	2.9	3.6	3.5	47.3
143	Qatar	4.3	2.1	4.9	3.1	4.8	2.9	5.9	2.0	5.6	2.5	5.0	4.0	47.1
144	Argentina	4.1	2.0	5.0	3.0	6.0	4.0	4.4	3.9	4.1	3.0	2.7	3.8	46.1
145	Estonia	3.5	3.3	5.9	3.9	4.3	3.5	3.8	3.0	2.4	2.9	5.5	3.3	45.3
145	Slovakia	3.2	2.0	5.0	4.5	4.6	5.2	4.3	3.5	3.0	2.3	3.7	3.9	45.3
147	Italy	3.8	3.3	4.7	2.6	3.6	4.8	4.7	2.4	2.9	5.0	4.8	2.0	44.6
148	Mauritius	3.8	2.2	3.5	3.6	4.8	4.1	4.1	3.8	3.5	3.3	3.2	4.6	44.5
149	Spain	2.8	2.3	5.8	3.0	4.1	5.5	3.3	3.3	2.2	4.1	6.0	2.0	44.4
150	Lithuania	3.8	2.9	3.7	4.1	5.2	4.5	3.8	3.4	2.9	2.5	3.0	3.2	43.0
151	Malta	2.8	5.2	4.0	4.1	3.5	3.6	4.1	2.3	3.3	3.7	2.0	3.8	42.4
152	Chile	4.9	2.4	3.5	2.8	5.5	4.1	3.8	4.3	3.5	2.9	1.4	3.2	42.3
153	Poland	3.5	2.8	3.8	5.0	3.9	3.5	3.4	2.8	2.9	2.5	3.6	3.3	40.9
154	Czech Republic	2.5	2.2	3.8	3.4	3.8	4.5	4.1	3.7	2.4	2.1	4.2	3.2	39.9
155	Uruguay	3.8	1.9	2.8	4.7	4.4	3.6	1.7	3.4	2.3	3.7	2.7	3.5	38.4
156	Japan	5.4	3.7	3.8	2.0	1.8	3.7	2.2	2.5	3.0	1.7	2.6	3.7	36.1
157	South Korea	3.0	2.0	3.1	3.9	2.9	2.0	2.9	1.9	2.6	2.1	3.6	5.4	35.4
158	Singapore	2.5	1.1	2.7	3.3	3.7	3.0	3.2	1.9	4.9	1.5	4.0	2.2	34.0
159	United States	3.0	2.3	4.2	1.0	4.8	3.2	2.3	2.4	3.2	2.2	3.9	1.0	33.5
160	United Kingdom	2.5	2.7	5.0	2.1	3.6	4.1	1.6	2.3	1.8	2.7	3.5	1.3	33.2
161	France	2.7	2.2	5.9	1.9	4.3	4.0	2.2	1.5	2.4	2.3	1.9	1.4	32.6
161	Portugal	2.8	1.6	2.3	2.6	3.4	5.4	2.1	3.5	2.7	1.6	1.3	3.3	32.6
163	Slovenia	2.5	1.4	3.3	3.2	4.5	3.6	2.8	2.1	2.5	2.5	1.6	2.3	32.3
164	Belgium	2.5	1.6	4.1	1.8	3.8	3.5	2.1	2.2	1.5	2.0	3.9	2.0	30.9
165	Germany	2.4	3.6	4.3	2.2	3.9	2.6	1.4	1.8	1.9	2.2	2.0	1.4	29.7
166	Austria	2.3	2.4	4.3	1.6	4.0	1.9	1.5	1.5	2.0	1.1	2.7	1.6	26.9
166	Netherlands	3.0	2.4	4.1	2.2	2.3	3.5	1.0	1.5	1.0	1.8	2.6	1.5	26.9
168	Canada	2.6	2.1	3.1	2.1	3.5	1.8	1.5	2.0	2.0	1.8	2.5	1.0	26.0

169	Australia	3.3	2.7	3.6	1.1	3.3	2.1	1.0	1.8	2.2	1.7	1.6	1.0	25.4
170	Ireland	2.2	1.4	1.6	2.8	2.5	3.9	1.9	1.9	1.3	1.8	1.3	2.2	24.8
171	Iceland	1.6	1.6	1.0	2.8	1.7	3.7	1.4	1.6	1.3	1.0	1.8	5.2	24.7
172	Luxembourg	1.7	1.8	2.8	2.1	1.5	1.5	1.9	1.3	1.0	2.3	3.4	2.0	23.3
173	New Zealand	2.1	1.1	3.5	2.4	3.4	3.6	0.5	1.8	1.2	1.1	1.1	1.0	22.7
174	Denmark	2.5	1.6	3.4	1.9	1.6	1.9	1.0	1.4	1.7	1.5	1.4	2.0	21.9
175	Switzerland	2.1	1.5	3.5	2.1	2.3	2.3	0.8	1.4	1.7	1.4	1.0	1.4	21.5
175	Norway	2.0	1.9	3.6	1.6	1.5	1.9	0.5	1.4	1.9	2.7	1.1	1.3	21.5
177	Sweden	2.5	2.4	1.0	1.7	1.7	1.7	0.5	1.9	1.3	2.2	1.8	1.0	19.7
178	Finland	1.9	1.6	1.4	2.3	1.0	3.2	1.0	1.5	1.1	1.0	1.1	1.0	18.0

Copyright (C) 2013 The Fund for Peace

ANEXA NR. 2 – PLANIGLOB – TOPUL STATELOR ESUATE 2013¹



Legenda

- State la nivel de alertă
- State la nivel de avertizare
- State stabile
- State sustenabile

¹ <http://ffp.statesindex.org/rankings-2013-sortable>

ANEXA NR. 3 – OPTIUNI DE VIZUALIZARE ALE CAST - AFGANISTAN¹

Fragile States Index Score	Fragile States Index Rank	Average Indicator Score	Year-on-Year Trend
106.0 of 178 countries	6th of 178 countries	8.8 Maximum 10.0	-1.5 Improved since 2013

ALERT	WARNING	STABLE	SUSTAINABLE
Current Pressures Assessment			
High Alert			

Indicator-by-Indicator in 2014

DP	REF	GG	HF	UED	ECO	SL	PS	HR	SEC	FE	EXT
9.3	9.2	9.2	7.2	7.8	8.2	9.4	8.8	8.4	9.9	9.4	10.0
EXCELLENT GOOD MODERATE WEAK POOR	EXCELLENT GOOD MODERATE WEAK POOR	EXCELLENT GOOD MODERATE WEAK POOR	EXCELLENT GOOD MODERATE WEAK POOR	EXCELLENT GOOD MODERATE WEAK POOR	EXCELLENT GOOD MODERATE WEAK POOR	EXCELLENT GOOD MODERATE WEAK POOR	EXCELLENT GOOD MODERATE WEAK POOR	EXCELLENT GOOD MODERATE WEAK POOR	EXCELLENT GOOD MODERATE WEAK POOR	EXCELLENT GOOD MODERATE WEAK POOR	EXCELLENT GOOD MODERATE WEAK POOR

Year-on-Year Trend Since 2013

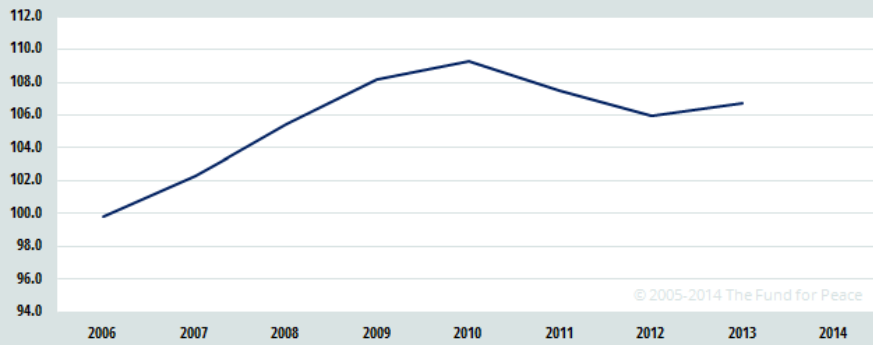
DP	REF	GG	HF	UED	ECO	SL	PS	HR	SEC	FE	EXT
+0.4	+0.2	-0.2	-0.1	-0.3	+0.5	-0.1	+0.3	-0.1	+0.2	0.0	0.0
WORSENERD	WORSENERD	IMPROVED	IMPROVED	IMPROVED	WORSENERD	IMPROVED	WORSENERD	IMPROVED	WORSENERD	UNCHANGED	UNCHANGED

Five Year Trend Since 2009

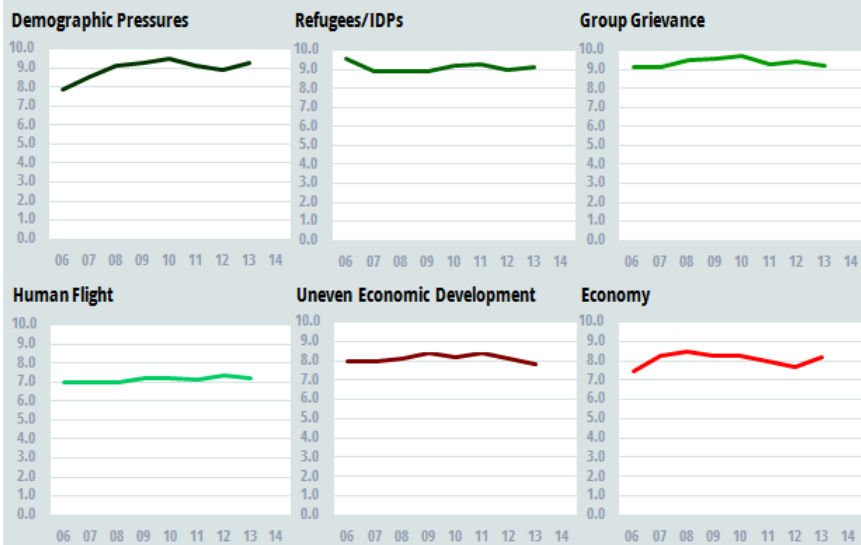
DP	REF	GG	HF	UED	ECO	SL	PS	HR	SEC	FE	EXT
+0.2	+0.3	-0.3	+0.2	-0.3	-0.3	+0.2	+0.5	0.0	+0.3	+0.6	0.0
WORSENERD	WORSENERD	IMPROVED	WORSENERD	IMPROVED	IMPROVED	WORSENERD	WORSENERD	UNCHANGED	WORSENERD	WORSENERD	UNCHANGED

¹ <http://ffp.statesindex.org/afghanistan>

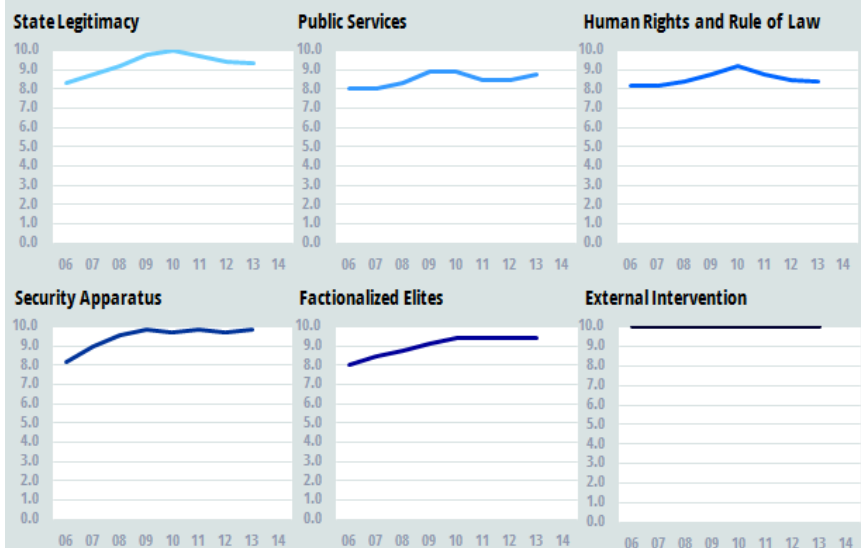
Afghanistan: Overall Trend, 2006-2014



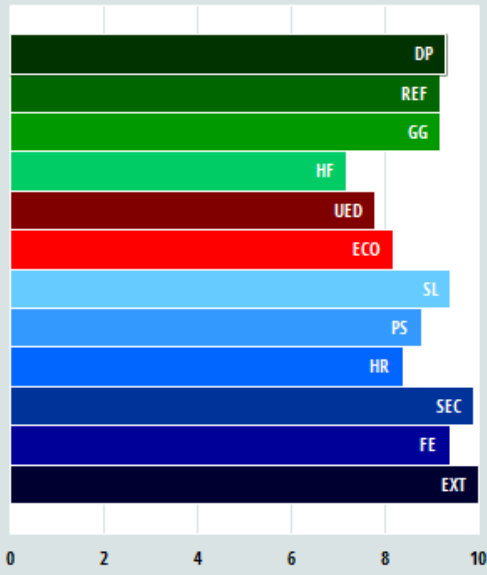
Afghanistan: Social and Economic Indicator Trends 2006-2014



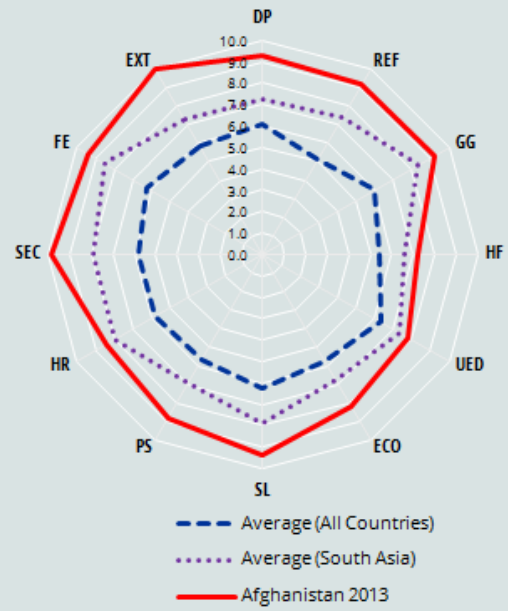
Afghanistan: Political and Military Indicator Trends 2006-2014



Afghanistan: Indicator Comparisons 2014



© 2005-2014 The Fund for Peace



CAPITOLUL 10. CENTRUL DE EXCELENȚĂ NATO ÎN DOMENIUL HUMINT DIN ORADEA – UN MODEL INSTITUȚIONAL DE DEZVOLTARE A UNEI CAPABILITĂȚI DIN SPECTRUL INTELLIGENCE

Centrele de Excelență NATO – generalități

Transformarea în NATO este un subiect de permanentă actualitate, care implică efortul atât a structurii de comandă a Alianței, cât și a factorilor de decizie politici și militari la nivelul națiunilor aliate. Prin multiplele implicații pe care le are în dezvoltarea capacităților militare, determinarea structurilor de forțe, asigurarea tehnico-materială, asigurarea interoperabilității, avansul tehnologiei din domeniul securității, abordarea comprehensivă, comunicarea strategică, relația cu partenerii ș.a.m.d., transformarea se bazează pe inovație și inițiativă, cooperare și coordonare, urmărind asigurarea unor forțe capabile să facă față unui larg spectru de amenințări, specifice mediului de securitate actual.

Procesul de transformare al Alianței Nord-Atlantice reprezintă cadrul conceptual și acțional care a dus la apariția Centrelor de Excelență NATO, inițiativă ce marchează la această dată acreditarea unui număr de 21 astfel de instituții:¹

1. Analysis and Simulation for Air Operations
2. Civil-Military Cooperation
3. Cold Weather Operations
4. Combined Joint Operations from the Sea
5. Command and Control
6. Cooperative Cyber Defence
7. Counter-Improvised Explosive Devices
8. Crisis Management and Disaster Response
9. Defence Against Terrorism
10. Energy Security
11. Explosive Ordnance Disposal
12. Human Intelligence
13. Joint Air Power
14. Joint Chemical, Biological, Radiological and Nuclear Defence
15. Military Engineering
16. Military Medicine
17. Military Police
18. Modelling and Simulation
19. Naval Mine Warfare
20. Operations in Confined and Shallow Waters
21. Strategic Communications

în vreme ce alte trei sunt în diferite faze ale procesului de activare:

22. Counter Intelligence
23. Mountain Warfare
24. Stability Policing

Centrele de Excelență au fost lansate ca o necesitate, urmărindu-se ca acestea să acopere cerințele de sprijin a dezvoltării capacităților NATO în condițiile reorganizării structurii de comandă militară a Alianței și a reorientării funcționale a elementelor acesteia, în urma summitului de la Praga din 2002.

¹ http://www.nato.int/cps/en/natolive/topics_68372.htm

Prin Conceptul privind Centrele de Excelență – MCM 236-03¹ – națiunile sunt încurajate să înființeze, într-un cadru stabilit și în anumite condiții, centre de excelență, instituții definite ca „entități naționale sau multi-naționale capabile să ofere expertiză și experiență recunoscută în sprijinul Alianței, în special în sprijinul transformării”. Centrele de Excelență sunt organizații militare internaționale, în conformitate cu prevederile Protocolului de la Paris, dar fără a fi parte din structura de comandă NATO.

Principiile ce stau la baza înființării și activității acestora sunt legate de utilitatea funcțională și eficiența instituțională, urmărindu-se neduplicarea resurselor și mijloacelor, sau competiția cu capacități existente ale NATO. Centrele de Excelență NATO sunt deschise către participarea tuturor membrilor Alianței și, în anumite condiții, a statelor partenere sau a unor organizații, actul decizional fiind asigurat de un Comitet Director, în baza principiilor consfințite prin Memorandumurile de Înțelegere operaționale și funcționale, sau a Acordurilor Tehnice. Acreditarea² Centrelor de Excelență presupune ca programul de lucru al acestora să fie în concordanță cu solicitările de sprijin ale NATO (sub coordonarea ACT, prin intermediul unei structuri specializate – Transformation Network Branch/TNB), finanțat din resurse proprii și conform cu procedurile, doctrinele, standardele și politicile de securitate ale NATO.

Înființarea rețelei Centrelor de Excelență NATO are multiple semnificații, atât pentru NATO, cât și pentru națiunile participante. Pe de o parte, Centrele gestionează proiecte și programe în sprijinul dezvoltării capacităților existente, în ce privește managementul lecțiilor învățate/ bunelor practici, activitatea de analiză, dezvoltare conceptuală și standardizare, asigurând totodată oportunități deosebite pentru procesul de educare și instruire în NATO; pe de altă parte, participarea națiunilor la Centrele de Excelență, dincolo de contribuția asumată, are rațiuni și interese bine justificate, avantajele imediate incluzând: asigurarea implementării viziunii și reprezentării intereselor naționale în produsele specifice, asigurarea accesului nemijlocit la dezvoltările de ultimă oră în domeniul funcțional și la produsele specifice ale centrului, în condiții preferențiale. În plus, pe lângă vizibilitatea internațională și la nivelul Alianței, relația cu partenerii din cadrul Centrului permite dezvoltarea de proiecte comune, facilitând interacțiunile bilaterale și multilaterale între națiunile participante.

Funcționarea centrelor de excelență acoperă, parțial sau în totalitate, o gamă largă de responsabilități ce se regăsesc în:

- sprijinirea forțelor NATO în vederea îmbunătățirii capacităților de planificare, pregătire și conducere a operațiilor;
- experimentarea, validarea și implementarea unor noi concepte, tehnici, tactici și proceduri, rezultate din procese de cercetare științifică sau ca bune practici/ lecții învățate din operații sau exerciții;
- sprijinirea inovației, a cercetării tehnice și tehnologice în domeniile de responsabilitate;
- furnizarea de produse și servicii specifice procesului de standardizare (doctrine, standarde, proceduri, instrumente de evaluare, etc.), în sprijinind cerințelor de interoperabilitate;
- asigurarea de expertiză pentru structurile NATO și statele partenere;
- conturarea cadrului educațional și de instruire, individuală și colectivă, în ariile funcționale asumate.

¹ Conceptul Comitetului Militar pentru Centrele de Excelență NATO, din 04 decembrie 2003

² Condițiile necesare în acest sens sunt cuprinse în IMSM 0416-04, Criteriile de Acreditare pentru Centrele de Excelență NATO, 11 iunie 2004

Centrul de Excelență NATO în domeniul HUMINT – de la proiect la realitate

Inițiativa înființării unui centru de excelență poate să vină din două direcții: NATO (ca urmare a identificării unor lipsuri în cadrul capacităților de care dispune) sau națiunile aliate (ca urmare a unor inițiative demarate la nivel tactic, operațional, strategic sau chiar politic). În oricare dintre situații, suportul între cele două părți implicate – NATO și națiunea-cadru – trebuie să fie mutual, iar inițiativa trebuie să găsească rezonanță la nivelul a cât mai multe națiuni care să se alăture proiectului.

În ce privește capacitatea HUMINT în NATO, Grupul de Coordonare pentru Intelligence al Autorităților Militare NATO (NATO Military Authorities Intelligence Coordination Group - NMAICG) a identificat deficiențe în funcționalitatea culegerii de informații din surse umane, fapt ce necesita o abordare coerentă și structurată din partea națiunilor aliate.

La acea dată, Armata Română își afirmase deja un corp de cadre experimentat, în condițiile dezvoltării unor capacități de lucru în comun cu structurile militare NATO în diferite teatre de operații (Kosovo, Bosnia, ulterior Irak și Afganistan) și dispunând de serviciile Direcției Generale de Informații a Apărării (DGIA), structură care s-a caracterizat prin viziune și flexibilitate în prefigurarea și construcția unor capacități naționale specifice, manifestând o prezență activă în cadrul grupurilor de coordonare și a demersurilor lucrative în sfera informațiilor militare în NATO¹.

Performanțele obținute, profesionalismul recunoscut, interesul și determinarea manifestate de către DGIA și structurile subordonate în domeniul HUMINT au justificat angajamentul României în a se constitui ca națiune-cadru a unui Centru de Excelență NATO cu obiect de activitate în domeniul informațiilor din surse umane, candidatură acceptată de către NATO. Acestui demers i-a urmat un proces intens de pregătire a fundamentelor legale de înființare a Centrului², precum și negocierea participării la proiect a altor națiuni NATO.

Documentele de bază elaborate în acest sens au fost: *Conceptul Centrului de Excelență*, care detaliază misiunea și sarcinile asumate, precum și viziunea privind dezvoltarea instituției ca pivot al transformării HUMINT în NATO, și *Memorandumurile de Înțelegere Funcțional și Operațional*, care prevăd modalitatea concretă de funcționare a Centrului. Acestea au fost semnate de către ACT, România și primul grup de națiuni participante – Grecia, Slovenia, Turcia și Ungaria, la 16 decembrie 2009, la Norfolk/ SUA. Ulterior, acestora li s-a adăugat Slovacia, Polonia, Cehia și SUA, procesul fiind în continuare deschis altor state membre NATO.

Centrul a fost înființat în Oradea, în cadrul unei vechi cazărmi (foto 10.1) care a beneficiat de renovare completă, facilitățile existente fiind aduse la standardele calitative necesare unei astfel de instituții, prin contribuția exclusivă a României în calitatea sa de națiune gazdă. Pe lângă infrastructura militară la dispoziție, la baza alegerii locației au stat și o serie de caracteristici ale municipiului: un cadru social relativ cosmopolit, permisiv, posibilități de acces facil (locația vestică, infrastructura de transport existentă), condiții de viață la standarde ridicate, posibilități de integrare socio-culturală pentru personalul străin.

¹Detalii privind nivelul de implicare al DGIA în sfera dezvoltării capacităților specifice se regăsesc în ediția aniversară a publicației direcției (Direcția Generală de Informații a Apărării, *Infosfera* (revistă de studii de securitate și informații pentru apărare), Anul I, nr. 3/2009, București)

²Având la bază Decizia nr. 12 din 26 Iunie 2008 a Parlamentului României privind înființarea pe teritoriul României a Centrului de Excelență NATO



Foto 10.1 Centrul de Excelență NATO în domeniul HUMINT din Oradea – intrarea de protocol

Pornindu-se de la o capacitate operațională inițială, au fost puse bazele funcționale și, în baza evaluării comisiei ACT, Centrul a obținut statutul de organizație militară internațională (conform prevederilor Protocolului de la Paris din 1952)¹, afiliată NATO.

Inaugurarea oficială a Centrului a avut loc la data de 16 martie 2010 și a fost onorată de prezența Președintelui României, Traian Băsescu, a ministrului Apărării Naționale, Gabriel Oprea și a Șefului Statului Major General, amiral Gheorghe Marin, iar din partea ACT - locțiitorul comandantului acestui comandament strategic, amiralul Luciano Zappata². (foto 10.2)



Foto 10.2 Inaugurarea Centrului de Excelență NATO în domeniul HUMINT din Oradea (16 martie 2010). Trecerea în revistă a gărzii de onoare de către Președintele României

Prin caracterul lor de noutate, fiecare etapă și fiecare aspect al procesului de înființare a instituției au fost o provocare în sine, indiferent de natura lor – funcțională sau operațională: asigurarea infrastructurii, complianța cu normele de securitate NATO, armonizarea legislativă (național vs. internațional/ NATO), selecția personalului, negocierile cu statele partenere, politica de relații publice și promovare, asigurarea sprijinului logistic necesar, programul investițional și bugetarea, relația cu autoritățile locale, conturarea programului de lucru,

¹***, *Protocol on the Status of International Military Headquarters Set up Pursuant to the North Atlantic Treaty*, Paris, 28 August 1952, în <http://www.nato.int/docu/basicxt/b520828a.htm>

²De asemenea, la eveniment au participat ambasadori și atașați militari acreditați la București, reprezentanți ai națiunilor sponsor, generali și ofițeri din conducerea Ministerului Apărării Naționale, precum și reprezentanți ai conducerii administrației publice județene și locale, marcând importanța evenimentului atât pentru mediul militar, cât și pentru cel civil.

stabilirea relațiilor de lucru cu alte structuri naționale sau internaționale, dezvoltarea comunității de interes în NATO, etc. Prin natura poziției deținute și a gradului de implicare pe care aceasta a presupus-o (și o presupune), corelarea determinărilor funcționale și operaționale cu nevoile de dezvoltare și transformare ale NATO, precum și identificarea comprehensivă a dimensiunilor de impact social, cultural, economic și administrativ pe care înființarea unui astfel de centru o are pe plan local, s-au dezvoltat într-o logică naturală.

Acest fapt a presupus o interacțiune susținută cu factori de răspundere pe plan național (factorii de decizie politici și militari, reprezentanți juridici, eșaloanele militare superioare, elemente de sprijin administrativ-logistic, etc.), responsabilii NATO cu privire la gestionarea rețelei de transformare a Alianței (TNB), precum și cu reprezentanții naționali ai țărilor interesate de participarea la proiectul centrului.

Toate aceste aspecte au depășit cerințele specifice managementului performant, solicitând calități mai degrabă antreprenoriale din partea echipei de proiect – un element de noutate într-un mediu atât de strict normat cum este cel militar. Spiritul antreprenorial presupune, în primul rând, gândire strategică și viziune; acestea s-au manifestat în mod elocvent în faza de dezvoltare a proiectului, pornind de la ideea centrală (conceptul) și contribuind decisiv la transpunerea acesteia în realitate (în virtutea unei proiecții temporale), prin activități ce au presupus – pe lângă cunoașterea domeniului specific de activitate – utilizarea unui vast arsenal de cunoștințe (management, marketing, legislație, servicii de sprijin, etc.).

Centrul de Excelență NATO în domeniul HUMINT – un exemplu de eficiență instituțională

Misiunea Centrului de Excelență NATO în domeniul HUMINT este de a furniza un punct de referință unic în NATO în ce privește activitățile de educare și instruire, dezvoltarea de politici și proceduri standardizate și sprijinirea Alianței în procesul de conturare a evoluției capabilităților sale în domeniul HUMINT.

Transpunerea în realitate a obiectivelor subsumate misiunii se realizează prin produse și serviciile rezultate ca urmare a unui program de lucru întocmit în baza cererilor de sprijin ale NATO și aprobat de către Comitetul Director, urmărind îndeplinirea lor din perspectiva a patru piloni de referință (corespunzând domeniilor acționale ale transformării în NATO):

- analiză și lecții învățate;
- dezvoltare conceptuală și experimentare;
- doctrină și standardizare;
- educație și instruire.

În mod concret, personalul Centrului este implicat în cursuri, exerciții, seminarii, grupuri de lucru, managementul documentelor de standardizare, experimente, activități de analiză, proiecte de cercetare științifică, toate contribuind la conturarea imaginii unei instituții complexe, la nivelul căreia energiile se concentrează în mod sinergic în vederea asigurării unui înalt nivel calitativ al produselor și serviciilor asigurate în cadrul Alianței.

Este de remarcat faptul că, în fiecare dintre domeniile amintite, Centrul se poziționează în postura de lider de opinie și principala sursă de expertiză. În primul rând, directorul Centrului asigură președinția principalelor entități ce guvernează – la nivel de specialiști – dezvoltarea capabilității HUMINT în NATO: Grupul de Lucru NATO pentru HUMINT (NHWG) și Grupul de Lucru NATO pentru Tehnologie HUMINT (NHTWG). În plus, Centrul asigură custodia doctrinei și procedurilor HUMINT în NATO, este un promotor activ al unor noi concepte operaționale, ocupă poziția de șef de departament pentru educație și instruire individuală în domeniul HUMINT în NATO, promovează standardizarea și interoperabilitatea în NATO prin intermediul unor serii de cursuri ce vizează aspecte ale

culegerii de informații din surse umane în teatrele de operații NATO¹, gestionează activitatea Comunității de Interes NATO pentru lecții învățate și bune practici în domeniul HUMINT.

La atingerea unui nivel de excelență în prestația Centrului contribuie în mod decisiv și baza de relaționare largă pe care instituția a construit-o și consolidat-o în timp scurt, printr-o politică pro-activă, prin disponibilitatea de angajament și prioritizarea judicioasă a resurselor, asigurându-și prezența și fiind reprezentat la nivelul principalelor entități decizionale și acționale în domeniul de interes.

Astfel, pe lângă structurile de coordonare din cadrul Comandamentelor Strategice ale Alianței, au fost stabilite relații de lucru în primul rând cu națiunile aliate, cu structuri din cadrul comandamentelor operaționale, cu centre de instruire NATO și cu alte centre de excelență a căror activitate se interconectează la diferite niveluri de interes.

Având în vedere faptul că procesele de reformă și transformare reclamă viziune, performanță și deschidere, trebuie să se țină cont și de necesitatea multiplicării domeniilor de expertiză ale personalului, asigurarea accesului acestora la medii care promovează confruntările de idei, facilitează înțelegerea procesualității fenomenelor și permit aprofundări multidimensionale ale problematicilor de interes. Deschiderea și interrelaționarea cu mediul academic, dezvoltarea de parteneriate cu universități, *think-tankuri*, institute de cercetare, ONGuri, în cadrul unor proiecte specifice, asigură premisele necesare unor astfel de ”achiziții” în materie de cunoaștere și know-how, permițând, totodată, promovarea culturii de securitate NATO (figura 10.4).

Pagina web a instituției (figura 10.3) reprezintă o altă interfață de comunicare prin care Centrul de Excelență se face cunoscut comunității de interes naționale și internaționale, facilitând informarea celor interesați cu privire la evenimente, produse și servicii cuprinse în programul de lucru.

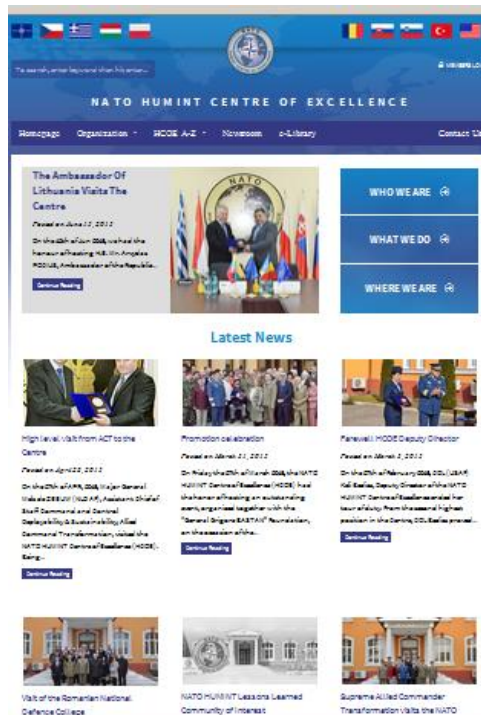


Figura 10.3 Pagina web a Centrului de Excelență NATO în domeniul HUMINT (www.natohcoe.org)

¹ la această data, centrul contabilizează peste 1300 de student care au absolvit cursurile organizate în cadrul instituției, fără a socoti formele de instruire colectivă sprijinite de instituție

NATO HUMINT Centre of Excellence



VISION

The NATO HUMINT Centre of Excellence (HCOE) will consolidate its position as the central point of HUMINT expertise within NATO and the spearhead position of all major HUMINT initiatives within the Alliance.

MISSION

HCOE provides the highest quality services and products in response to the requirements and needs of the NATO Command Structure, NATO Forces Structure, of the NATO Nations and, when feasible, of Partner Nations.

DIRECTOR'S OBJECTIVES

1. HC OE consolidates as the focal point for the HUMINT individual training and education within the Alliance.
2. HC OE takes and retains the leading role for all HUMINT standardization publications in NATO and increases its contribution to other HUMINT-related publications.
3. HC OE brings tangible improvement to the HUMINT capabilities of NATO through Concept Development and Experimentation (CD&E), and enhances its status of active contributor to other connected capabilities.
4. HC OE becomes the repository of NATO HUMINT Lessons Learned/ Best Practice and the principal advisor on HUMINT expertise to NATO.
5. HC OE enhances its external communication and visibility, expands its co-operation with other NATO institutions, increases its presence and relevance in high level committees and groups and retains the chairmanship of NATO HUMINT Working Group and NATO HUMINT Technology Working Group, striving for growing performance of the activity performed within the NATO HUMINT Community of Interest.
6. HC OE pro-actively supports the transformation of NATO HUMINT capability under the aegis of new priorities dictated by the shift from operational involvement to readiness (with direct impact on NATO Response Force – NRF).
7. HC OE matures as an organization and increases its efficiency by:
 - continuing to enhance the expertise and knowledge of its personnel;
 - continuously improving the working conditions (infrastructure, internal processes, strategic focus);
 - implementing a robust Information Knowledge Management (IKM) process.



Section 1 Doctrine and Standards

Is responsible for the management of the NATO HUMINT standardization documents (HC OE is the custodian of NATO HUMINT Doctrine and HUMINT Procedures), contributing to harmonization with other intelligence publications and being committed to overall doctrine development in support of NATO HUMINT standardization and interoperability goals.

Current projects:

- Revision/ development of NATO HUMINT standardization documents;
- Development of the NATO HUMINT Glossary;
- Study on HUMINT support to Air and Maritime Operations;
- NATO Field HUMINT Team Operator Handbook;
- Subject matter expertise to NATO bodies on different projects.

Section 2 Concept Development and Experimentation (CD&E)

Conducts research, initiates proposal for new concepts development (within an integrated approach) and assists with experimentation in order to meet NATO adaptive process of transformation and coordinate activities related to NATO HUMINT CD&E in close support and coordination with all other HC OE Sections.

Current projects:

- Human Aspects of the Operational Environment Project;
- NATO HUMINT Operator Toolset;
- Support the development of the "Countering Hybrid Treats" Capstone concept;
- HUMINT in cyber environment.

Section 3 Education and Training

Department head for HUMINT individual education and training in NATO; Responsible for delivery of individual education and training in HUMINT field according to NATO doctrine and procedures, via resident courses or Mobile Education and Training Teams (METTs); Supports with Subject Matter Experts (SMEs) the collective training in NATO, on the HUMINT side;

Current courses:

- NATO HUMINT Course;
- NATO HUMINT Callators Course;
- NATO HUMINT Contact Handling Course.

Section 4 Lessons Learned and Publications

Actively supports the Lessons Learned (LL) process in conjunction with Joint Analysis Lessons Learned Centre (JALLC);

Maintains a Military HUMINT related Lessons Identified (LI) and LL database; Serves as Subject Matter Expert (SME) to support the gathering and processing of Military HUMINT related LI and LL; Through NATO HUMINT Best Practice (BP) / LL Community of Interest identifies and studies BP and LL from current operations in Theatres of Operations to develop knowledge and to improve future NATO HUMINT operations and activities.

Current involvements:

- leading the NATO HUMINT LL/BP community of Interest;
- analysis of observations and BP collected in NATO theatres of operations and training events.



Hosting nation: Romania
Location: Craiova



Contact information:
Address: 500200, Craiova
NATO HUMINT COE
Armata Română Str. 24/A
Craiova
Code: 410067
Bld. Romaniaia
Phone/Fax: +4 0239434932
E-mail: mg@nato-hcoe.org

www.nato-hcoe.org

Figura 10.4 Poster de prezentare a Centrului de Excelență NATO în domeniul HUMINT, destinat expunerii în cadrul evenimentelor academice

Centrul de Excelență NATO în domeniul HUMINT – perspective de integrare instituțională

Integrarea instituțională reprezintă o adevărată provocare pentru orice organizație nou apărută, în orice mediu de referință. În acest sens, factorii manageriali ai instituției trebuie să gestioneze două direcții funcționale de integrare, una aparținând de structura și relațiile interioare, iar cealaltă ținând de integrarea externă într-un sistem - sau sisteme - funcționale superioare (Simion, 2012).

În ce privește funcționarea internă, principalele referințe rezidă într-o ”construcție” interdependentă de oameni, procese și tehnologii (incluzând procedurile de lucru). Într-o abordare sistemică, intrările și ieșirile (resurse și proceduri vs. produs) este, de asemenea, contabilizată. În final, tipul organizației și scopul acesteia definește și determină modul de abordare a analizei instituționale.

Din punct de vedere funcțional, Centrul de Excelență NATO în domeniul HUMINT realizează un ciclu complet de procese menite să contribuie la activitatea de sprijin a dezvoltării capacității HUMINT: de la culegerea și procesarea de lecții identificate și asimilarea de bune practici, dezvoltarea și experimentarea de noi concepte, transpunerea rezultatelor activității analitice și de cercetare în politici, doctrine, proceduri și, în final, transferul de cunoștințe și dezvoltarea de abilități prin intermediul activității de educare și instruire.

Din punct de vedere al cadrului sistemic, subliniem o primă conexiune a organizației cu entitățile externe. Organizațiile fiind, în general, caracterizate de procese complexe, dinamice, orientate spre obiective, ne putem asuma raportul dintre ”intrări” (sarcinile internalizate și asigurarea resurselor) vs. ”ieșiri” (produsul) ca o importantă caracteristică de integrare instituțională, atât în ce privește indicatorii calitativi, cât și cei cantitativi. Din acest punct de vedere, putem marca un pas decisiv către integrarea instituțională la parametri maximi: în conformitate cu documentele sale constitutive, Centrul de Excelență NATO în domeniul HUMINT și-a constituit propriul program de lucru în baza cererilor de suport ale Alianței, centralizate de către structura directoare a Rețelei de Transformare, fiind totodată deschis cererilor particulare ale națiunilor participante sau ale altor beneficiari din cadrul NATO. În ce privește resursele, toate piesele angrenajului – buget, personal, proceduri, rețele de interconectare, tehnologii, etc. sunt clar specificate în documentele constitutive, precum și în legislația națională (luând în considerare localizarea Centrului) și asigurate astfel încât să contureze premisele necesare și condițiile optime desfășurării activității specifice.

Pe de altă parte, pentru o mai bună înțelegere a adaptării organizației la mediul de acțiune, teoria complexității ne oferă o perspectivă a unei sume de strategii și structuri ce facilitează integrarea ”întregului” (organizația în sine) prin contabilizarea performanțelor conective ale substructurilor componente.

În consecință, pentru o organizație militară, unde independența de acțiune a sub-sistemelor componente este puternic limitată și controlată de către reguli specifice, se impune o strategie adecvată care să potențeze la maxim oportunitățile și inițiativele palierelor subordonate, succesul lor transpunându-se în succesul organizației.

Asumându-ne suficientă flexibilitate la nivelul managementului Centrului de Excelență NATO în domeniul HUMINT și o viziune clară privind rolul și viitorul instituției, putem afirma că sub-structurile acestuia au fost astfel direcționate încât să contribuie, atât individual cât și în cadrul efortului comun, la realizarea racordării cu structurile relevante ale Alianței; schema organizatorică a Centrului (figura 10.5) este ea însăși concepută astfel încât să asigure o conectare specializată, corespondentă pilonilor transformării în NATO, cu branșele responsabile din cadrul comandamentelor strategice și cele operaționale, precum și cu alte structuri aliate angrenate în procesul de dezvoltare a capacităților militare ale Alianței –

Centrul pentru Lupta Întrunită (Stawanger, Norvegia), Centrul de Instruire al Forțelor Întrunite (Bydgoszcz, Polonia), Centrul de Analiză Întrunită și Lecții Învățate (Monsato, Portugalia), etc.

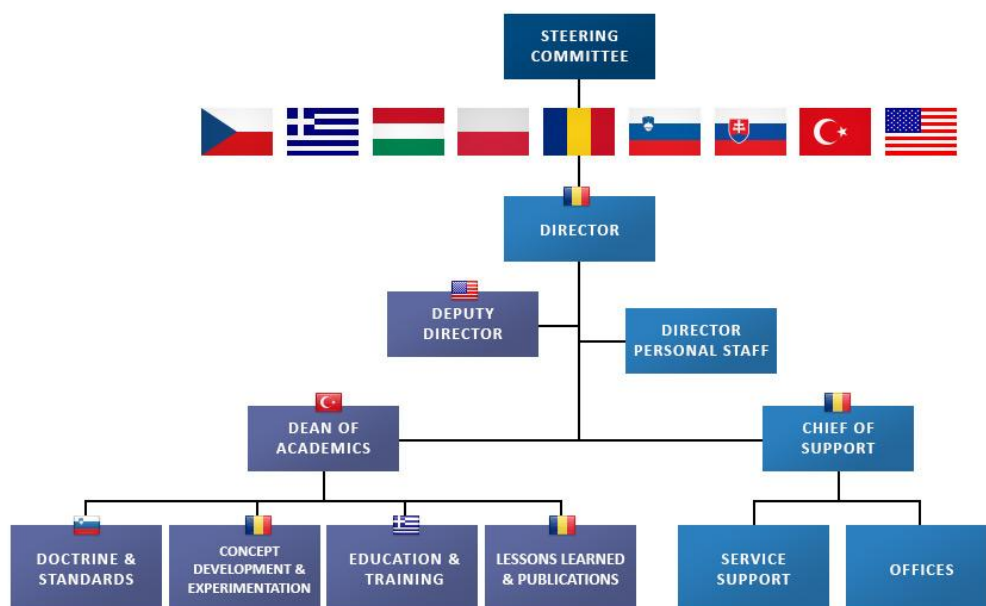


Figura 10.5 Organigrama Centrului de Excelență NATO în domeniul HUMINT
http://www.natohcoe.org/en/organisational_chart/

Din perspectiva dezvoltării obiectului de activitate a Centrului – capacitatea HUMINT în NATO – unul dintre obiectivele prioritare ale instituției este constituirea unei comunități de interes în domeniul HUMINT care să se coaguleze în jurul Centrului de Excelență din Oradea, interesând structuri NATO, națiuni și alte organizații, și având ca scop constituirea unui forum de dezbateri și dezvoltarea de activități menite să asigure informarea reciprocă a participanților în legătură cu acțiuni, evenimente, evoluții semnificative în domeniu (prin acțiuni formale ca: publicarea unui buletin informativ, gestionarea unei pagini web dedicate, organizarea de conferințe și ateliere de lucru, etc.).

Din acest punct de vedere, în timp scurt de la începerea activității, centrul a reușit să atingă o serie de obiective strategice, fundamentale pentru proiecția pe termen lung a sprijinului său pentru transformarea și dezvoltarea capacității HUMINT în NATO:

- **2009:** HCOE devine gazda permanentă a exercițiului NATO pentru HUMINT;
- **2010:** HCOE demarează procesul de instruire de specialitate, derulând până în 2015 peste 40 iterații a 5 cursuri de specialitate distincte;
- **2011:** directorul HCOE preia președinția Grupului de lucru NATO pentru HUMINT (NHWG), ulterior și a Grupului de lucru NATO pentru tehnologie HUMINT (NHTWG);
- **2011:** HCOE preia custodia Doctrinei NATO pentru HUMINT (AJP-2.3) și a publicației NATO pentru procedurile HUMINT (AIntP-5);
- **2013:** în cadrul procesului de reformare a politicilor de educație și instruire în NATO și alinierii la standardele civile (procesul Bologna), instituției noastre îi este conferit *“sigiliul calității”* de către autoritatea responsabilă (Joint Force Trainer) din cadrul Comandamentului Aliat pentru Transformare, ca recunoaștere a calității

infrastructurii, sistemelor, proceselor și procedurilor de lucru, a managementului și standardelor academice aplicate;

- **2013:** constituirea comunității de interes NATO pentru lecții învățate și bune practici în domeniul HUMINT.
- **2015:** HCOE este desemnat de către Comitetul Militar NATO ca *department head* pentru educația și instruirea în domeniul HUMINT în NATO.

Dincolo de aspectele funcționale legate de obiectul de activitate, Centrul de Excelență NATO în domeniul HUMINT s-a făcut remarcat în cadrul Rețelei de Transformare NATO ca o organizație pro-activă, participând la toate evenimentele importante din domeniul HUMINT sau legate de aspecte concrete ale conectării sale la pulsul Alianței, fiind reprezentat în cadrul a diferite proiecte¹, grupuri și ateliere de lucru, foruri de coordonare și standardizare, etc.

Depășind specificitatea câmpului de expertiză și a ariei de interes a Centrului de Excelență din Oradea, dezvoltarea sa ca organizație bazată pe cunoaștere prin integrarea viziunii, politicii și cerințelor NATO în materie de management al cunoașterii informației, adoptate și adaptate ca fundament al propriilor necesități de schimb de informații, reprezintă un element de maximă importanță pentru integrarea instituțională completă.

Centrul de Excelență NATO în domeniul HUMINT – relevanța locală, națională și regională. Considerații privind perspectivele de integrare instituțională multispectrală (socială, economică, culturală)

Din punct de vedere strategic, decizia politico-militară de poziționare a României ca națiune-cadru pentru dezvoltarea Centrului de Excelență NATO în domeniul HUMINT reflectă viziunea unui angajament coerent al țării în angrenajul aranjamentelor de securitate asumate odată cu intrarea în Alianța Nord-Atlantică, eveniment cu profunde semnificații ce exced aspecte pur militare. Având în vedere parteneriatul stabilit cu alte state participante la proiect (inclusiv pornind de la reciprocitatea angajării de resurse în proiecte similare ale partenerilor), se manifestă o consolidare a relațiilor bilaterale în diferite domenii ale câmpului larg al securității și creșterea nivelului de coeziune în asumarea obiectivelor promovate în cadrul NATO sau a unor inițiative regionale.

La nivel național, Centrul de Excelență NATO în domeniul HUMINT reprezintă un adevărat pașaport de calitate al instituției Armatei Române, iar imaginea sa a fost folosită (alături de alte repere relevante²) ca argument al importanței contribuției României la eforturile Alianței în câmpul securității, într-un material video ("*What NATO means for us*" – "*Ce înseamnă NATO pentru noi*") parte a campaniei de diplomatie publică a Alianței³. Acest fapt este doar unul dintre motivele care ne fac să credem că Centrul va constitui un reper permanent pe lista realizărilor cu care Armata Română se mândrește și prin intermediul cărora își asigură o poziție relevantă în peisajul capabilităților NATO.

Dincolo de prestigiul internațional și de relevanța politică pe care existența Centrului de Excelență o are în plan național, la nivel local se înmulțesc în mod semnificativ și se diversifică implicațiile legate de integrarea instituțională.

1 A se vedea, ca exemplu, contribuția adusă în cadrul experimentului legat de dezvoltarea conceptului de Contracarare a Amenințărilor Hibride (Counter Hybrid Threats) – în <https://transnet.act.nato.int/WISE/CHTIPT/Newsletter/AprilNewsI/file/WFS/CHT%20Newsletter%20-%20Edition%20-%20-%20final.pdf>

²Principalele realizări ale Armatei Române în relația cu NATO sunt prezentate sintetic de către ministrul Apărării Naționale, Gabriel Oprea, în articolul "*Armata și interesul național*" din revista Infosfera, Anul II, nr. 2/2010, p. 3-8

³<http://www.mae.ro/en/node/6038>

Încă de la înființarea sa, Centrul de Excelență din Oradea a provocat imaginația populației locale (și nu numai). Descrierea sa ca „*centru de instruire pentru spionii NATO*” a prevalat în mass-media¹ - dar în timp relativ scurt latura spectaculoasă a acestei imagini s-a disipat, iar localnicii au realizat ce reprezintă cu adevărat Centrele de Excelență NATO (și, în mod special, cel găzduit de orașul de pe Crișul Repede).

În continuare, vom contura o serie de abordări pe care aspecte legate de integrarea funcțională a instituției pe plan local le determină.

În primul rând, în zona furnizării de servicii (fără a lua în considerare cheltuielile de mentenanță aferente funcționării cazarmii), străinii care intră în relații de lucru cu Centrul de Excelență (într-un număr considerabil, ca medie lunară) și, totodată, profită de această oportunitate pentru a vizita Oradea (eventual și împrejurimile) sunt excelenți consumatori. Ei folosesc hoteluri de bună calitate, care furnizează servicii complexe, închiriază autoturisme, se bucură de zonele de relaxare (restaurante, pub-uri, stațiunile cu băi termale – Băile Felix și I Mai) și vizitează obiective culturale de interes.

În acest sens, Centrul este în permanență preocupat să contribuie la orientarea corectă a oaspeților săi, care devin și oaspeți ai orașului. În cadrul activităților de lucru, instituția asigură colaboratorilor prezentări generale ale locației, orașului și zonelor înconjurătoare, face recomandări legate de specificul local, furnizează hărți de buzunar, direcționează oaspeții în funcție de intențiile exprimate ale acestora, desfășoară activități de însoțire/ ghidare în cadrul unor scurte tururi turistice la principalele obiective de interes. În acest sens, dispunând de o balanță oarecum disproporționată a timpului liber față de cel dedicat activităților profesionale în favoare acestora din urmă, ne bazăm pe referințe caracterizate de calitate și atractivitate; aceste trăsături vor constitui motive de promovare mai departe, în cercul apropiaților, a unor argumente menite să determine reîntoarcerea lor ca turiști, însoțiți de familie și prieteni.

Este evident faptul că sunt încă multe de făcut în ce privește potențarea și scoaterea în evidență a caracteristicilor culturale ale zonei (managementul și marketingul profesionist al potențialului turistic cu accent pe obiective și evenimente culturale), conectarea acestora la alte evenimente, crearea de parteneriate reciproc avantajoase, a unui pachet de oferte care să asigure tururi de cunoaștere complexe²; ne orientăm, într-o primă fază, asupra disponibilității Muzeului ”Țării Crișurilor”, a Muzeului Militar și a Cetății Oradei (în proces de renovare), urmărindși o valorificare superioară a diferitelor festivaluri, zile comemorative sau sărbători. În acest sens, parteneriatul cu organele administrației publice, factorii de răspundere instituționali, organizații neguvernamentale ar fi mai mult decât util.

O promovare originală a obiceiurilor culinare locale are loc cu ocazia activităților specifice care întrunesc un număr mai mare de persoane, când hrănirea este asigurată în regim de catering, într-o concepție care nu presupune doar simpla asigurare a hranei, ci constituie o excelență oportunitate de a servi feluri de mâncare specifice zonei. Acest fapt este deosebit de apreciat de vizitatori, care ajung chiar să învețe denumirile în limba română a felurilor preferate. În acest sens, parteneriatul Centrului cu furnizorii de servicii în domeniul hrănirii reprezintă o caracteristică integrațională importantă în acest domeniu economic, asigurând predictibilitate, relații de colaborare îmbunătățite și o calitate constantă a prestațiilor, în condiții reciproc avantajoase.

¹<http://www.gandaculdecolorado.com/america/4-america/1218-coala-secret-de-spioni-nato-din-romania>; http://www.adevarul.ro/locale/oradea/oradea-adevarul-de-seara-nato-spioni-eduard-simion-luciano-zapatta-humint_0_226177558.html; <http://www.ziuaveche.ro/top-secret/armata-2/nato-inaugureaza-un-centru-de-spionaj-la-oradea-8759.html>

²În general, Centrele de Excelență NATO nu acordă o atenție deosebită acestui aspect, însă considerăm că o manifestare pro-activă în acest sens reprezintă nu numai o datorie față de comunitate, ci și o oportunitate pentru scoaterea în evidență a ofertei socio-culturale a orașului, fapt de maxima importanță în evaluarea condițiilor generale de trimitere la post a personalului civil.

Pornind de la necesitatea focalizării pe performanță ca trăsătură a excelenței, implicarea Centrului în domeniul cooperării academice se profilează ca o prioritate emergentă. Proiectele de cercetare teoretică în care Centrul se implică solicită o solidă abordare intelectuală, schimburile de experți în câmpuri de interes comun întărind reciproc calitatea și atractivitatea diferitelor evenimente în care instituția este parte.

Un proiect de interes public, gestionat de Centrul de Excelență, este un demers finanțat de către structura NATO focalizată pe provocările emergente în materie de securitate (Emerging Security Challenges Division/ ESCD), intitulat ”*Aspecte umane ale mediului operațional*” (Human Aspects of the Operational Environment - HAOE). Centrul asigură directoratul proiectului și nucleul de lucru de bază, colaborând cu experți politici și militari, consilieri culturali, antropologi, sociologi, istorici, specialiști în comunicare, reprezentanți ai organizațiilor neguvernamentale, etc. din străinătate și din țară¹.

Scopul proiectului este de a asigura suport pentru o mai bună înțelegere a caracteristicilor populației din zonele de conflict și să asigure fundamentul pentru un posibil concept major al NATO în acest domeniu. Studiul se concentrează la nivelul strategic și operațional, fără a exclude însă unele implicații la nivel tactic².

Acesta a reprezentat și o excelentă oportunitate de a implica mediul academic militar prin organizarea unui atelier de lucru pe această temă în cadrul Conferinței Internaționale ”The Knowledge – Based Organization/ KBO 2012”, organizat de Academia Forțelor Terestre ”Nicolae Bălcescu” din Sibiu.

Nevoia de performanță în activitate își găsește rezonanța începând de la nivel individual. Personalul Centrului este activ implicat în dezvoltarea propriei pregătiri academice, urmând programe de masterat și doctorat în diferite domenii (în acest caz, abordările interdisciplinare care antrenează domeniul fundamental al științelor militare și informațiilor, fiind în măsură să asigure spațiul necesar contribuțiilor de valoare exploatabile în activitatea profesională). Totodată, aceștia participă la conferințe, sesiuni de comunicări și ateliere de lucru, proiecte de cercetare, etc., urmărind obiective de dezvoltare personală ce contribuie decisiv la creșterea capacității intelectuale, a volumului de cunoaștere și expertiză și, în cele din urmă, a calității prestației profesionale. Principalele instituții cu care se colaborează în acest sens sunt: Universitatea din Oradea, Academia Forțelor Terestre ”Nicolae Bălcescu” din Sibiu, Colegiul Național de Apărare ”Carol I” București, Universitatea ”Lucian Blaga” din Sibiu, Universitatea Națională pentru Intelligence (SUA).³

¹În perioada 6-8 Septembrie 2011 a avut loc primul atelier de lucru, în Oradea, la care au participat 20 de experți în domeniile de interes identificate reprezentând instituții și organizații de renume din diferite țări NATO și non-NATO: ACT Human Factors Branch; Acta Non-Verbal (România); Allied Rapid Reaction Corps (Marea Britanie); Behavioural Dynamics Institute/ Royal Institute of Great Britain; Centre for Policy and Quality Standards (Afganistan), Centre for Strategic and International Studies, SUA; Centrul de Excelență pentru Apărare împotriva Terorismului (Turcia), Graduate Institute of Development Studies, Geneva; Information Options Ltd. (Marea Britanie); International Security and Assistance Forces (ISAF), ISAF Joint Command; Irregular Warfare Program, SUA; King’s College London, Marea Britanie; Michigan State University, SUA; Neurolinguistic Programming /NLP 101 Life, Marea Britanie; comandamentul ONU; University of Cambridge, Marea Britanie; University of Duisburg – Essen, Germania; University of Leiden, Olanda; University of Oxford, Marea Britanie; Western Illinois University, SUA.

²În acest sens, următoarele direcții de analiză au fost considerate ca necesare: principalii factori motivatori ai acțiunilor umane; determinarea profilului comunității; comunicarea interculturală; dinamica situației locale; percepția și acceptarea operațiilor/misiunilor NATO; indicatori măsurabili ai atitudinii populației privind operațiile NATO; Aspectele Umane în Planificarea Operațională.

³Toate Centrele de Excelență NATO abordează cu deosebită seriozitate relația cu mediul academic, datorită naturii activității lor predilect intelectuale, cu concretizare în sfera educării și instruirii, dezvoltării conceptuale și cercetării.

Există o serie întreagă de alte aspecte care pot fi abordate din perspectiva unei mai bune integrări în plan local, atât la nivel instituțional, cât și la nivel social – având în vedere nevoile specifice ale personalului internațional al Centrului. Pornind de la multiculturalismul zonei – un cadru excelent pentru adaptarea personalului străin și a familiilor acestora cu un mediu social tolerant, pot fi lansate întrebări legate de capacitatea sistemului de învățământ (și reprezentarea sa la nivel local) de a asigura o ofertă cu adevărat utilă din punct de vedere al cerințelor pieței educaționale.

Dacă învățământul în limbile maghiară și germană este bine reprezentat, ar trebui ca factorii de răspundere din domeniul educației să realizeze și nevoia de asigurare a acestor servicii în limba engleză, făcând facilitatea de educație accesibilă unei plaje mult mai largi de clienți (familiile investitorilor străini pe plan local, ale personalului străin aflat la post – cum e cazul Centrului de Excelență, dar și elevilor și studenților orădeni care urmăresc să își dezvolte competențe care să le asigure succesul dezvoltării profesionale viitoare într-o lume caracterizată de uniformizarea generată de presiunile integraționiste ale globalizării).

Concluzionăm că, pentru Oradea, înființarea Centrului de Excelență reprezintă o oportunitate unică pentru promovarea sa în exterior, în spațiul de interes NATO.

Municipiul capătă notorietate prin relațiile de lucru pe care Centrul le derulează cu o multitudine de structuri NATO sau organizații naționale și internaționale active în câmpul securității și în mediul academic. Oradea (și județul Bihor) sunt promovate cu ocazia tuturor evenimentelor găzduite de către Centru, dar și de către delegații Centrului participanți la diferite activități în afară. Mai mult, toate referirile la Centrul de Excelență NATO în domeniul HUMINT care se fac în comunitatea Alianței Nord-Atlantice se leagă de orașul gazdă - Oradea, detalii despre acesta fiind făcute cunoscute prin prezentări postate pe websiteul NATO și pe pagina web a Centrului, toate cu scopul de a contribui la cunoașterea sa pe plan internațional.

Condiționările de securitatea activităților specifice se transpun și în planul relațional al Centrului de Excelență NATO din Oradea, limitând interacțiunea în domeniul specific de expertiză la nivelul comunității de interes HUMINT din cadrul Alianței. Cu toate acestea, instituția nu este izolată de mediul civil, dezvoltând și participând în mod activ la proiecte deschise publicului larg, promovând cultura de securitate a Alianței Nord-Atlantice și urmărind dezvoltarea prezenței sale în comunitatea academică prin punerea în valoare a potențialului uman de care dispune.

Concluzii

O abordare cuantificabilă a determinării în materie de securitate demonstrează că Alianța Nord-Atlantică este una dintre organizațiile cu cea mai mare deschidere în ce privește asumarea de responsabilități în câmpul de referință conceptual al securității. Nevoia de transformare¹ a NATO este generată atât de modificările geostrategice de securitate generate de trecerea de la sistemul unipolar la cel multipolar (sau poate la cel poliarhic- Brown, 2007) și, subsecvent, de căutarea rolului Alianței în acest context, cât și de noile provocări în materie de securitate.

¹Transformarea, după cum o vede John J. Garstk, înseamnă o schimbare susținută, coerentă, care urmărește realizarea obiectivului strategic de a crea sau menține un avantaj în cadrul competiției sau de a anihila avantajul unui adversar nou sau deja existent. Conceptul este relevant pentru organizațiile confruntate cu provocări și oportunități care nu pot fi abordate în mod real prin metodologiile consacrate, pentru a putea aduce îmbunătățiri incrementale organizațiilor, proceselor, tehnologiilor, managementului resurselor umane și modelelor de afaceri existente. (Garstk, 2005)

La nivelul Alianței, transformarea constă, în fapt, într-o sumă de inițiative lansate progresiv și care se dezvoltă complementar (Bell, 2005), în corelație și influențându-se reciproc cu procesul de reformare a altor organizații relevante în câmpul securității. Transformarea în NATO a fost pozitiv influențată de dezvoltarea Politicii Europene de Securitate și Apărare; în același timp, forma și eficacitatea viitoare a Organizației Națiunilor Unite sunt importante pentru NATO, deoarece mandatul ONU reprezintă, de multe ori, o precondiție pentru ca mulți dintre aliații europeni să ia în considerare folosirea forței (Riecke, 2005).

În cadrul organizației militare, transformarea implică schimbări la nivelul doctrinelor, organizării și structurii forțelor, a activității de informații, instruirii, educației și achizițiilor, managementului personalului și programării bugetare; acestea devin domenii principale de aplicare a transformării în domeniul militar, care se reflectă, ca efort și resurse, la nivelul tuturor națiunilor aliate.

Este important de subliniat rolul pe care Conceptul Strategic adoptat la Summitul de la Lisabona, dar și recente decizii determinate de provocările din flancul estic al Alianței îl joacă în procesul decizional al NATO, ca referință privind finalitatea efortului depus în slujba securității, promovând consensul transatlantic și imaginea unei organizații transparente și coerente. Direcțiile trasate prin Conceptul Strategic constituie un adevărat vector al orientării sarcinilor de transformare a structurilor și capabilităților de apărare a statelor NATO. În tot acest angrenaj, rolul major în procesul de transformare, la nivel militar, îl va juca în continuare Comandamentul Aliat pentru Transformare - ACT.

Cum capabilitățile Alianței pentru implementarea acestor cerințe sunt relativ limitate, în special în ce le privește pe cele legate de educație și instruire, este de așteptat ca rolul Centrelor de Excelență NATO să crească exponențial, acestea având atât capacitatea, cât și cadrul legal flexibil pentru a răspunde cererilor de sprijin adresate de comandamentele NATO în cadrul procesului de transformare.

Prin activitatea lor, Centrele de Excelență NATO caută să devină principalii agenți ai transformării în ariile de expertiză care le corespund prin dezvoltarea, promovarea și implementarea de politici, concepte și noi strategii în scopul creșterii calitative a capabilităților operaționale și atingerii obiectivelor de interoperabilitate propuse.

Produsele Centrelor de Excelență sunt compliantă cu scopul final al procesului de transformare în NATO: capabilități îmbunătățite, interoperabilitate crescută și întărirea valorilor comun împărtășite, totul aliniat viziunii strategice și politicilor de dezvoltare ale Alianței, contribuind în mod plener la programul "Smart Defence".

Este important să observăm că domeniile transformării în NATO vor purta, astfel, amprenta predilectă a națiunilor înregimentate în cadrul centrelor. În această logică, o largă participare și reprezentare în clubul centrelor de excelență va asigura o acceptabilitate și legitimitate sporită a produselor acestora, constituindu-se, în egală măsură, într-o oportunitate care să permită manifestarea valorilor, experienței acumulate, bunelor practici și lecțiilor învățate ale națiunilor.

Pe lângă faptul că se constituie în adevărați ambasadori ai mesajului NATO în cadrul propriilor comunități de interes, sprijinind o mai bună aprofundare a viziunii și rolului asumat de către Alianță în plan internațional, participarea națiunilor la centrele de excelență este o șansă de manifestare a propriilor puncte forte și de promovare a imaginii naționale.

România beneficiază din plin de aceste oportunități, în calitate de națiune cadru și gazdă a Centrului de Excelență NATO în domeniul HUMINT. Prin calitatea produselor sale, centrul este un excepțional promotor al imaginii țării și instituției militare naționale în primul rând în cadrul NATO, dar și în plan internațional largit. Mai mult, prezența centrului de excelență are semnificații deosebite și pe plan local, poziționarea sa în ansamblul instituțiilor

publice și integrarea într-un cadru social specific generând o serie de abordări de real interes pentru o multitudine de actori.

Centrul de Excelență NATO HUMINT din Oradea reprezintă deja un model și exemplu de urmat pentru inițiative similare, naționale sau aparținând unor structuri instituționale ale altor state. Abordarea structurată pe care o urmărește tema propusă poate deschide astfel de orizonturi și pentru alte entități interesate, atât în ce privește gestionarea unei astfel de instituții, cât și stabilirea de relații în arii funcționale de interes comun cu Centrele de Excelență NATO.

Bibliografie

1. ***, *Protocol on the Status of International Military Headquarters Set up Pursuant to the North Atlantic Treaty*, Paris, 28 August 1952, în <http://www.nato.int/docu/basicxt/b520828a.htm>
2. BELL, Robert, (2005) *Fișa transformării NATO*, în <http://www.nato.int/docu/review/2005/issue1/romanian/summaries.html>
3. Conceptul Comitetului Militar pentru Centrele de Excelență NATO, din 04 decembrie 2003
4. Decizia nr. 12 din 26 Iunie 2008 a Parlamentului României privind înființarea pe teritoriul României a Centrului de Excelență NATO
5. Direcția Generală de Informații a Apărării, *Infosfera* (revistă de studii de securitate și informații pentru apărare), Anul I, nr. 3/2009 și Anul II, nr. 2/2010, București
6. GARSTK, John, (2005) *Provocarea transformării*, în <http://www.nato.int/docu/review/2005/issue1/romanian/special.html>
7. IMSM 0416-04, Criteriile de Acreditare pentru Centrele de Excelență NATO, 11 iunie 2004
8. RIECKE, Henning, (2005) *Nevoia de schimbare*, în <http://www.nato.int/docu/review/2005/issue1/romanian/summaries.html>
9. SIMION, Eduard, (2012) *A view on the integration of NATO HUMINT Centre of Excellence from Oradea in the local institutional landscape*, în *Revista Română de Geografie Politică/ Romanian Review on Political Geography*, Year XIV, no. 1/ May
10. http://www.adevarul.ro/locale/oradea/oradea-adevarul_de_seara-nato-spioni-eduard_simion-luciano_zapatta-humint_0_226177558.html
11. <http://www.mae.ro/en/node/6038>
12. http://www.nato.int/cps/en/natolive/topics_68372.htm
13. https://transnet.act.nato.int/WISE/CHTIPT/Newsletter/AprilNews1/file/_WFS/CHT%20Newsletter%20-%20Edition%20%20-%20final.pdf
14. www.natohcoe.org

CAPITOLUL 11. INTELLIGENCE ȘI AMENINȚĂRILE DIN MEDIUL CIBERNETIC

Securitatea cibernetică – domeniu de referință pentru Intelligence în domeniul cibernetic

Tehnologiile digitale, sistemele informatice, bazele de date, conexiunile în rețele, Internetul, toate au devenit esențiale vieții moderne, devenind o extensie virtuală a acesteia, un spațiu de manifestare a tuturor aspectelor funcționale ale proceselor, evenimentelor, relațiilor din toate domeniile.

Strategia de securitate cibernetică a României definește spațiul cibernetic ca *mediu virtual, generat de infrastructurile ciberneticе, incluzând conținutul informațional procesat, stocat sau transmis, precum și acțiunile derulate de utilizatori în acesta*; spațiul cibernetic se caracterizează prin lipsa frontierelor, dinamism și anonim, generând deopotrivă oportunități de dezvoltare a societății informaționale bazate pe cunoaștere, dar și riscuri la adresa funcționării acesteia (la nivel individual, statal și chiar cu manifestare transfrontalieră) (*Strategia de securitate cibernetică a României, 2013*).

Odată cu dezvoltarea spectrului cibernetic, vulnerabilitățile specifice (probleme tehnice, imperfecțiuni de software, sisteme de protecție neactualizate), incidentele (erori umane sau hazarde naturale) sau riscurile complexe generate de atacuri generează un tablou complet al riscurilor de securitate la care acestea sunt supuse. Este o realitate ușor de cuantificat faptul că atacurile ciberneticе au devenit tot mai frecvente și mai organizate, nivelul pagubelor în ce privește activitatea administrației de stat, afacerile, domeniul economic, transporturile și rețelele de aprovizionare sau amenințările asupra infrastructurii critice atingând cote înalte, în măsură să amenințe prosperitatea, securitatea și stabilitatea.

Amenințările în spectrul cibernetic sunt generate de actorii statali (ca parte a arsenalului ofensiv al acestora, în mod direct sau prin intermediari, sau în cadrul operațiilor de spionaj cibernetic) și de actori nonstatali, activi în ceea ce privește:

- infracțiunile ciberneticе (ce urmăresc câștiguri financiare),
- extremismul cibernetic (în baza motivațiilor ideologice) și
- terorismul cibernetic (susținerea activităților teroriste prin servicii în mediul cibernetic) (Cosmoiu, 2013).

Acestora din urmă li se adaugă: actorii implicați în spionajul comercial, activiștii, persoane din interior, oportuniști, etc. (FS-ISAC, 2013).

În acest context, *securitatea cibernetică* reprezintă starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive¹ prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic, a resurselor și serviciilor publice sau private, din spațiul cibernetic (*Strategia de securitate cibernetică a României, 2013*).

NATO și securitatea în domeniul cibernetic

Apărarea în domeniul cibernetic este un subiect de actualitate în NATO, în confruntarea cu o vastă paletă de atacuri asupra rețelelor informatice și de comandă, control și comunicații ale Alianței sau în dezvoltarea capacităților de răspuns la agresiunile ciberneticе exercitate asupra statelor membre.

¹ Acestea includ, între altele: politici, concepte, standarde și ghiduri de securitate, managementul riscului, activități de instruire și conștientizare, implementarea de soluții tehnice de protecție a infrastructurilor ciberneticе, managementul identității, managementul consecințelor

Încă din anul 2000, Alianța a recunoscut importanța protecției infrastructurilor informatice critice împotriva atacurilor cibernetice, această problemă apărând pentru prima dată pe agenda summitului de la Praga din 2002 și fiind reconfirmată în reuniunea de la Riga, în 2006.

Atacurile cibernetice asupra Estoniei, în aprilie și mai 2007, au dus la executarea de evaluări privind locul și rolul Alianței în apărarea împotriva unor astfel de agresiuni. O primă politică comună privind apărarea în domeniul cibernetic a fost aprobată în aprilie 2008, la summitul de la București.

Conceptul Strategic NATO din 2010¹ a luat în considerare necesitatea ca Alianța să-și accelereze eforturile de prevenire, detectare și apărare în domeniul cibernetic, precum și sprijinirea refacerii rapide a țărilor membre după astfel de atacuri. Aplicarea metodologiei procesului de planificare NATO în acest domeniu ar fi de natură să asigure coordonarea capacităților naționale de securitate cibernetică, asigurând un nivel superior de informare, avertizare și răspuns în cadrul protecției cibernetice centralizate.

La 8 iunie 2011, NATO a aprobat o Politică revizuită privind Apărarea în Domeniul Cibernetic și un Plan de Acțiune pentru implementarea acesteia, urmate de:²

- stabilirea elementelor critice ale capacității operaționale depline a sistemului NATO de răspuns la incidente în rețelele informatice (NATO Computer Incident Response Capability – NCIRC)³, din februarie 2012;
- integrarea apărării cibernetice în Procesul de Planificare a Apărării în NATO, începută în aprilie 2012;
- reafirmarea hotărârii șefilor de state și guverne, la summitul de la Chicago din mai 2012⁴, de a îmbunătăți nivelul de apărare cibernetică în cadrul Alianței prin punerea în comun a rețelelor NATO sub protecție centralizată⁵ (responsabilitate preluată de către Agenția NATO pentru Comunicații și Informații - NCI, din iulie 2012) și îmbunătățirea parametrilor NCIRC;
- instalarea în aprilie 2013 a infrastructurii de bază pentru gestionarea apărării rețelelor și a capacității analitice la Centrul Tehnic al NCIRC în Mons, Belgia;
- în cadrul primei întâlniri a miniștrilor apărării din NATO dedicată exclusiv apărării cibernetice (la 4 iunie 2013) a fost stabilită crearea Echipelor de Reacție Rapidă pentru protejarea sistemelor NATO în cadrul NCIRC, precum și dezvoltarea procedurilor de sprijin și asistență din partea NATO pentru națiunile aliate ce solicită asistență în caz de atac cibernetic⁶.
- mai mult, Declarația adoptată la Summitul NATO din Țara Galilor extinde garanțiile colective din Tratat la spațiul cibernetic - ca urmare, un atac împotriva unei rețele informatice a unui stat membru va fi considerat un atac împotriva tuturor⁷; teoretic, în condițiile unui atac cibernetic cu consecințe devastatoare, acest act poate duce la expunerea agresorului la represalii din partea NATO, inclusiv prin mijloace militare convenționale.

¹NATO, *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*, adopted by Heads of State and Government at the NATO Summit in Lisbon, 19-20 November 2010, http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf

²http://www.nato.int/cps/en/natolive/topics_78170.htm

³Centrul de coordonare a NCIRC se află la comandamentul NATO din Bruxelles

⁴http://www.nato.int/cps/en/natolive/events_84074.htm

⁵Infrastructura critică națională rămâne o responsabilitate a națiunii respective, care trebuie să își dezvolte propriile capacități de protecție

⁶Sprijinul acordat se concretizează în schimbul de informații și bune practici, executarea de exerciții practice, asigurarea de expertiză, etc.

⁷http://www.nato.int/cps/en/natohq/official_texts_112964.htm

Eforturile NATO în domeniul apărării cibernetice sunt sprijinite în mod consistent de Centrul de Excelență NATO în domeniul Apărării Cibernetice prin Cooperare (Cooperative Cyber Defence Centre of Excellence - CCDCOE) din Estonia¹, în special în domeniul cercetării și instruirii (figura 11.1).



Figura 11.1 Pagina web a Centrului de Excelență NATO în domeniul Apărării Cibernetice prin Cooperare (www.ccdcoe.org)

A. Klimburg desemnează în Manualul cadru pentru Securitatea Cibernetică Națională (elaborat sub auspiciile CCDCOE) aspectele de interes pentru NATO în domeniul cibernetic: activitățile militare, combaterea criminalității în rețelele informatice, intelligence și CI, protecția infrastructurii critice și managementul crizelor, diplomație și guvernarea internetului (Klimburg, 2012).

Principalele activități privind apărarea cibernetică în NATO se referă la: asistarea națiunilor aliate, integrarea apărării cibernetice în Procesul de Planificare a Apărării în NATO, dezvoltarea apărării cibernetice ca inițiativă ”smart defence”, cercetare și instruire (sprijinită consistent de CCDCOE), cooperarea cu națiunile partenere, organizațiile internaționale, mediul academic și industria de securitate², coordonarea și ghidarea cu privire la măsurile practice de apărare cibernetică³.

¹<http://www.ccdcoe.org/>

²În prezent, NIAG (NATO International Armaments Group) derulează un studiu privind acțiunile de colaborare ale NATO cu industria pentru facilitarea apărării cibernetice pe timpul situațiilor de criză

³Responsabilități în acest sens regăsindu-se la nivelul ESCD – Emerging Security Challenges Division, a conducerii NC3 - NATO Consultation, Control and Command, a NMA - NATO Military Authorities și NCI - NATO Communications and Information Agency

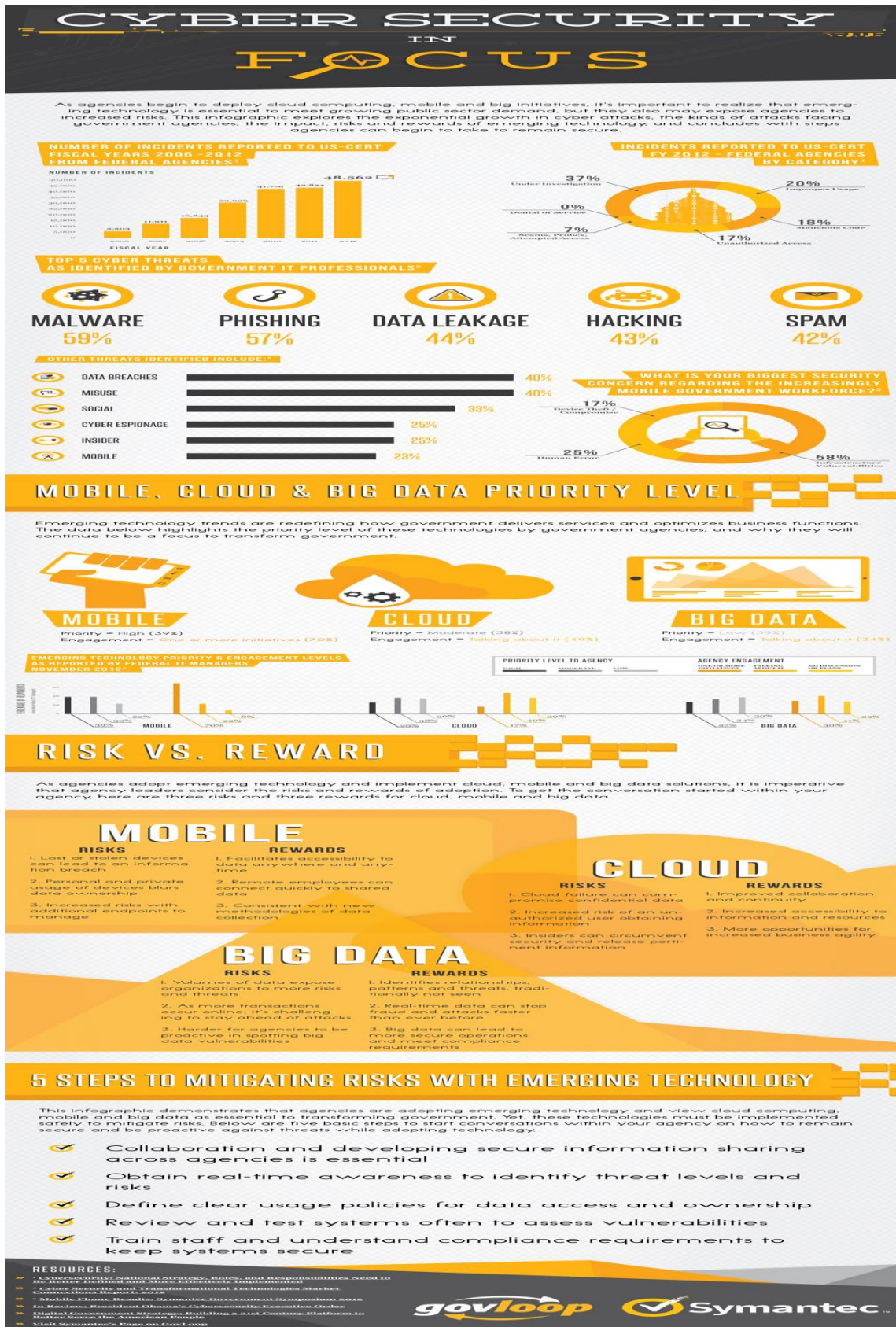


Figura 11.2 Infografie NATO privind domeniul securității cibernetice¹

¹<http://www.nato.int/docu/review/2013/Cyber/Cyber-Security-in-Focus/EN/index.htm>

Abordarea apărării cibernetice în NATO se bazează și pe o strânsă cooperare cu țările partenere, după caz, precum și cu organizațiile internaționale - printre care UE, Consiliul Europei, ONU și OSCE, cu sectorul privat și mediul academic.

Pentru publicul larg, websiteul NATO facilitează accesul la informații, expuneri și dezbateri de idei în domeniul apărării cibernetice în secțiunea dedicată acestui subiect¹, fiind o resursă utilă pentru cei doritori să își dezvolte perspectiva în acest domeniu – a se vedea ca exemplu infografia din figura 2.

În 2011, România și NATO au semnat un Memorandum de înțelegere pentru cooperare în domeniul securității cibernetice², care asigură cadrul pentru schimbul de informații, cooperare și sprijin între autoritatea națională în domeniu (SRI) și structurile responsabile ale Alianței Nord-Atlantice.

Mai mult, România este parte³ și la inițiativa *smart defence* concretizată în proiectul ”The Multinational Cyber Defence Capability Development” (MN CD2)⁴, proiect gestionat de către Agenția NATO pentru Comunicații și Informatică în vederea dezvoltării și dobândirii în condiții de eficiență, prin cooperare, a capacităților naționale de apărare cibernetică.

Securitatea în domeniul cibernetic în Uniunea Europeană și România

Agenda Uniunii Europene în materie de securitate cibernetică cuprinde:

- stabilirea Computer Emergency Response Team (CERT) naționale și la nivelul UE⁵,
- organizarea de simulări pentru incidente de securitate în mediul cibernetic și
- asigurarea sprijinului pentru pregătirea împotriva atacurilor cibernetice în cadrul Uniunii, cu precădere în ceea ce privește protecția infrastructurii critice⁶.

Fundamentarea măsurilor de securitate cibernetică la nivelul UE este realizată de Strategia de Securitate Cibernetică a Uniunii⁷ și de Directiva privind Securitatea Rețelelor și a Informației în UE, propusă de Comisia Europeană în februarie 2013 și votată în Parlamentul European la 13 martie 2014⁸.

¹<http://www.nato.int/docu/review/2013/Cyber/EN/index.htm>

²<http://www.infolegal.ro/memorandum-nato-romania-in-domeniul-securitatii-cibernetice/2011/10/18/>

³<http://militar.infomondo.ro/actualitate/sri-mapn-si-proiectul-multinational-cyber-defence-capability-development.html#more-15606>

⁴<http://mncd2.ncia.nato.int/Pages/default.aspx>

⁵http://cert.europa.eu/cert/plainedition/en/cert_about.html

⁶<http://ec.europa.eu/digital-agenda/en/cybersecurity>

⁷<http://ec.europa.eu/digital-agenda/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace>

Strategia oferă priorități clare pentru politica internațională a UE în materie de spațiu virtual

(http://eeas.europa.eu/policies/eu-cyber-security/index_ro.htm):

- Libertate și deschidere: strategia va prezenta viziunea și principiile privind aplicarea valorilor și drepturilor fundamentale ale UE în spațiul virtual.
- Legile, normele și valorile fundamentale ale UE se aplică în spațiul cibernetic și în lumea materială: responsabilitatea pentru un spațiu cibernetic mai securizat le revine tuturor participanților la societatea informațională globală, de la cetățeni la administrații naționale.
- Dezvoltarea consolidării capacităților în materie de securitate cibernetică: UE va colabora cu parteneri și organizații internaționale, precum și cu reprezentanți ai sectorului privat și ai societății civile pentru a sprijini consolidarea capacităților globale în țările terțe. Aceasta va include îmbunătățirea accesului la informații și la un internet deschis, precum și prevenirea amenințărilor cibernetice.
- Încurajarea cooperării internaționale în materie de spațiu cibernetic: păstrarea unui spațiu cibernetic deschis, liber și securizat reprezintă o provocare la nivel mondial, pe care UE ar trebui să o abordeze împreună cu partenerii și organizațiile internaționale relevante, sectorul privat și societatea civilă.

⁸http://europa.eu/rapid/press-release_STATEMENT-14-68_en.htm

Pe lângă CERT-EU, activitățile privind securitatea cibernetică în UE sunt în responsabilitatea Agenției Europene pentru Securitatea Rețelelor și a Informației (European Network and Information Security Agency/ ENISA)¹.

În România, sistemul național de securitate cibernetică (SNSC) reprezintă cadrul general de cooperare care reunește autorități și instituții publice, cu responsabilități și capacități în domeniu, sub coordonarea Consiliului operativ de securitate cibernetică (COSC)², în vederea coordonării acțiunilor la nivel național pentru asigurarea securității spațiului cibernetic, inclusiv prin cooperarea cu mediul academic și cel de afaceri, asociațiile profesionale și organizațiile neguvernamentale. (*Strategia de securitate cibernetică a României, 2013*)

În cadrul SRI – în calitate de autoritate națională pentru cyberintelligence – funcționează Centrul Național CyberINT³, cu misiunea de a asigura colectarea, analiza, reacția, managementul consecințelor și diseminarea informațiilor privind amenințările și atacurile cibernetică. În acest sens, responsabilitățile Centrului includ:

- identificarea amenințărilor cibernetică generate prin intermediul rețelelor naționale sau internaționale de date;
- punerea la dispoziția beneficiarilor legali a unor informații și analize utile pentru prevenirea și gestionarea situațiilor de criză;
- contribuția la securizarea infrastructurilor de comunicații și procesare a datelor;
- asigurarea suportului tehnic pentru realizarea unor operațiuni de contracarare a atacurilor cibernetică la adresa infrastructurilor IT&C naționale.⁴

Dezvoltarea infrastructurii de tehnologia informației și comunicațiilor a antrenat și apariția unui larg spectru de amenințări la adresa utilizatorilor acestora, fapt ce a reclamat nevoia de protecție sau reacție la astfel de evenimente. Această necesitate la nivel public, totodată o nișă de piață pentru companiile private, a dus la consolidarea și evoluția permanentă a metodelor și mijloacelor de asigurare a securității în domeniul cibernetic.

Atât în cadrul organizațiilor și instituțiilor publice, cât și la nivelul companiilor private, pe lângă mijloacele de protecție pasivă existente, se impune necesitatea unor structuri specializate care să monitorizeze și să răspundă unui număr de amenințări tot mai complexe, care – odată cu evoluția tehnologiei – ies din tiparele clasice de agresiune (și apărare) cibernetică.

Echipele specializate în acest sens sunt cunoscute ca echipe CERT sau CSIRT (Computer Security Incident Response Team/ Echipa de Răspuns la Incidente de Securitate Cibernetică), fiind formate din specialiști în securitate cibernetică și având atât rolul de a interveni urgent în situații complexe, cât și prevenirea apariției unor incidente similare pe viitor.

¹<http://www.enisa.europa.eu/>

²Din COSC fac parte, în calitate de membri permanenți, reprezentanți ai Ministerului Apărării Naționale, Ministerului Afacerilor Interne, Ministerului Afacerilor Externe, Ministerului pentru Societatea Informațională, Serviciului Român de Informații, Serviciului de Telecomunicații Speciale, Serviciului de Informații Externe, Serviciului de Protecție și Pază, Oficiului Registrului Național pentru Informații Secrete de Stat, precum și secretarul Consiliului Suprem de Apărare a Țării. Conducerea COSC este asigurată de un președinte (consilierul prezidențial pe probleme de securitate națională) și un vicepreședinte (consilierul prim-ministrului pe probleme de securitate națională). Coordonatorul tehnic al COSC este Serviciul Român de Informații, în condițiile legii. (*Strategia de securitate cibernetică a României, 2013*)

³înființarea unității cu atribuții în securitatea cibernetică fiind aprobată în ședința Consiliului Suprem de Apărare a Țării din 22 iulie 2013 (<http://gov.ro/ro/guvernul/procesul-legislativ/note-de-fundamentare/nota-de-fundamentare-hg-nr-241-02-04-2014&page=2>)

⁴Documentul sinteză al SRI privind prioritățile strategice pe termen mediu ale ordonatorilor principali de credite pentru anul 2013 și perspectiva 2014-2016, http://discutii.mfinante.ro/static/10/Mfp/proiect_buget2013/SRI.pdf

În România, principalul obiectiv al CERT-RO¹ (structură guvernamentală independentă pentru cercetare, dezvoltare și expertiză în domeniul securității cibernetice²) stabilit prin lege este ”înființarea sistemului național de alertă timpurie și informare în timp real privind incidentele cibernetice în scopul avertizării și emiterii de rapoarte cu privire la distribuția și natura incidentelor, precum și colaborarea cu autoritățile naționale responsabile în asigurarea securității cibernetice în vederea prevenirii și înlăturării efectelor incidentelor”³.

Pentru asigurarea eficienței la nivel național și a relevanței în plan instituțional internațional, toate instituțiile publice (utilizatori, sisteme și rețele din spațiul cibernetic românesc) sunt obligate să se înroleze în acest sistem; totodată, CERT-RO este membră a comunității TF-CSIRT⁴, comunicând și cooperând cu alte CSIRT (figura 11.3).



Figura 11.3 Locații CERT în Europa (<http://www.enisa.europa.eu/activities/cert/background/inv>)

Comitetul de coordonare al CERT-RO este format din reprezentanți ai:⁵

- a) Ministerului Comunicațiilor și Societății Informaționale;
- b) Ministerului Apărării Naționale;
- c) Ministerului Administrației și Internelor;
- d) Serviciului Român de Informații;
- e) Serviciului de Informații Externe;
- f) Serviciului de Telecomunicații Speciale;
- g) Serviciului de Protecție și Pază;
- h) Oficiului Registrului Național al Informațiilor Secrete de Stat;

¹înființarea CERT-RO are la bază H.G. 494 / 11 May 2011

²RFC 2350 description for CERT-RO (Romanian National Computer Emergency Response Team) (2012), în <http://www.cert-ro.eu/files/doc/RFC2350.pdf>

³http://adevarul.ro/news/eveniment/aurelian-Tolescu-sri-saptamanal-colectam-12-milioane-evenimente-securitate-cibernetica-1_50aee3e67c42d5a663a17dce/index.html

⁴<http://www.enisa.europa.eu/activities/cert/background/coop/status-quo/evaluation/tf-csirt>

⁵<http://www.cert-ro.eu/files/doc/RFC2350-CERT-RO.pdf>

i) Autorității Naționale pentru Administrare și Reglementare în Comunicații.
În vederea îndeplinirii atribuțiilor ce revin CERT-RO, directorul general al acesteia emite decizii și instrucțiuni.

Echipele CERT oferă o serie de servicii clasificate ca:

a. reactive:

- alerte și avertizări, concretizate în notificări imediate care fac referire la incidente de securitate aflate în desfășurare, precum noi viruși sau viermi care afectează un număr din ce în ce mai mare de calculatoare, atacuri informatice complexe de natură recentă care afectează un anumit tip de organizații, precum bănci, companii energetice, agenții guvernamentale, ori noi acțiuni ingenioase de inginerie socială menite să obțină date privind cărțile de credit sau date cu caracter personal;
- tratarea incidentelor de securitate (prin intervenție la locul incidentului sau acordarea de suport la distanță);
- managementul vulnerabilităților (atât hardware, cât și software);
- culegerea probelor (identificarea fișierelor de pe un calculator atacat, care au fost instalate de un criminal cibernetic în mod direct sau prin intermediul unui cod malițios precum troieni, viruși sau viermi informatici, sau chiar descoperirea unor probe digitale pe calculatorul de pe care a fost lansat atacul, care atestă faptul că acesta a stat la originea acțiunii criminale);

b. proactive:

- anunțurile;
- urmărirea evoluției tehnologice;
- evaluările de securitate;
- configurarea și menținerea soluțiilor de securitate;
- dezvoltarea uneltelor de securitate;
- servicii de detectare a intruziunilor;
- diseminarea informațiilor din domeniul securității. (Provision IT Group, 2013)

Metodologia de lucru a CERT face apel și la utilitatea folosirii de echipe CERT private, care să completeze resursele publice și să deservească consumatori de mare calibru în domeniul IT&C și sectoare vizate în mod agresiv de incidente de securitate cibernetică, precum cel al telecomunicațiilor sau din mediul bancar.

Pentru a acoperi cererea existentă, furnizorii privați de servicii de securitate informatică își ajustează oferta proprie în servicii reactive și/sau proactive de tip CERT, în condiții de confidențialitate, pe care le oferă contra cost (prin abonament sau servicii punctuale).

Websiteul CERT-RO, pe lângă ghiduri de protecție, listează și o serie de link-uri către websiteuri ce furnizează programe și aplicații protecție în mediul cibernetic:¹

- aplicații pentru devirusare troian FLAME/GAUSS:
[Bitdefender Gauss Removal Tool](#)
[Bitdefender Flame Removal Tool](#)
[Kaspersky Virus Removal Tool 2011 SITU Edition](#)
- aplicații gratuite împotriva software rău intenționat (AntiMalware):
[Avast Free Antivirus](#)
[AVG Free Antivirus](#)
[Bitdefender Free Edition](#)
[Microsoft Security Essentials](#)

¹<http://www.cert-ro.eu/programe.php>

- [Microsoft Malicious Software Removal Tool](#)
- [Kaspersky Free Virus Scan](#)
- program testare web-server:
 - [Apache Benchmark](#)
- instrumente de identificare în baza urmelor lăsate (Forensic Tools):
 - [Mandiant Red Curtain](#)
 - [Mandiant Red Line](#)
- accesare de la distanță:
 - [PuTTY](#)
- aplicații de criptare:
 - [Pretty Good Privacy - GnuPG](#)
 - [TrueCrypt](#)
- aplicații de tip Firewall:
 - [COMODO Free Firewall](#)
 - [ZoneAlarm Free Firewall](#)
- aplicații de detectare a intruziunilor:
 - [OSSIM](#)
 - [OSSEC](#)
 - [SNORT](#)
- scanner de porturi:
 - [Angry Ip Scanner](#)
 - [Net Scan](#)
 - [NMAP](#)
- server proxy:
 - [Paros Proxy](#)

Intelligence în domeniul cibernetic. De la Cyber Threat Intelligence (CTI) la CYBERINT

Sistemele informatice și de comunicații ale unui stat, precum și datele gestionate de acestea, sunt tot mai dependente de spațiul cibernetic. Totodată, mediul cibernetic găzduiește elementele de manifestare ale lumii reale, începând cu multiple comunități de interes și rețele umane ce se manifestă în mediul virtual. Dincolo de beneficiile evidente pe care acest mediu le are în facilitarea tuturor aspectelor existenței umane – de la cele economice, financiare, sociale, culturale și până la cele politice și militare – acesta facilitează și o serie de riscuri specifice, în special în absența unor măsuri de securitate adecvate.

Atât entitățile statale, cât și cele non-statale (la o scară care le pune aproape pe picior de egalitate cu agențiile guvernamentale în acest cadru), în baza propriilor interese, pot recurge la agresiuni cibernetic împotriva competitorilor sau opozanților.

După cum o relevă SRI, astfel de atacuri cibernetic pot fi îndreptate împotriva sistemelor de tehnologia informației și de comunicații, care fie reprezintă infrastructuri critice în sine (de exemplu telecomunicațiile și rețeaua Internet), fie sunt esențiale pentru buna funcționare a celorlalte infrastructuri critice ale statului (de exemplu infrastructura de transport aerian, feroviar și rutier, sistemele de aprovizionare cu energie, gaze, petrol și apă, serviciile medicale, sistemul financiar-bancar etc.)¹.

Prevenirea, apărarea și limitarea efectelor unor astfel de atacuri implică eforturi multidisciplinare, acțiuni complexe și procese decizionale ce necesită o informare corectă, completă și oportună cu privire la caracteristicile atacului cibernetic, vectorii purtători ai

¹<http://www.sri.ro/Cyberintelligence.html>

amenințării și actorii agresori. Ca în orice alt tip de proces decizional, recurgerea la produsele de Intelligence – cu diferite grade de complexitate – este o opțiune firească, indiferent dacă facem trimitere la entități publice sau private.

Rolul Intelligence – raportat la orice sistem de referință – este cel de a colecta, analiza și produce informații menite să furnizeze evaluări complete, exacte, oportune și relevante cu privire la amenințări, în vederea fundamentării deciziilor factorilor de răspundere.

După cum am arătat într-o temă anterioară, definirea conceptului ”Intelligence” se leagă de parametrii acestuia în calitate de produs, proces sau organizație. Din această perspectivă, și abordarea problematicii Intelligence în domeniul cibernetic comportă o serie de nuanțe, în funcție de sistemul de referință. La rândul ei, fiecare disciplină de culegere a informațiilor din spectrul Intelligence se raportează la aspecte specifice în ce privește obiectivele operaționale și modalitatea de manifestare în fiecare dintre etapele ciclului Intelligence – planificare și direcționare, colectare, procesare și producție, diseminare – raportate la definirea cerințelor de informații, tipul de date colectate, metodologia de colectare, resursele implicate/ senzorii utilizați, modul de procesare a datelor și informațiilor primare, diseminarea produselor de intelligence, caracterul acestora și asigurarea conexiunii inverse (feed-back).

Cartea albă a Alianței pentru Intelligence și Securitate Națională (The Intelligence and National Security Alliance/INSA)¹ din SUA, un parteneriat public-privat în domeniu, evaluează necesitatea depășirii planului tactic (”sistemul” sau ”rețeaua”) în acest domeniu și orientarea către cerințele de informații necesare la nivel strategic, într-un efort conjugat care face referire la:

- definirea sistematică și stabilirea unor proceduri clare în materie de Cyber Intelligence, profesionalizarea abordării și stabilirea unui set de abilități, educație și instruire și tehnologii necesare;
- facilitarea elaborării de politici și proceduri de abordare în domeniul Cyber Intelligence, la nivel de entități guvernamentale, industriale, academice și al organizațiilor non-profit, implicate în conștientizarea situațională, furnizarea de date de avertizare, analize și rapoarte;
- stabilirea de parteneriate în regim public-privat pentru abordarea problemelor de securitate cibernetică;
- construirea unui parteneriat virtual între toate entitățile relevante pentru schimbul de informații, analiza și măsurile de răspuns privind amenințările în domeniul cibernetic.

Însă, înainte de toate, se impune diferențierea abordărilor privind analiza modului de manifestare a disciplinelor de colectare a datelor, comun acceptate, ale spectrului Intelligence față de îmbogățirea acestui spectru prin definirea unei activități de culegere a informațiilor de sine stătătoare, raportată la acest mediu – Intelligence cibernetic (Cyber Intelligence/ CYBERINT).

Ciclul Intelligence în domeniul cibernetic

Procesualitatea consacrată a ciclului Intelligence se raportează la o serie de activități complexe – planificarea și direcționarea, colectarea, procesarea, producția și diseminarea, completate de conexiunea inversă (feedback) (figura 11.4) – care se regăsesc, în diferite forme de interpretare (ciclu sau proces), în cadrul fiecăreia dintre disciplinele de colectare a informațiilor (particularizate prin relația dintre domeniu/mediu, senzor și surse).

¹Intelligence and National Security Alliance/ INSA (2011) *Cyber intelligence: Setting the landscape for an emerging discipline*, http://www.insonline.org/i/d/a/Resources/Cyber_Intelligence.aspx



Figura 11.4 Ciclul Intelligence

În domeniul cibernetic, **planificarea și direcționarea** – ca etapă definită de exprimarea scopului/ intențiilor – poate urmări descoperirea serverelor de comandă și control a unui software rău intenționat (malware) în vederea blocării acestuia; **colectarea datelor** în mediul cibernetic se desfășoară în zone ca: puncte de atracție (honeypots), datele de acces ale programelor filtru (Firewall) sau ale sistemelor de detectare a accesărilor neautorizate (Intrusion Detection System), scanări ale Internetului, etc.; **procesarea** constă în conversia informațiilor colectate în formate adaptate utilizării acestora; **producția** asigură transformarea datelor într-un produs de tip ”intelligence” care să răspundă nevoilor de informații; **diseminarea** asigură transferul de intelligence către beneficiar, în timp ce **conexiunea inversă** confirmă sau infirmă acuratețea produsului de intelligence raportat la planificare și direcționare (Lee, 2014a).

Cyber Threat Intelligence (CTI)

Beaupré și Hellberg descriu conceptul de Cyber Threat Intelligence (CTI) ca abilitate de a colecta, împărtși și analiza date în vederea elaborării răspunsului la o amenințare în domeniul cibernetic, solicitând o serie de caracteristici și principii specifice disciplinei Intelligence – oportunitatea, acuratețea (surse de încredere, date validate), relevanța, corelarea datelor provenite de la mai multe surse, analiza, formularea de recomandări, determinarea trendului în materie, raportarea la un sistem de ierarhizare a severității amenințărilor, caracterul interactiv (cooperare și consultare) (Beaupré și Hellberg, 2012) - care să facă produsul finit al CTI util în prevederea, prevenirea, combaterea și limitarea efectelor amenințărilor cibernetic.

Centrul pentru Schimbul de Informații și Analiză/ SUA (Information Sharing and Analysis Center/ ISAC) folosește conceptul de **Intelligence pentru amenințările cibernetic** (Cyber Threat Intelligence/ CTI) pentru a determina cadrul de direcționare, culegere, procesare și diseminare a datelor și informațiilor în sprijinul procesului decizional în ce privește amenințările în mediul cibernetic, listând o serie de definiții conturate în cadrul diferitor comunități de interes din domeniu:

- ”disciplină emergentă în domeniul securității informației ce are ca scop recunoașterea și înțelegerea unor adversari ciberneticici complecși și, în mod special, determinarea motivațiilor și modalităților prin care aceștia amenință date, rețele și afaceri” (Cyber Squared, 2011);

- ”informație în posesia unui element al comunității de Intelligence, cu referire directă la o vulnerabilitate sau amenințare la adresa unui sistem sau rețele guvernamentale sau private, incluzând informația referitoare la protecția unui sistem sau rețele față de eforturile de degradare, întrerupere sau distrugere a acestuia, prevenirea furtului sau însușirii frauduloase a informațiilor private sau guvernamentale, a proprietății intelectuale sau a datelor personale” (Cyber Intelligence Sharing and Protection Act / CISPA).

Dacă o capabilitate CTI este, în general, realizabilă – la diferite niveluri de complexitate – în cadrul organizațiilor, în baza culegerii de date din surse interne și externe, publice și private, prelucrate de analiști de trend, cu sprijinul unor tehnologii specifice (Beaupré și Hellberg, 2012), CYBERINT – ca disciplină de culegere a datelor în cadrul ciclului Intelligence -solicită o metodologie și proceduri standard mult mai complexe.

CYBERINT

Compania “Deloitte”, specializată în consultanță în afaceri (incluzând servicii de securitate cibernetică), descrie **Cyber Intelligence** ca set complex de tactici și instrumente de avertizare și management a amenințărilor în domeniul cibernetic, capabilitate ce se manifestă la nivel de:

- analiză - *Cyber analysis* - (pentru detectarea căilor de acțiune în sisteme și rețele, analiza jurnalelor de securitate fizică și analiza de intelligence a amenințărilor în spectrul cibernetic pentru prezicerea atacurilor viitoare),
- abordare științifică a urmelor - *Cyber forensics* - (dedicată analizei cauzelor atacurilor cibernetică și urmării căilor de atac de la sursă și pe parcursul infiltrării în sistemele și rețelele proprii),
- logistica în domeniul cibernetic - *Cyber logistics* - (resursele și mijloacele de asigurare a securității, incluzând răspunsul în caz de incident cibernetic),

toate sub umbrela cerințelor de securitate cibernetică, ce creează cadrul de identitate, acces și control pentru protejarea mijloacelor în conformitate cu politicile și procedurile implementate la nivelul organizațiilor.¹

Dupa CyberInt Group, companie specializata in securitatea informatiei si razboi cibernetic, **Cyber Intelligence**, ca activitate desfășurată în mediul privat în vederea asigurării securității informației și a rețelelor, se bazează pe: investigații în domeniul digital (investigația fiind o metodă de lucru a contrainformațiilor – în acest caz având ca obiectiv depistarea fraudelor bazate pe folosirea computerelor, detectarea spionajului industrial, încălcarea dreptului de proprietate intelectuală, etc.); depistarea prezenței intrușilor și analiza de expunere a clienților, în vederea prevenirii scurgerilor de informații și atenuării vulnerabilităților; folosirea de tehnici și metodologii OSINT pentru crearea de rapoarte de intelligence în sprijinul proceselor decizionale².

The Software Engineering Institute Innovation Center al Carnegie Mellon University definește **Cyber Intelligence** ca reprezentând ”*colectarea și analiza informațiilor pentru identificarea, urmărirea și prezicerea de capabilități, intenții și activități în domeniul cibernetic ce conturează cursuri de acțiune menite să îmbunătățească procesul decizional*”³ și dezvoltă un proiect multidisciplinar (ce implică domeniul guvernamental, industria și academia) pentru determinarea parametrilor conceptuali ai Cyber Intelligence - Cyber Intelligence Tradecraft Project (CITP)⁴.

¹http://www.deloitte.com/assets/Dcom-SouthAfrica/Local%20Assets/Documents/Cyber_Intelligence.pdf

²<http://www.cyberint.com/>

³<https://www.webcaster4.com/Webcast/Page/139/2631>

⁴<http://www.sei.cmu.edu/about/organization/etc/citp.cfm>

În cadrul CITP, securitatea cibernetică este văzută ca fiind direct conectată la ciclul Cyber Intelligence, constând în cinci funcțiuni: mediul, colectarea de date, analiza funcțională, analiza strategică, raportarea și conexiunea inversă (feedback) (figura 11.5) corespunzătoare ciclului Intelligence.



Figura 11.5 Securitatea cibernetică și ciclul CYBERINT¹

Una dintre principalele provocări în definirea unei discipline CYBERINT este adaptarea metodologiilor specifice Intelligence mediului cibernetic. O primă diferență notabilă față de ciclul clasic al Intelligence o reprezintă chiar interpretarea etapelor acestuia din perspectiva facilităților, dar și a limitărilor, specifice mediului cibernetic.

Astfel, în viziunea CITP, **mediul** ("environment") este cel care stabilește scopul CYBERINT, **culegerea de date** se realizează prin mijloace automate, **analiza funcțională** se concentrează asupra aspectelor de analiză tehnică în sprijinul misiunii de securitate cibernetică (răspunde întrebărilor "ce?" și "cum?" legat de amenințările de natură cibernetică), **analiza strategică** interpretează datele funcționale din perspectivă strategică (răspunde întrebărilor "cine?" și "de ce?") și raportează produsul de Intelligence factorilor de decizie; în baza informațiilor disponibile, aceștia influențează dinamica mediului cibernetic. Un aspect notabil este și asigurarea de către utilizatorul final de CYBERINT a conexiunii inverse (feedback), în măsură să determine aspectele calitative ale produselor furnizate (oportunitatea, utilitatea și caracterul acționabil al acestora), precum și gradul de încredere al surselor.

Caracteristic procesului de analiză funcțională în CYBERINT este nevoia de adaptare permanentă a metodologiei și instrumentelor de lucru la evoluția spectrului și a gradului de complexitate a amenințărilor și a nivelului de rafinament al adversarului. Cunoașterea capacităților acestuia și a trendurilor de dezvoltare, precum și accesul la serviciile de avertizare situațională sunt de natură să îmbunătățească în mod radical performanțele CYBERINT.

¹<http://www.sei.cmu.edu/about/organization/etc/citp-summary.cfm>

Pe de altă parte, cerințele specifice pentru performanța analistului în CYBERINT pornesc de la stăpânirea cunoștințelor specifice (infrastructură, proceduri, protocoale, securitate) și a limbajului tehnic necesar. Mixul de experți tehnici și analiști de intelligence trebuie să asigure o abordare unitară a datelor și informațiilor privind amenințările din mediul cibernetic, fiind necesare, în acest sens, sensibilizarea, conștientizarea, educarea și instruirea corespunzătoare (transdisciplinaritate), dar și un limbaj comun.

Lipsa unei abordări unitare din punct de vedere conceptual privează CYBERINT de o utilitate la parametri universali. Cu toate că un lexicon specific la nivel tehnic este, în mare parte, consacrat la nivelul specialiștilor în domeniul IT, nivelul strategic de adresare (relevanța domeniului cibernetic dincolo de spațiul tehnic) nu asigură un reper terminologic unitar necesar analizei strategice și acțiunii conjugate la acest nivel, ținând cont de multitudinea domeniilor de manifestare a amenințărilor ciberneticе: guvernamental, industrial, mediul academic, etc. Aceeași problemă se manifestă și în ce privește metodologia de lucru (ciclul sau procesul CYBERINT), care cunoaște interpretări diferite raportat la mediul funcțional și expertiza acestuia în materie de Intelligence.

La capitolul diseminare/ raportare, bunele practici în materie de proceduri ale Intelligence cer ca produsul final să marcheze încă din titlu un sumar relevant al conținutului, cuprinsul acestuia oferind detalii esențiale cu privire la informația evaluată, precum și opiniile analistului – judecăți de valoare bazate pe istoricul subiectului, informațiile conexe și gândirea critică a acestuia, cu valențe anticipative relativ la evoluția viitoare a amenințării (Lee, 2014b).

INSA consideră că CYBERINT nu este o disciplină de culegere a informațiilor în sine ci, în mod similar cu MEDINT, este o disciplină analitică ce se bazează pe informații colectate din surse consacrate ale spectrului Intelligence, în vederea elaborării de produse informative în sprijinul procesului decizional în domeniul de expertiză (cibernetic), la toate nivelurile (strategic, operativ, tactic).¹

În baza cererilor de informații, CYBERINT la **nivel strategic** furnizează evaluări de risc menite să orienteze factorii de decizie în ce privește planificarea și investițiile în securitatea cibernetică. Informațiile relevante care sunt analizate la acest nivel privesc atât date de rețea, activități ciberneticе în derulare, cât și evenimente geopolitice cu potențial de influență asupra securității ciberneticе.

La **nivel operațional**, amenințările în domeniul cibernetic reflectă interesele de nivel strategic din spatele vectorilor de atac și urmăresc blocarea capacităților de comandă și control asupra elementelor tactice, cu efecte în lumea reală. Totodată, amenințările ciberneticе la acest nivel pot fi coordonate cu acțiuni în lumea reală care, conjugate, să sprijine producerea unor efecte dorite.

CYBERINT la nivel operațional se poate concentra asupra:²

- analizelor de trend, menite să indice direcțiile de evoluție ale adversarului din punct de vedere tehnic;
- identificării de indicatori cu privire la modalitatea selectată de adversar pentru atacarea entității proprii;
- identificării de indicatori cu privire la construirea de către adversar a unor capacități în vederea exploatării unor căi de atac;
- descoperirii tehnicilor, tacticilor și procedurilor adversarilor;
- înțelegerii ciclurilor/ proceselor operaționale ale adversarului;
- identificării vulnerabilităților adversarului (tehnice, sociale, financiare, etc.);

¹http://www.insaonline.org/i/d/a/b/CyberIntel_embed.aspx

²http://www.insaonline.org/i/d/a/b/CyberIntel_embed.aspx

- informațiilor menite să influențeze acțiunile adversarului odată declanșat atacul cibernetic.

Nivelul tactic al domeniului cibernetic este reprezentat de cadrul concret al acțiunilor în rețea, cuprinzând atacurile ciberneticе și măsurile de protecție, apărare și contracarare a acestora. Identificarea atacurilor se bazează pe alertele sistemelor de securitate, detectarea de "semnături" specifice ale acestora, analiza acțiunilor unor actori cunoscuți sau a urmelor comportamentului în rețea. La acest nivel, în anumite contexte geopolitice, CYBERINT poate viza actori statali care acționează direct sau prin intermediari, determinând identitatea lor, probabilitatea unor atacuri și orizontul de timp al producerii acestora.

Concluzii

Mediul cibernetic constituie un domeniu acțional în culegerea de date și informații pentru mai multe discipline de colectare din spectrul Intelligence (OSINT, MASINT, SIGINT) sau un facilitator/ interfață prin oportunitățile de comunicare și relaționare pe care le asigură (HUMINT). În acest sens, orice demers specific ciclului Intelligence în ce privește amenințările din mediul cibernetic pot fi subsumate clasei de produse intitulate Cyber Threat Intelligence.

Dincolo de această abordare, putem sesiza în cadrul comunităților de interes guvernamentale și private un nivel ridicat de interes în ce privește definirea unei discipline specializate de colectare a informațiilor în mediul cibernetic - CYBERINT.

Scopul CYBERINT este de a furniza produse informative menite să faciliteze avertizări strategice predictive privind amenințările în domeniul cibernetic, diminuarea riscurilor asociate cu aceste amenințări, îmbunătățirea abilităților de evaluare a efectelor atacurilor ciberneticе și asigurarea securității ciberneticе în condiții de eficiență financiară, în baza unor decizii fundamentate în mod adecvat.

În limitele stricte impuse de mediul de operare, chiar dacă CYBERINT nu este o disciplină a cărei parametri conceptuali sunt clar definiți și acceptați, folosirea produselor de Intelligence în mediul cibernetic, la toate nivelurile de decizie și acțiune, este o necesitate evidentă. Legat de aceasta, reținem că domeniul cibernetic adresează nevoia unor cunoștințe tehnice avansate, în special la nivelul analiștilor în domeniu, incluzând înțelegerea proceselor și protocoalelor informatice, limitele și oportunitățile oferite de rețele, folosirea terminologiei specifice, etc., dar fără a face rabat de la cunoașterea aprofundată a adversarului (state, competitori în afaceri, organizații criminale), mediile operaționale ale acestuia și a fundamentului uman al acțiunilor malițioase în mediul cibernetic (intenția, motivația, planificarea, rețelele de coordonare, modalitățile de execuție, etc.).

După cum am arătat și în cadrul lucrării, capabilitățile de protecție împotriva amenințărilor în domeniul cibernetic sunt variate, pornind de la un banal program antivirus și până la sisteme complexe, care implică capacități analitice care să coreleze informații provenite de la multiple surse.

La nivel individual, o minimă educație pentru persoanele ce beneficiază de servicii Internet este, de asemenea, necesară. În acest sens, considerăm foarte utile indicațiile pe care websiteul SRI le pune la dispoziția publicului în vederea educării pentru asigurarea propriei protecții în mediul online, dar și ca facilitator pentru depistarea atacurilor ciberneticе sau a altor riscuri la adresa securității, cu privire la: protecția informațiilor clasificate, navigarea sigură pe Internet, depistarea și semnalarea riscurilor teroriste, protejarea de acțiunea serviciilor secrete străine.¹ Acestea constituie doar un prim pas în asigurarea unui nivel minim

¹<http://www.sri.ro/ce-poi-face-tu/ce-poti-face-tu.html>

de avertizare și capacitate de reacție, pornind de la nivel individual și avansând către sisteme publice naționale și chiar internaționale.

Bibliografie

1. COSMOIU, Florin (2013) *Cyber threats - a Romanian perspective*, 3rd Information Security and Cyber Defence Conference, http://www.nbf.hu/anyagok/prezentaciok/Florin%20Cosmoiu_SRI%20Romania.pdf
2. de BEAUPRÉ, Adrien, HELLBERG, Natasha (2012) *Developing Cyber Threat Intelligence...or not failing in battle*, Intru-Shun.ca Inc., AtlSecCon
3. Documentul sinteză al SRI privind prioritățile strategice pe termen mediu ale ordonatorilor principali de credite pentru anul 2013 și perspectiva 2014-2016, http://discutii.mfinante.ro/static/10/Mfp/proiect_buget2013/SRI.pdf
4. Financial Services - Information Sharing and Analysis Center/ FS-ISAC (2013) *Evolution and Revolution of Cyber Threat Intelligence*, <http://www.nymissa.org/wp-content/uploads/2013/02/FSISAC-EVOLUTION-CYBER-THREAT-INTEL-201303020-final-santized.pdf>
5. Guvernul României, *Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică*, publicat în Monitorul Oficial, Partea I nr. 296 din 23.05.2013
6. H.G. 494 / 11 Mai 2011
7. Intelligence and National Security Alliance (2014) *Strategic Cyber Intelligence is Essential to Business Security*, http://www.insaonline.org/i/f/pr/2014/03.27.14_StrategicCyber.aspx
8. Intelligence and National Security Alliance/ INSA (2011) *Cyber intelligence: Setting the landscape for an emerging discipline*, http://www.insaonline.org/i/d/a/Resources/Cyber_Intelligence.aspx
9. Klimburg, Alexander (Ed.) (2012) *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn
10. LEE, Robert M. (2014a) *An introduction to Cyber Intelligence*, în <http://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber-intelligence/>
11. LEE, Robert M. (2014b) *Developing Your Cyber Intelligence Analyst Skills*, în <http://www.tripwire.com/state-of-security/security-data-protection/developing-cyber-intelligence-analyst-skills/>
12. NATO, *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*, adopted by Heads of State and Government at the NATO Summit in Lisbon, 19-20 November 2010, http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf
13. Provision IT Group, ISEC Associates (2013) *Ghid referitor la rolul structurilor de tip CERT și utilitatea CERT-urilor private*, document realizat în cadrul campaniei de conștientizare a riscurilor de securitate cibernetică derulată în România sub egida ECSM de către CERT-RO, <http://www.cert-ro.eu/rapoarte.php>
14. RFC 2350 description for CERT-RO (Romanian National Computer Emergency Response Team) (2012), în <http://www.cert-ro.eu/files/doc/RFC2350.pdf>
15. http://adevarul.ro/news/eveniment/aurelian-Tolescu-sri-saptamanal-colectam-12-milioane-evenimente-securitate-cibernetica-1_50aee3e67c42d5a663a17dce/index.html
16. http://cert.europa.eu/cert/plainedition/en/cert_about.html
17. <http://ec.europa.eu/digital-agenda/en/cybersecurity>
18. <http://ec.europa.eu/digital-agenda/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace>;
19. http://eeas.europa.eu/policies/eu-cyber-security/index_ro.htm
20. http://europa.eu/rapid/press-release_STATEMENT-14-68_en.htm
21. <http://gov.ro/ro/guvernul/procesul-legislativ/note-de-fundamentare/nota-de-fundamentare-hg-nr-241-02-04-2014&page=2>
22. <http://militar.infomondo.ro/actualitate/sri-mapn-si-proiectul-multinational-cyber-defence-capability-development.html#more-15606>
23. <http://mncd2.ncia.nato.int/Pages/default.aspx>
24. <http://www.ccdcoe.org/>
25. <http://www.cert-ro.eu/files/doc/RFC2350-CERT-RO.pdf>
26. <http://www.cert-ro.eu/programe.php>
27. <http://www.cyberint.com/>
28. http://www.deloitte.com/assets/Dcom-SouthAfrica/Local%20Assets/Documents/Cyber_Intelligence.pdf

29. <http://www.enisa.europa.eu/>
30. <http://www.enisa.europa.eu/activities/cert/background/coop/status-quo/evaluation/tf-csirt>
31. <http://www.infolegal.ro/memorandum-nato-romania-in-domeniul-securitatii-cibernetice/2011/10/18/>
32. http://www.insaonline.org/i/d/a/b/CyberIntel_embed.aspx
33. http://www.nato.int/cps/en/natohq/official_texts_112964.htm
34. http://www.nato.int/cps/en/natolive/events_84074.htm
35. http://www.nato.int/cps/en/natolive/topics_78170.htm
36. <http://www.nato.int/docu/review/2013/Cyber/Cyber-Security-in-Focus/EN/index.htm>
37. <http://www.nato.int/docu/review/2013/Cyber/EN/index.htm>
38. <http://www.sei.cmu.edu/about/organization/etc/citp.cfm>
39. <http://www.sei.cmu.edu/about/organization/etc/citp-summary.cfm>
40. <http://www.sri.ro/ce-poi-face-tu/ce-poti-face-tu.html>
41. <http://www.sri.ro/Cyberintelligence.html>
42. <https://www.webcaster4.com/Webcast/Page/139/2631>
43. www.insaonline.org