Intelligence și globalizare

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

Veröffentlichungsversion / Published Version
Monographie / monograph

Mihai Marcel Neag **Eduard SIMION** **Alexandru KIS**

~ INTELLIGENCE ȘI GLOBALIZARE ~

EDITURA TECHNO MEDIA
Sibiu, 2015

Biblioteca Naţională a României

Descrierea CIP a Bibliotecii Naţionale a României

ISBN 978-606-616-189-3

Coperta: Alin KIS ©

CUPRINS

CAPITOLUL 1. INTELLIGENCE ÎN ERA GLOBALIZĂRII. COMUNITĂŢILE 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 existenţiale, efecte a căror înţelegere este necesară deoarece schimbă fundamentele analitice cu care ne-am obişnuit, modificând percepţii, comportamente şi atitudini într-o largă varietate de opţiuni şi cauzalități, ce pot fi traduse în beneficii sau dezavantaje. Modalităţile de cuantificare ale acestora diferă, la rândul lor, în funcţie de interesele, obiectivele şi cultura organizaţională a instituţiilor 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 şi tehnologic în ţările dezvoltate, ca sursă principală a creşterii lor economice, vulnerabilitatea macroeconomică ridicată a ţărilor în curs de dezvoltare la şocurile externe, precum şi contrastul dintre gradul înalt de mobilitate a capitalului şi mobilitatea internaţională a muncii, în special forţa de muncă necalificată, pot constitui surse de instabilitate (criză economică şi socială) şi produc situaţii de risc la adresa securităţii. Gestionarea economicului este puternic subordonată factorului politic, reverberaţiile dezechilibrelor de natură economică găsindu-şi o puternică reprezentare în stabilitatea şi coeziunea comunităţilor.

Totodată, globalizarea reduce capacitatea statelor de a menţine monopolul asupra informaţiei şi puterii, accentuează permeabilitatea graniţelor şi permite actorilor nonstatali să acumuleze capital. Organizaţiile societăţii civile se dezvoltă şi încep să acţioneze global, fără intermedierea guvernelor naţionale pe care le concurează ca reprezentate legitime în promovarea intereselor comunităţilor, mai puţin interesate de expresia politică, cât de acţiuni concrete care să le sprijine dezvoltarea şi bunăstarea.

Pentru a contracara această influenţă, sistemele politice naţionale trebuie să dea dovadă de flexibilitate şi să îşi dezvolte capacităţi de acţiune coordonată/ integrată, să redevină exponente ale intereselor maselor largi (promovând o formă avansată, modernă, a modelului statului social) şi să evite alienarea funcţională (înţelegând prin aceasta aservirea şi subordonarea energiei politice unor scopuri pur clientelare).

Din definiţia globalizării nu trebuie eliminată dimensiunea militară, care, în ultimii ani, s-a manifestat în special prin lupta împotriva terorismului şi fenomenelor de insurgenţă, mai mult sau mai puțin asociate acestuia. În contextul globalizării, această interconectare şi „afiliere" este un argument necesar şi suficient pentru a putea afirma că securitatea unei zone date este inseparabilă de securitatea globală. Cu toate că formele tradiţionale de luptă împotriva pericolelor şi ameninţărilor la adresa securităţii internaţionale - alianţele militare - sunt încă necesare eliminării factorilor şi surselor de insecuritate ce se globalizează, simpla proiecţie a puterii militare a statelor nu mai este suficientă. Conflictul, de orice natură, capătă noi caracteristici, suferind dezvoltări cărora statele şi instituţiile internaţionale nu sunt pe deplin pregătite să le facă faţă, dar la care reacţionează printr-un proces adaptativ ad-hoc.

Putem afirma că, prin dimensiunile sale de manifestare, globalizarea crează germenii unor presiuni ce influenţează mediul internaţional de securitate, dar şi modul în care percepţia securităţii se reflectă la nivelul experienţelor de securitate fizică şi spirituală ale fiecărui individ[1]. În ansamblu, globalizarea conduce la o nouă structură internaţională, divizată între acele ţări care sunt integrate în economia globală şi 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, scarcitatea 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 „unipolarităţii" (SUA ca principal agent de putere la nivel global) a constituit doar segmentul de tranziţie care a reliefat nevoia de reformă în înţelegerea noilor repere ale interdependenţelor dintre actorii arenei internaţionale. Noua arhitectură de securitate se manifestă ca un teren competiţional în care se redefinesc sisteme de referinţă, repere relaţionale şi niveluri de ambiţie, în virtutea unor seturi de valori şi interese mai mult sau mai puţin diferite, dar care poziționează statele în raport cu principalele entități - "subiecte" și "obiecte" ale scenei relațiilor internaționale.

Statele se definesc, din această perspectivă, ca puteri[2] (tradiționale/ emergente) – atribut dat de potențialul politic, economic, militar[1] al acestora – în antiteză cu statele

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

[2] Conceptul de putere capătă o înţelegere nuanţată. Dacă Joseph Nye o lega exclusiv de atingerea obiectivelor şi scopurilor propuse (în virtutea unui program predefinit) (Nye Jr., 1990, 177), dicţionarele definesc puterea: ca abilitate de a face anumite lucruri în parametri doriţi şi capabilitate de a exercita control/ autoritate/ influenţă (Oxford Mini Dictionary&Thesaurus); ca statut de forţă şi 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 organizaţiile internaţionale guvernamentale și o întreagă pleiadă de actori non-statali (organizaţii ale societăţii civile, reţele teroriste, firme transnaţionale, 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 fiinţa umană atunci când îşi evaluează existenţa şi perspectivele. Prin mecanismele complexe dezvoltate în timp, statul – într-o formulă a sa ideală – este garantul securităţii fizice şi demnităţii cetăţenilor, promovând premizele bunăstării şi asigurând libertatea individuală de exprimare şi opţiune. Strategia de securitate națională a României (SSNR, 2006, 4) își definește scopul ca vizând "*atât prevenirea şi contracararea pericolelor generate de mediul internaţional, cât şi garantarea stării de securitate internă, în ansamblul său, a siguranţei personale şi securităţii comunităţilor*", cerințe raportate la aspecte privind: securitatea individuală, securitatea energetică şi alimentară, securitatea transporturilor şi a infrastructurii, securitatea sănătăţii publice, sanitară, ecologică şi culturală, securitatea financiară, informatică şi informaţională.

Pe de altă parte, în condiţiile în care resortul principal al globalizării rezidă în dezvoltarea economică, aspecte ca: accesul la resurse, securitatea căilor de transport, dezvoltarea capacităţilor de producţie, asigurarea forţei de muncă adecvate (nivel de calificare în balanţă cu costul acesteia), găsirea şi prezervarea de noi pieţe de desfacere, transferul de bunăstare, pierderea exclusivităţilor, accesul la informaţie, duc la reconsiderarea distribuţiei rolurilor ierarhice ale statelor în sistemul relaţiilor internaţionale.

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

Procesul repoziţionării statelor pe scena relaţiilor politice internaţionale are o puternică semnificaţie în plan intern. Dobândirea unor avantaje economice strategice, asigurarea unui nivel decisiv de influenţă în evoluţia unor procese vitale, controlul procesualităţilor sistemice, prezervarea securităţii naţionale (şi reflectarea propriei securităţi la nivel regional şi global), ca obiective ale politicilor internaţionale, 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 şi responsabilă de roluri diferite, ca natură şi 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.

[1]capacitatea 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 naţional, situaţie în care echilibrul obţinut ar fi unul precar, supus contagiunii vecinătăţilor şi conexiunilor insecurizante. Securitatea fiecărei naţiuni trebuie concepută în context mult mai larg, care acceptă anumite ierarhii şi dinamici multidimensionale, dar nu și compromisuri care să alieneze spiritul ”contractului social” pe care apartenența la o formă de organizare statală o presupune. Alianţele şi aliaţii sunt esenţiali în a gestiona aspectele de securitate ale globalizării, atât din perspectiva resurselor, cât și a succesului acestei intreprinderi.

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 denumește aceste sistem teritorial ”*complex de securitate*” (Buzan, 2000, 196), în care interacțiunile militare, politice, economice, socio-culturale transced – facilitate de realități geopolitice – legăturile funcționale cu alte state, sub ”cupola” globalizării.

Dezvoltarea, la nivel global, a unui mare număr de organizaţii şi agenţii internaţionale indică o atenţie crescută a statelor cu privire la viaţa economică şi socială a popoarelor. Sprijinul pe care statele şi-l acordă bilateral sau multilateral capătă o importanţă aparte, securitatea socială depăşind tot mai mult barierele naţionale, cunoscând succesiuni graduale ale dezvoltării către limite teritoriale regionale.

Pe de altă parte, disfuncţiile interne sau cele de relaţionare 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 intervenţia sistemelor de securitate configurate tocmai în vederea diminuării riscurilor identificate – de aici reieşind rolul pe care organizaţiile internaţionale interguvernamentale îl au în domeniul securităţii.

Organismele internaţionale au un rol aparte în procesul de evaluare continuă a situaţiei de securitate la nivel regional şi global[1], prin analiza şi reconsiderarea permanentă a priorităţilor de securitate regională şi globală şi adaptarea conceptelor de securitate în raport cu noile evoluţii din toate domeniile de referinţă.

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 hibride[2], 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 Naţiunilor Unite pentru Dezvoltare (UNDP), prin ”Raportul anual asupra

[1]Modelul liberal al securităţii internaţionale se bazează pe utilizarea a patru instrumente: dreptul internaţional (substituie rezolvarea diferendelor prin conflict armat), organizaţiile internaţionale, integrarea politică şi democratizarea. Organizaţiile internaţionale sunt folosite de către comunitatea internaţională în scopul întăririi dreptului internaţional şi a prevenirii sau stopării agresiunii.

[2]Amenințările 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 (şcoli) distincte – absenţa fricii (*freedom from fear*) şi absenţa nevoilor (*freedom from wants*) (UNDP, 1994, 24). Concret, *absenţa fricii* se referă la protejarea indivizilor de conflicte violente, asociate cu sărăcia, lipsa capacităţilor statale de suport şi a altor forme de inechitate (promovând ca soluţii: asistenţa de urgenţă, prevenirea şi rezoluţia conflictelor, construcţia păcii), pe când *absenţa nevoilor* reprezintă o abordare holistică a rezolvării necesităţilor umane legate de: foamete, boli, dezastre naturale, care afectează mult mai mulţi oameni decât conflictele violente (şi 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 şi a democraţiei.

Şcoala "absenţei fricii" a căutat să impună ca subiect esenţial primatul protecţiei indivizilor în faţa conflictelor violente[3] (de aici decurgând asigurarea condiţiei minimale pentru drepturile și libertățile recunoscute), abordare considerată ca asigurând dimensiuni realiste şi gestionabile demersurilor analitice, operând cu termeni ca "asistenţa în caz de urgenţă" (*emergency assistance*), "prevenirea şi încheierea conflictelor" (*conflict prevention and resolution*), "construcţia păcii" (*peace-building*), dar şi cu o componenetă cheie a agendei sale, care a determinat o adevărată revoluţie în modalitatea de interpretare a ideii de suveranitate statală – conceptul "responsabilităţii de a proteja"[4].

Curentul absenţei nevoilor ca şi condiţie primordială a securităţii umane (conceptul "extins" al securităţii umane) porneşte de la premiza că foametea, bolile şi dezastrele naturale ucid de departe mult mai mulţi oameni decât războaiele, genocidul şi terorismul la un loc, fiind necesară asocierea acestora celorlaltor ameninţări la adresa securităţii umane. Eliberarea de nevoi, dincolo de asocierea cu violenţa 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 şi politice ca: dreptul inerent la viaţă, nesupunerea la tortură sau acte de cruzime, la arest sau detenţie ilegală, dreptul la prezumţia de nevinovăţie, la un proces rapid şi corect, dreptul la liber sufragiu, la intimitate, la libertatea de expresie, asociere şi întrunire. Această libertate cuprinde şi drepturile economice, sociale şi culturale – dreptul la hrană, sănătate, educaţie şi protecţie socială, dreptul la muncă, dreptul de a participa la viaţa culturală a comunităţii şi a se bucura de beneficiile progresului ştiinţific şi a aplicaţiilor sale. Demnitatea, ca dimensiune a trăirii, presupune absenţa oricărei forme de deprivare, ca: foametea, ignoranţa, incapacitatea, dizabilitatea şi 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 referinţe de securitate economică, alimentară, a sănătăţii, a mediului, siguranţă personală şi a comunităţii şi securitate politică

[2] Raportul 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

[4] Principiile de bază ale *responsabilităţii de a proteja*, ca recurs la acţiune în condiţii specificate de risc la adresa securităţii umane, au fost conturate în 2001, în cadrul sesiunii Comisiei Internaţionale privind Intervenţia şi 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 siguranţei, bunăstării individuale şi a demnităţii umane inclusiv prin eludarea autorităţii de stat, în condiţiile în care aceasta devine ea însăşi ameninţare la adresa securităţii propriilor cetăţeni. De aici rezultă că recunoaşterea internaţională a suveranităţii unui stat implică o responsabilitate subsidiară în ce priveşte protecţia comunităţii 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 şi consistent la procesele democratice care le vor afecta vieţile şi viitorul ca indivizi sau ca persoane.

În acest context intră în discuţie problematica intervenţiei cu scop umanitar[1], care se referă la interferenţa armată[2] a unui stat (grup de state) pe teritoriul suveran al altui stat, cu obiectivul declarat de a pune capăt sau a reduce suferinţele populaţiei acestuia, rezultate ca urmare a unui conflict armat intern, a crizei umanitare sau a crimelor la care sunt supuşi de către aparatul propriului stat, obiectiv care nu poate fi asociat cu scopuri anexioniste sau atingeri aduse integrităţii teritoriale[3] a statului ţintă. Actualmente, această logică este limitată de către ONU la cazuri de genocid, purificare etnică şi crime împotriva umanităţii[4], situaţii în naţiunile se declară pregătite ca – prin rezoluţie a Consiliului de Securitate – să intervină militar, în caz de epuizare a mijloacelor pacifiste menite să amelioreze situaţia.

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 scientifizată a mediului uman din teatrul de operații, care are ca scop dezvoltarea, antrenarea și integrarea produselor de

---

[1]Bernard Kouchner este considerat părintele intervenţionismului modern, care promovează responsabilitatea democraţiilor 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 faţetei umanitare a intervenţiei militare este prezentată în Kis, 2008

[2]După Kofi Annan, intervenţia nu trebuie înţeleasă ca un recurs exclusiv la forţă, existând multe alte posibilităţi de asistenţă (Kofi A. Annan,*Two concepts of sovereignty*, în ”*The Economist”*, 18.09.1999, apud http://www.un.org/News/ossg/sg/stories/articleFull.asp?TID=33&Type=Article).

[3] Aşa cum s-a întâmplat în cele din urmă cu Serbia, căreia i s-au oferit garanţii privind integritatea sa teritorială, ulterior nesocotite

[4]Genocidul, purificarea etnică şi crimele împotriva umanităţii sunt în egală măsură ameninţări atât din perspectiva securităţii umane, cât şi la adresa securităţii şi păcii internaţionale.

[5] R. 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 operațional[1].

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 partenere există preocupări similare, materializate în determinarea relevanței pentru mediul operațional a analizei bazate pe metodologia Terenului Uman (ABCA[2]) sau dezvoltarea capabilității de înțelegere a aspectelor culturale (Finabel[3]).

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 capabilitate este responsabilă. Specialiștii din cadrul CIMIC COE au fundamentat conceptul de *Advanced Cultural Competence* (*Competență Culturală Avansată*), model care servește înțelegerea și faciliteaza 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 naţională" şi „securitatea naţională", 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 partnere 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-I-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 obţinere,
- sursa/origineaşi/sau mijloacele de obţinere,
- tehnica de înregistrare sau forma de exprimare,
- modul de reglementare,
- procedura de descriere,
- scop/utilitate,
- deciziile şi acţiunile la care servesc,
- direcţia şi sensulde vehiculare (circuitele fluxului informaţional),
- legătura dintre producătorul informaţiei şi mediu,
- preponderenţa elementelor componente,
- nivelurile de analiză,
- regimul juridic,
- criteriile de analiză,
- domeniile de activitate socială la care se referă (politic, economic, tehnic, ştiinţific, militar etc.) şi/sau domeniile de realizare a siguranţei naţionale (ordine constituţională, antiterorism, siguranţă economică etc.).

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

În aceeași idee, S. Petrescu arată că *”informaţiile 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 informaţii, sintetizate etc., vor*

[1]Propunere 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 şi conţinut operativ în măsură să servească factorului de decizie (produse de tip intelligence)" (Petrescu, 2007, 32).

În dicţionarele româneşti, *informaţia* este definită ca *"fiecare dintre elementele noi, în raport cu cunoştinţele prealabile, cuprinse în semnificaţia unui simbol sau a unui grup de simboluri (text scris, mesaj vorbit, imagini plastice, indicaţie a unui instrument etc.)"*(DELR, ediţia a II-a, 1998), sau *"totalitatea materialului de informare şi de documentare"* (Marele dicţionar de neologisme, 2000)[1].

Oxford Dictionary defineşte *intelligence* ca *"informaţie, în special cu valoare militară"* (Homby, 1999, 620), însă considerăm această explicaţie doar parţial satisfăcătoare ca relevanţă în ceea ce priveşte marcarea diferenţei dintre informaţia brută, neprelucrată (date iniţiale) şi informaţia rezultată în urma procesului denumit, în limbaj de specialitate, "*ciclul Intelligence*" (figura 1.1). În schimb, această definiţie ar servi ca argument al traducerii în limba română a termenului englezesc "*intelligence"* ca "*informaţii militare",* în condiţiile în care traducerea sa ca *"informaţie"* este relativ suficientă, iar ca *"inteligenţă"*, nerelevantă şi producătoare de confuzii[2].

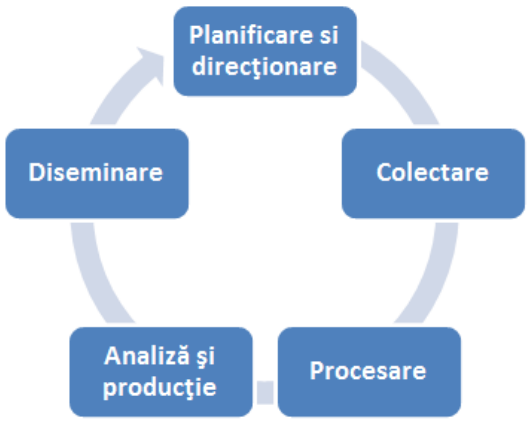


Figura 1.1: Ciclul Intelligence[3]

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 şi în domeniul afacerilor ("*business intelligence*", *"competitive intelligence"*) (Măzăreanu, 2006, 361) – cu rezerve faţă de traducerea termenului *intelligence* ca *inteligenţă* 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 acesteia în timp și spațiu (figura 1.2).

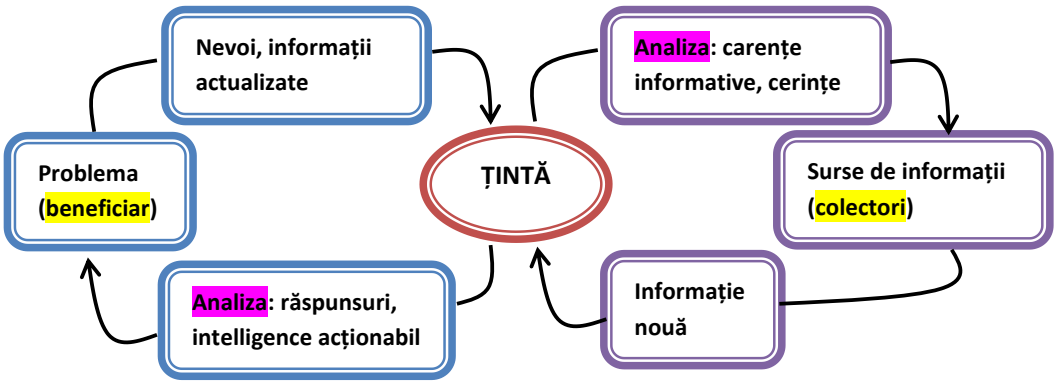


Figura 1.2: Procesul Intelligence din perspectiva orientării spre țintă (Clark, 2003)

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 capabilităților și intențiilor adversarului, care afectează folosirea propriilor capabilități în baza deciziei elementelor de comandă. (JP-2.0, 2013)

După I. Tulică, conceptul *intelligence* defineşte în sens general, ansamblul de activităţi ce ţin de domeniul informaţiilor, contrainformaţiilor şi protecţiei intereselor fundamentale ale statului ori a sistemelor de valori naţionale. (Tulică, 2009, 3-4)

La nivelul Academiei Naţionale de Informaţii (ANI), termenul *intelligence* a fost adoptat ca atare, regăsindu-se în atât în produsele activităţii de cercetare ale Academiei, cât şi în denumirea *Institutului Naţional de Studii de Intelligence* din cadrul acesteia.[1] Acest împrumut lexical şi conceptual este un compromis determinat de necesitatea de a opera o distincţie - anume că *intelligence* nu înseamnă doar informaţie (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 ***”Informaţii pentru securitate naţională”*** - produs analitic, rezultat al activităţii specializate de căutare, identificare, obţinere, prelucrare/procesare a datelor referitoare la disfuncţii, vulnerabilităţi, factori de risc, ameninţări, stări de pericol la adresa principiilor şi normelor politico-sociale statornicite prin Constituţie (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 şi informaţiilor 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 informaţii colectate sau furnizate de către surse umane/ *AAP-6*), GEOINT (Geospatial Intelligence – date şi informaţii geospaţiale înregistrate prin intermediul sateliţilor, fotogrametriei aeriene[2], hărţilor şi datelor despre teren), MASINT (Measurement and Signature Intelligence – date rezultate în urma analizei rezultatelor măsurătorilor şi a semnăturilor electronice), OSINT (Open Source Intelligence – informaţii 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 şi

[1] http://www.animv.ro/ro/index.php?ccs=30

[2] aceste două surse acoperă denumirea de IMINT / Imagery Intelligence (informaţii rezultate din analiza imaginilor satelitare şi a fotografiilor aeriene)

electronice), TECHINT (Technical Intelligence – informaţii rezultate din analiza armamentului şi echipamentelor folosite de către forţele armate ale altor naţiuni), FININT (Financial Intelligence – informaţii rezultate din analiza tranzacţiilor financiare, etc.) și altele.

Noțiunea de *Intelligence* se regăsește la nivel strategic, operaţional şi 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 priveşte capabilităţi, vulnerabilităţi şi cursuri de acţiune probabile ale altor naţiuni - 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, rezultantele ciclului *Intelligence* sprijină deciziile necesare operaţiilor tactice, fiind focalizate pe mediul acţional şi ameninţările specifice[1], pemițând comandanților să ia decizii pentru acțiuni și sarciniîn 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, capabilități de procesare și diseminare, etc.

Capabilitatea Intelligence în societatea informațională

Începutul secolului XXI este dedicat eforturilor de a dezvolta forme de cooperare şi politici de securitate care să răspundă globalizării insecurităţii, conştientizând, totodată, că globalizarea nu elimină preocupările geopolitice tradiţionale. Poziţiile divergente, dar şi nevoia atingerii une arii de consens, sunt puternic vizibile în cadrul forumurilor şi summiturilor unde se întrunesc lideri-cheie ai planetei; aceştia sunt provocaţi să depăşească sfera intereselor strict naţionale (presiunile politice și sociale interne) şi să adopte un limbaj politic global (o soluție de compromis), în care să încadreze propriile priorităţi. În acest sens, este evident că o capacitate adecvată de control şi gestiune a securităţii presupune previziune, anticipare; orice politică de acţiune trebuie să se bazeze pe predicţii 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.

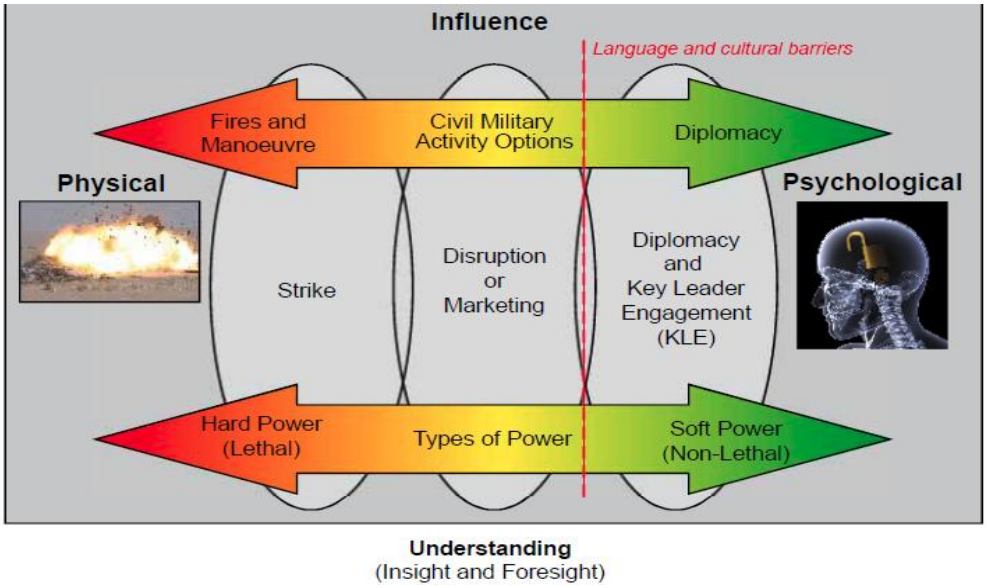


Figura 1.4 Spectrul de influență în cadrul operației, raportat la capacitatea de înțelegere - după doctrina britanică (JDP 2-00, 2011, fig. 1.4)

Comunitățile de Intelligence au cunoscut, la rîndul 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 guvernanțe 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 rămânînd o problemă de actualitate.

Dezvoltarea **cadrului colaborativ** (figura 1.5), pe plan național sau internațional, între serviciile și agențiile din spectrul intelligence (dar și cu o gamă variată de parteneneri.), 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. Contracararea optimă a amenințărilor actuale la adresa securității impune cooperarea în cadrul formal al unor comunităţi naţionale de informaţii[1], completate cu ramificațiile și legăturile externe de cooperare și conlucrare ale acestora în vederea determinării eficiente a riscurilor şi amenințărilor de securitate la nivel naţional, regional şi internaţional.

[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,

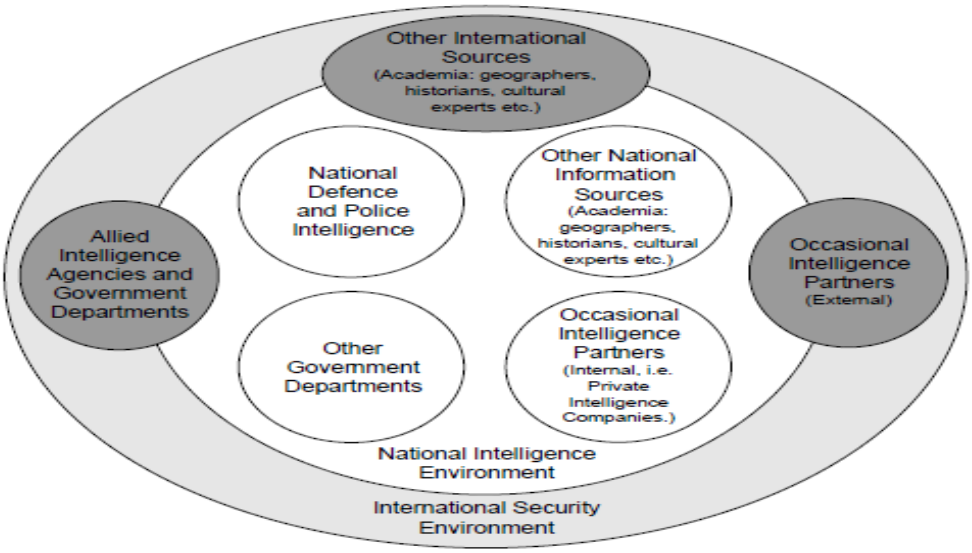


Figura 1.5 Cadrul general de relaționare în domeniul securității și al Intelligence (JDP 2-00, fig. 1.3)

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 definire 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 capabilității Intelligence (Steele, 2013)

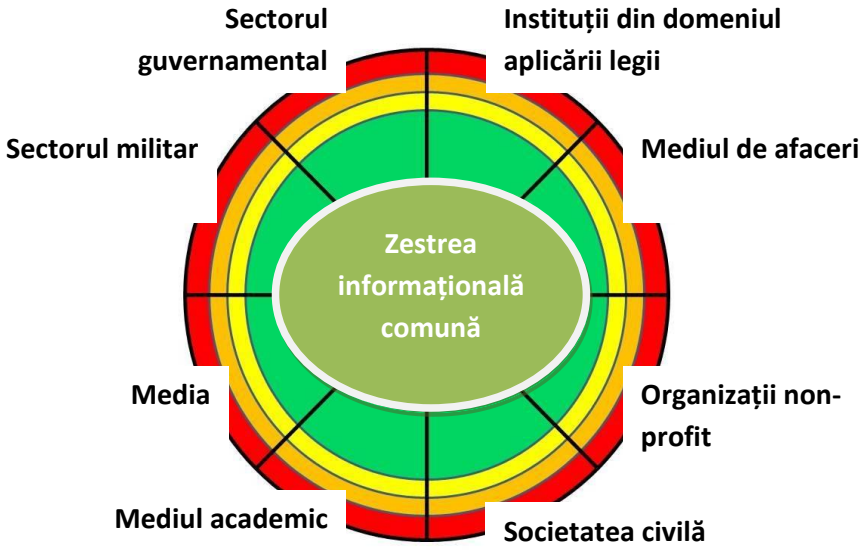


Figura 1.6 Cele opt medii ce contribuie la zestrea informațională comună (Steele, 2013)

Conceptul „Intelligence” este, în mod general, abordat din trei perspective – ca proces, organizaţie şi 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.

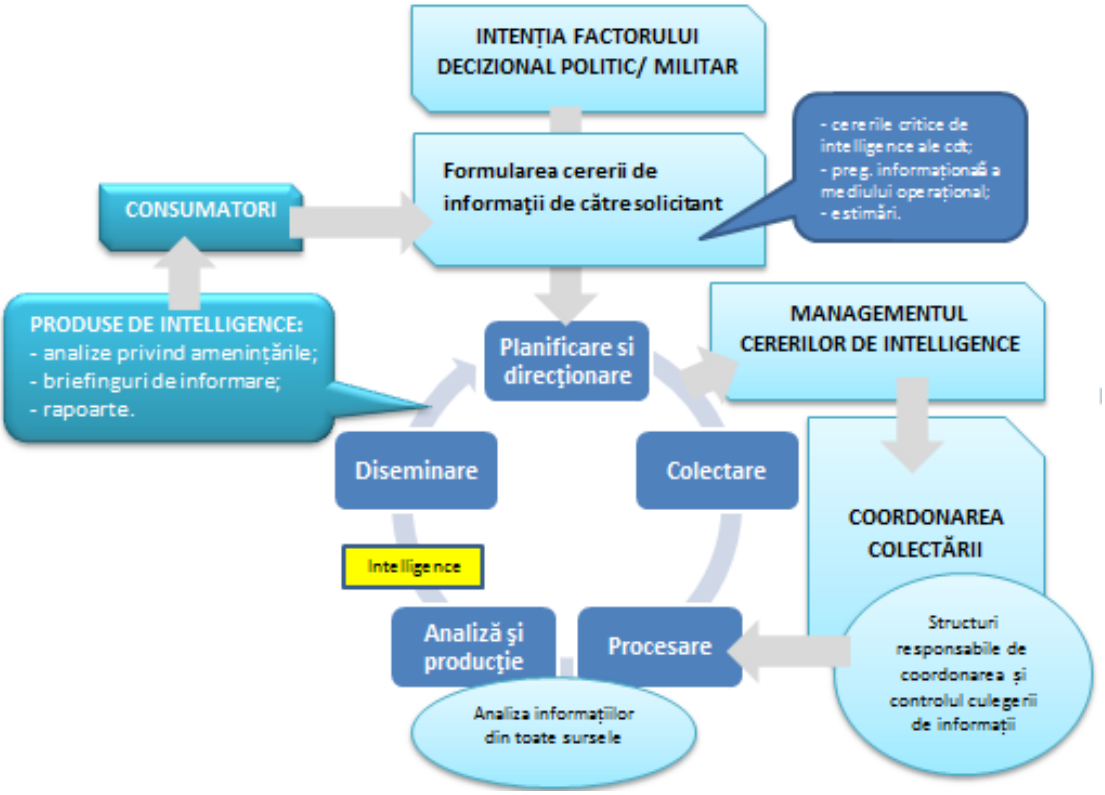


Figura 1.7 Structuri și activități în ciclul Intelligence

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 mutaţie a intereselor dinspre zona geopolitică spre cea geoeconomică, abilitatea statului constând acum în gestionarea cunoaşterii la nivel strategic pentru consolidarea sectorului administraţiei publice, al economiei, al educaţiei, al cercetării şi 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.

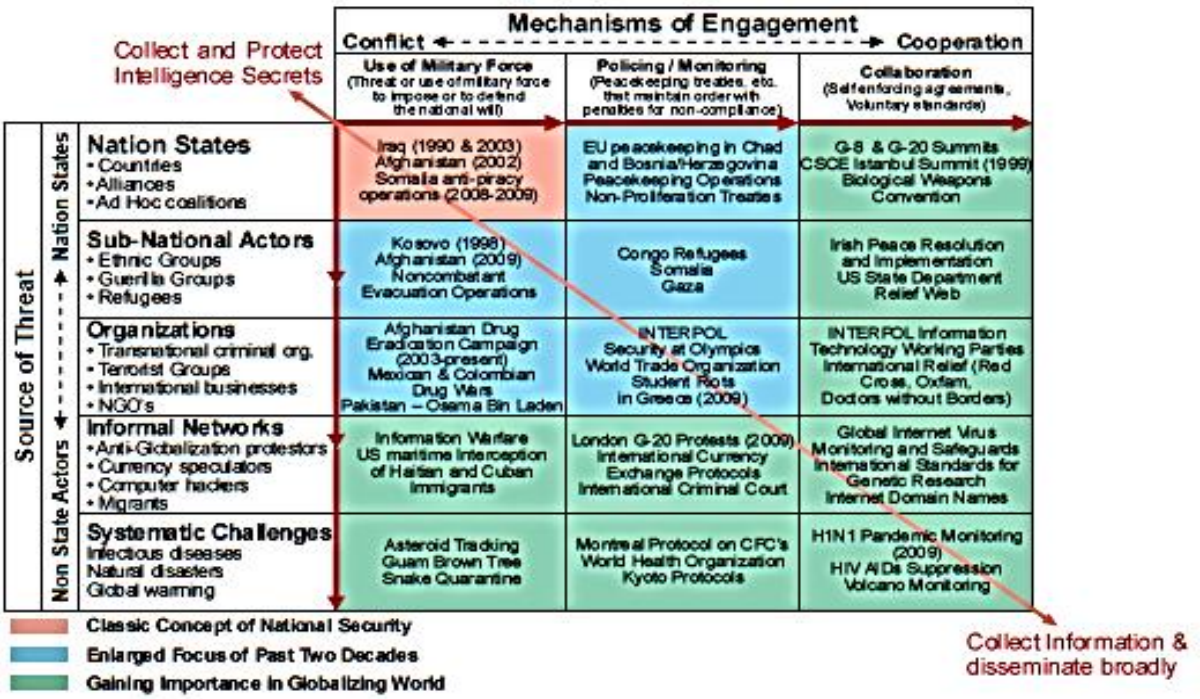


Figura 1.8 Colectarea și diseminarea informațiilor raportat la conceptul extins al securității naționale. Tipuri de amenințări și mecanisme de angajare (Pherson, 2009, 15)

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 capabilitățile 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 capabilităților 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 informații[1] și diseminarea acestora, facilitată de inovațiile din domeniul tehnologiei informațiilor (Vallima și Hoffman, 2008), care permite inter-conectivitatea în combinații practic nelimitate a rețelelor de cunoaștere.

[1] realitate care, în absența controlului asupra proveniență 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, capabilități 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 importanţă tot mai mare în filtrarea/ analiza informaţiilor şi semnalarea ameninţărilor emergente.

O posibilă soluție este folosirea *crowdsourcing*-ul - opţiune 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 şi diferitele organizaţii folosesc informaţii obţinute etic şi 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 capabilitatea 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, carefundamentează 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 concurenţă cu serviciile guvernamentale). Pe măsură ce securitatea îşi lărgeşte aria de referinţă, tot mai multe organizaţii (think-tankuri, mediul academic, societăţi private cu obiect de activitate în domeniul securităţii, organizaţii ale societăţii 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 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 atît 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 problematici 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 agreate privind managementul informației, pornind de la echilibrul adecvat dintre principiile *nevoii de a cunoaşte* (”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 informaţii, 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 relaţii active cu beneficiarii, în sensul transformării *feed-back*-ului într-un instrument de îmbunătăţire a performanţei, 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, înţelegerea profundă a tendinţelor majore și a nuanțelor regionale de evoluţie ale securităţii internaţionale, precum şi a oportunităților de afirmare națională în acest context, constituie o condiţie esenţială a progresului şi prosperităţii.

Asociată cu înţelegerea şi evaluarea corectă a proceselor interne, securitatea fiecărei ţări, ca şi securitatea comunităţii internaţionale, se bazează nu numai pe capacitatea de adaptare și reacţie la noile realități sau provocări ci, mai ales, pe capacitatea de anticipare (unde disciplina Intelligence joacă un rol esențial) şi de acţiune pro-activă.

Strategiile naționale de securitate urmăresc integrareaîntr-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 eforturidincolo 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 aliniază tendințelor globale, în linie cu politicile generale ale structurilor supra-naționale la care statul este parte, și se regăsește în toate aspectele definitorii ale capabilității, 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 naționale[1] 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 instituţii ale României**:** Serviciul Român de Informaţii (SRI), pentru informaţiile din interiorul ţării, Serviciul de Protecţie şi Pază (SPP), pentru protecţia demnitarilor români şi străini pe timpul prezenţei lor în România, a sediilor de lucru şi a reşedinţelor acestora[2], Serviciul de Informaţii Externe (SIE) - specializat în obţinerea de

[1]din 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/

informaţii din străinătate[1], Ministerul Apărării Naţionale- prin Direcția Generală de Informații pentru Apărare[2], Ministerul Administraţiei şi Internelor - prin Direcţia Generală pentru Informaţii şi Protecţie Internă (DGIPI)[3], Ministerul Justiţieișisi Serviciul de Telecomunicaţii 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 acestorautorităţi sunt exercitate de către Preşedintele României, Parlament,Consiliul Suprem de Apărare a Ţării (CSAT) şi 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 si 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 șiBorn, 2003)

În plan funcțional, activitatea autorităţilor din domeniulsecurității și al informațiilor este planificată lanivel strategic de către Comunitatea Naţională de Informaţii, carefuncţionează sub coordonarea CSAT şi care reprezintă „reţeauafuncţională a autorităţilor informative din sistemul securităţiinaţionale” (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 instituţia de stat specializată în domeniul informaţiilor externe privind siguranţa naţională, apărarea României şi a intereselor sale (http://www.sie.ro/index.html)

[2] structura specializată responsabilă pentru colectarea, procesarea şi verificarea informaţiilor privind factorii de risc interni şi externi, militari şi nonmilitari, coordonarea măsurilor contrainformative şi cooperarea cu serviciile/ structurile departamentale naţionale de informaţii, cât şi cu cele ale statelor membre ale alianţelor, coaliţiilor şi organizaţiilor internaţionale la care România este parte şi asigură securitatea informaţiilor clasificate naţionale, NATO şi UE la nivelul Ministerului Apărării Naţionale (Duțu și Bogzeanu, 2010, 58-59)

[3] structura specializată a Ministerului Afacerilor Interne care desfăşoară activităţi de informaţii şi protecţie internă, în vederea asigurării ordinii publice, prevenirii şi combaterii ameninţărilor la adresa siguranţei naţionale privind misiunile, personalul şi informaţiile clasificate în cadrul ministerului (http://www.dgipi.ro/)

[4] organul central de specialitate, cu personalitate juridica, ce organizeaza si coordoneaza activitatile in domeniul telecomunicatiilor speciale pentru autoritatile publice din Romania si alti utilizatori prevazuti de lege (http://www.stsnet.ro/)

viitorului. Influența pe care procesele asociate globalizării o au asupra capabilității 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.

Caracteristice 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 şi neconvenţionale, prin care să se realizeze obiectivele referitoare la misiunile antiteroriste, contra proliferării armelor de nimicire în masă, contra insurgenţei, 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 informaţiilor 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 naţional care implică nu doar instituţiile guvernamentale şi civile, ci merg până la responsabilizarea individuală a cetăţeanului și la promovarea unei culturi de securitate[1] care să răspundă cerințelor actuale de cunoaștere.

Bibliografie

1. AARONSON, Michael, DIESSEN, 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 Ştiinţifice cu participare naţională *Tehnologiile mileniului al III – lea şi viitorul activităţii de informaţii* Ediţia a III—a, 27 Noiembrie, Bucureşti
3. ANNAN, Kofi A. (1999)*Two concepts of sovereignty*, în "*The Economist"*, apud http://www.un.org/News/ossg/sg/stories/articleFull.asp?TID=33&Type=Article
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`ingerence*. *Peut-on les laisser mourir?*, Denoel, Paris
6. BUZAN, Barry (2000) *Popoarele, statele si 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-Ştefan (2005) *Componenta etnico-religioasă a conflictelor*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti
9. DUŢU, Petre (2013) *Ameninţări asimetrice sau ameninţări hibride: delimitări conceptuale pentru fundamentarea securităţii şi apărării naţionale*, Editura Universităţii Naţionale de Apărare „Carol I" Bucureşti, http://cssas.unap.ro/ro/pdf_studii/amenintari_asimetrice_sau_amenintari_hibride.pdf
10. DUŢU, Petre, BOGZEANU, Cristina (2010) *Interesele naţionale şi folosirea instrumentelor de putere naţională pentru promovarea şi apărarea acestora. Cazul României*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti
11. DUVAC, Ion (2007) *Suport de curs Intelligence – aplicații*, Facultatea de Sociologie și Asistență Socială, Universitatea din București, București

[1] o abordare proactivă a cestui aspect impune colaborarea reprezentanţilor comunităţii de intelligene cu membrii societăţii 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, JOHNSSON,Anders B. (redactori-şefi), BORN, Hans (redactor şi autor principal) (2003) *Controlul parlamentar al sectorului de securitate*. *Principii, mecanisme si 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) *"Inteligenţă" în business intelligence*, Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza" din Iași, Tomul LII/LIII Ştiinţe Economice 2005/2006, în http://anale.feaa.uaic.ro/anale/resurse/54_Mazareanu_V_-_"Inteligenta"_in_Business_Intelligence.pdf
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, Bucureşti
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 şi 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) înhttp://www.fsw.vu.nl/en/research/research-programmes/social-and-cultural-anthropology/index.asp
34. ***, *Doctrina naţională a informaţiilor pentru securitate* (2004) Editura S.R.I.,. Bucureşti, 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. Dicţionarul Explicativ al Limbii Române (DELR), ediţia 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 dicţionar 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 Alianţa se va confrunta, cu un orizont de acţiune până în 2030, în scopul identificării ameninţărilor relevante şi implicaţiilor militare şi 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 entităţi (statale sau non-statale);
- Fragilitatea altor entităţi (incluzând instabilitatea cauzată de statele eşuate);
- Natura (dezastre naturale, resurse energetice, asigurarea apei şi hranei, etc.);
- Schimbări societale sistemice (care antrenează transformarea organizaţiilor militare în cadrul societăţilor aflate în schimbare);
- Mediul operațional complex.

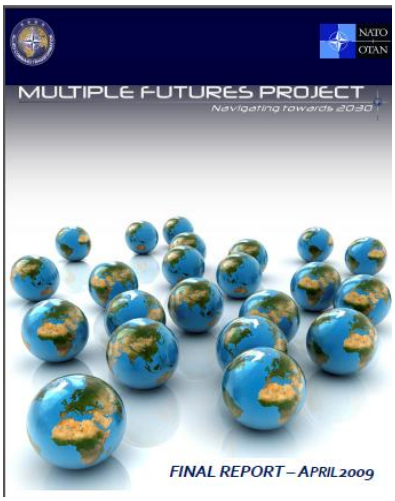


Figura 2. 1 Raportul final al MFP

Studierea algoritmilor MFP privind evoluția stării de securitate a viitorului, sugestiv denumiți: ”Latura întunecată a exclusivităţii” (statele slabe şi eşuate generează instabilitate în ariile de interes, iar statele lumii globalizate se confruntă cu opțiunile strategice ce decurg din această realitate), ”Stabilitatea înşelătoare” (statele dezvoltate preocupate de schimbările societale şi problemele demografice în detrimentul riscurilor geopolitice), ”Contradicţiile modernităţii”(societăţile avansate, raţionale, bazate pe reţele, cu fragilităţi inerente, sunt supuse provocărilor unor regimuri externe autoritariste) şi ”Politicile noilor puteri” (un număr crescând de puteri majore, competiţia şi proliferarea subminează valoarea organizaţiilor internaţionale) (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 şi premizele a patru direcţii fundamentale ale transformării Alianţei, sintetizate în:

- reasigurarea determinării de a acţiona împotriva unui atac armat, în conformitate cu prevederile art. 5;
- flexibilizarea în ce priveşte tipurile de atac ce se încadrează în categoria non-art. 5 – provocări netradiţionale sau dezastre umanitare ce reclamă contribuţia cu forţe militare;

- responsablitatea împărţită a tuturor membrilor în ce priveşte contribuţia la gestionarea crizelor în condiţiile în care Consiliul Nord-Atlantic agreează o astfel de misiune;
- reafirmarea angajamentelor cu partenerii şi alte naţiuni din afara teritoriului Alianţei în vederea asigurării premiselor diplomaţiei defensive, a cooperării militare, construcţiei şi întăririi capacităţilor de parteneriat. (Binnendijk şi Hoon,2010,1)

Conceptul Strategic NATO din 2010 preia și prefigurează prioritățile strategice pentru următoarea decadă, furnizând cerințele și asigurând cadrul de dezvoltare a capabilităților – 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 capabilitățile 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 capabilitățile actuale ale Alianței trebuiesc menținute și dezvoltate[2] - concurent logicii inițiativei Smart Defence[3], regăsită în diferite proiecte și programe de dezvoltare a capabilităților (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/ NORDEFCO, 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 Summitului[4] prevede inclusiv îmbunătățirea capabilităților de

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

[2] în special pentru capabilități 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, capabilitatea 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 capabilități 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 capabilitățile pe bază de rețea[1]. 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 şi al reţelelor lucrative pe care statele aliate le-au realizat în timp, în cadrul acţiunilor presupuse de dezvoltarea şi experimentarea conceptelor, actualizarea doctrinelor şi procedurilor, derularea unor proiecte de cercetare ştiinţifică şi tehnologică, planificarea apărării, educarea şi instruirea personalului – ca domenii funcţionale ale transformării.

Nivelul conceptual al transformării – inclusiv pentru domeniul Intelligence – este exploatat şi îşi găseşte 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 România[2]).

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 capabilităţile specificate în obiectivele forţei la nivelul structurilor cu care contribuie în cadrul Alianţei.

Dincolo de exprimarea voinței politice și asigurarea resurselor bugetare, de aici decurg responsabilităţi privind asigurarea interoperabilităţii, dislocabilităţii, achiziţiilor de echipamente, modernizarea procesului de educare şi instruire, adecvarea sistemului legislativ şi reglementărilor specifice, dezvoltarea şi participarea la forme instituţionalizate ale sprijinului acordat procesului de dezvoltare în NATO, asumarea de responsabilități și participarea în diferite forme de cooperare.

[1] Abilitatea cognitivă şi tehnică a Alianţei de a conjuga diferite componente ale mediului operaţional prin intermediul reţelelor informatice şi a infrastructurii de informaţii (concretizată în Capabilitatea bazată pe reţea a NATO - NNEC) ilustrează crezul cooperării („a împărţi [*informaţie* – n.a.] pentru a învinge") ca trăsătură de cultură organizaţională, conducând către o mai bună avertizare situaţională şi sprijinind procesele decizionale ce duc, în ultimă instanţă, la interoperabilitate şi eficienţă acţională, optimizarea consumului de resurse, salvarea de vieţi omeneşti, etc. Urmărind asigurarea coerenţei şi integrării eficiente a sistemelor deja existente, NNEC urmăreşte obiective specifice la nivel de personal/ operatori, arhitectura proceselor şi tehnologia de suport, cu implicaţii la nivelurile strategic, operativ şi 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

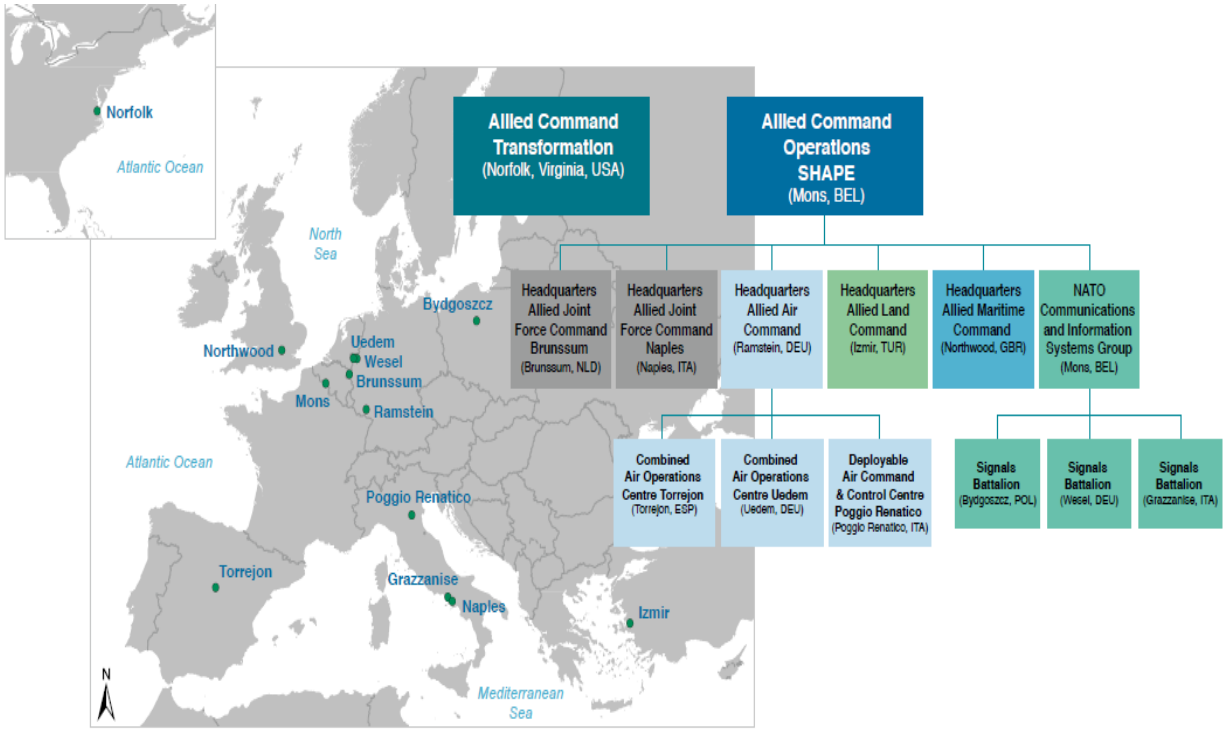


Figura 2.2: Structura actuală de comandă a NATO
(Sursa: NATO Public Diplomacy Division, *The Secretary General's Annual Report 2012*, 16)

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 capabilităților 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 capabilitatea 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 capabilității 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 acurateței necesare 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 acesteia.

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 standarde[1] care să acopere întreg spectrul acestora.

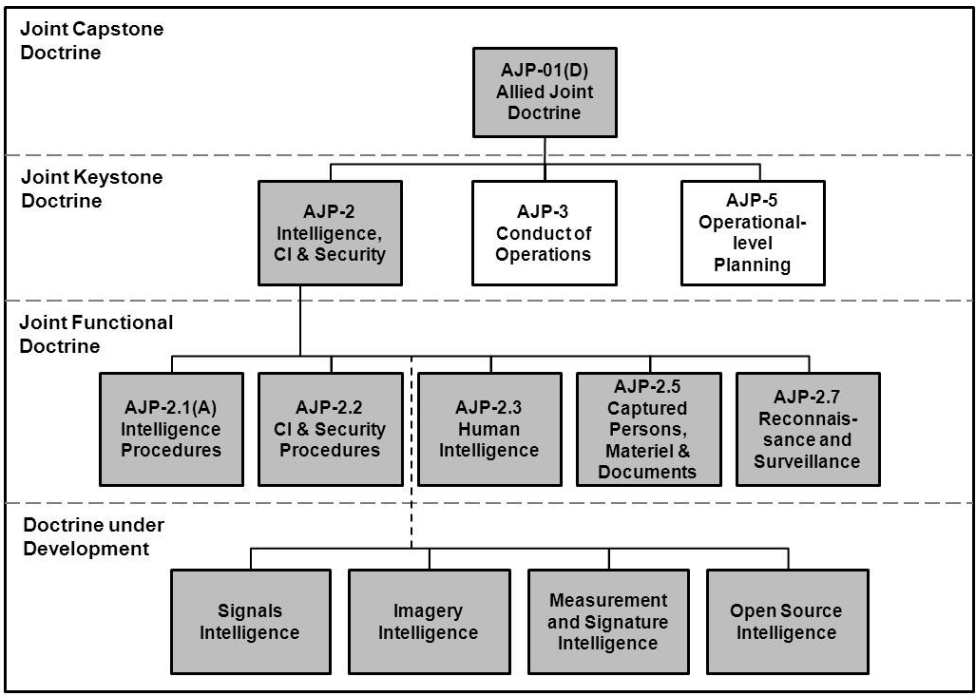


Figura 2.3 Arhitectura doctrinelor întrunite pentru Intelligence în NATO

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, distingem[2]:

- Intelligence Acustic (ACINT), derivat din date legate de sunet, interceptat prin diferite dispozitive speciale: hidrofoane, geofoane, 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

[1]SIGINT (Olanda), IMINT (Canada), MASINT (Canada), OSINT (Canada), Biometria în sprijinul operațiilor militare (Olanda)
[2]Descrierea 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 capabilități integrate – Intelligence, Supraveghere și Recunoașteri Întrunite/ Joint Intelligence, Reconaissance, 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 operațiilor[1].

Bineînțeles, nivelul de integrare a capabilităților ISR naționale la nivelul Alianței este unul perfectibil[2], 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 (MAJEX[4]), 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.

[1]Inițiativa 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%93-NATO-Agency-hosted-exercise-puts-NATO%E2%80%99s-Joint-ISR-Smart-Defence-initiative-into-practice.aspx

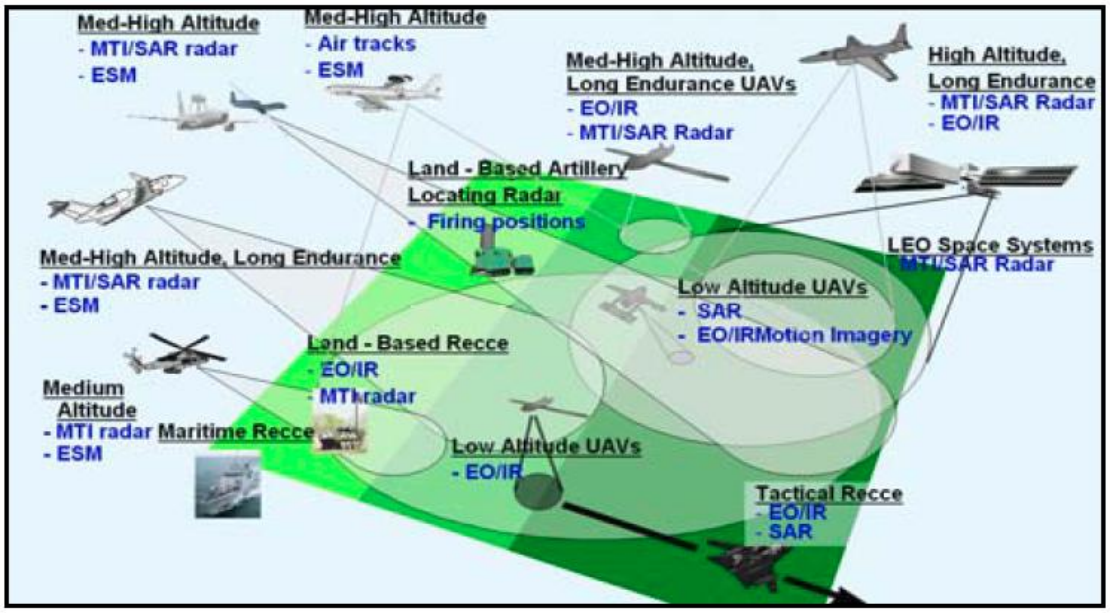


Figura 2.4 Schema senzorilor ISR din MAJIIC (2006), axată exclusiv pe colectorii tehnici (http://www.nato.int/docu/update/2007/pdf/majic.pdf)

Exercițiul-test Unified Vision, ediția 2014 (figura 2.5), a avut în vedere nu doar interconectarea capabilităților 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 capabilității JISR în NATO este reprezentat în figura 2.6, cuprinzând principalele etape ce vor permite realizarea cerințelor specifice până la finalul anului 2014.

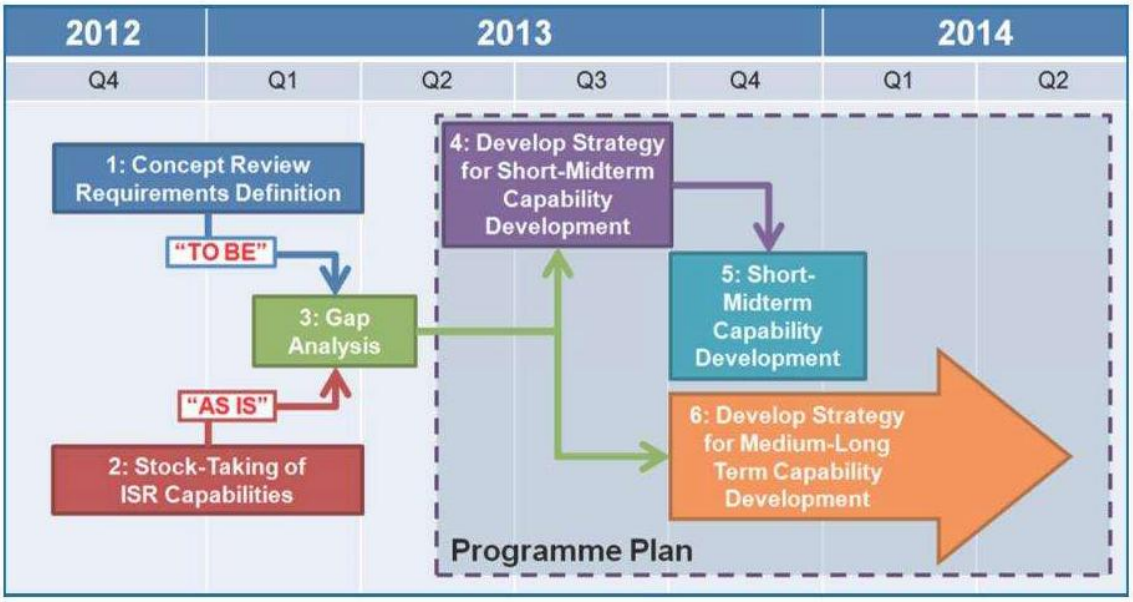


Figura 2.6 Planul de dezvoltare a capabilității JISR în NATO (http://www.aofs.org/wp-content/uploads/2013/10/131010.03-NIAG-SG177-Munday.pdf)

Dezvoltarea capabilității 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)

[1] http://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 2017[1] (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 (subscrise 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 capabilitățile, 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)

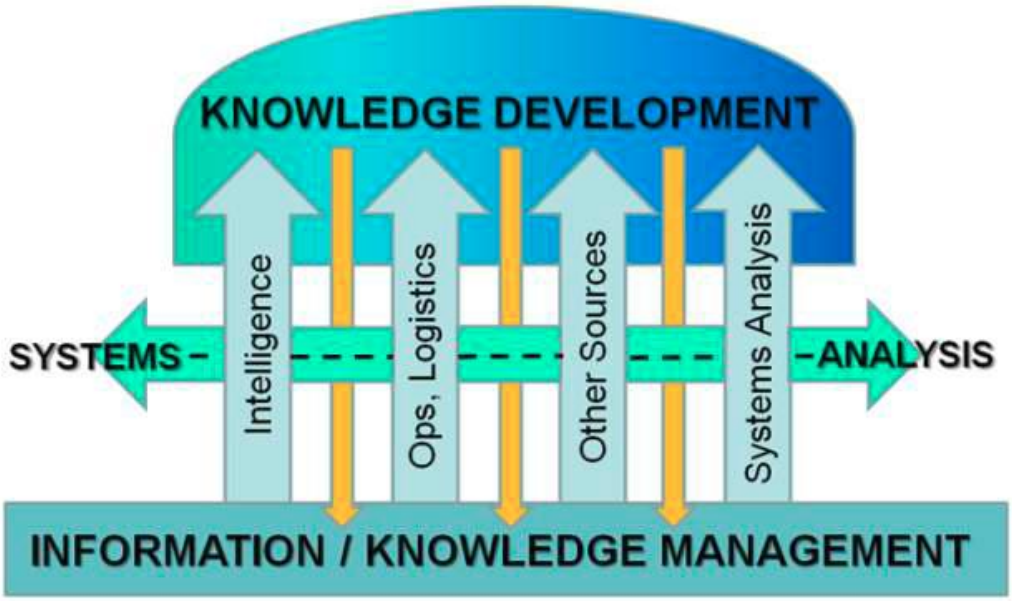


Figura 2.7 Relația dintre dezvoltarea cunoașterii și managementul informației/ cunoașterii (Bi-SC – KD, 2011, 5-1)

Conceptul comun al Comandamentelor Strategice privind Dezvoltarea Cunoașterii descrie KD ca integrare a datelor izolate într-un bloc informațional și relațional utilizabil[1], 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 capabilității 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 capabilitățile 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 capabilități biometrice în cadrul NATO, fapt demonstrat de realitatea mediului operational 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 4715[1]) în măsură să asigure cerințele de interoperabilitate ale sistemelor biometrice naționale.

Partea de fundamentare doctrinară a modalității de folosire a acestei capabilități este în plin proces de dezvoltare, proiectul inițial al publicației aliate întrunite denumite ”Countering Threat Anonimity: Biometrics in support of NATO Operations”, a cărei custode este Olanda, fiind lansat spre dezbatere 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 acestuia[2]

Efortul de standardizare a capabilității 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.

[1] *STANAG4715*, Biometric Data Interchange, Watch listing and Reporting Standard, octombrie 2013
[2] http://kitup.military.com/2013/08/marines-soldiers-biometrics-tool.html

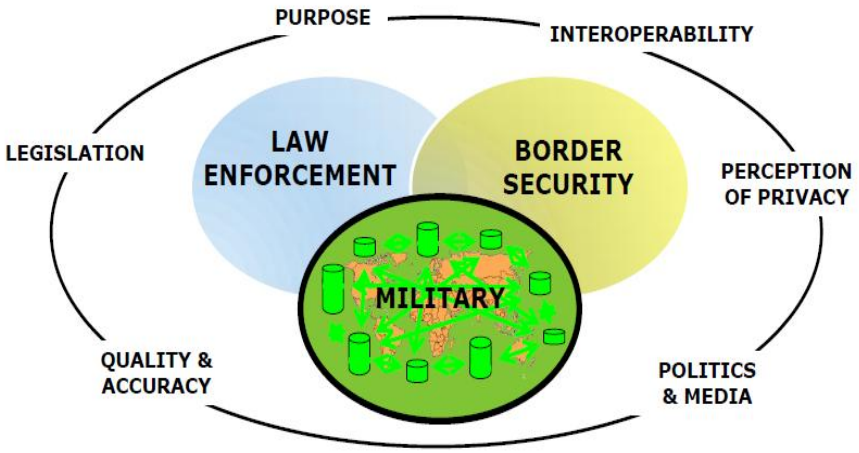


Figura 2.8 Maximizarea eficienței capabilității biometrice; limitări și oportunități de colaborare (Wulfse, 2013)

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 ar 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 MAJIIC Again*, în 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 şi un grad sporit de complexitate, capacitatea de adaptare devine critică. Din perspectivă organizaţională adaptabilitatea poate fi ca "abilitatea de a schimba ceva sau pe cineva pentru a se potrivi unei schimbări în curs" (Andresen şi Gronau, 2005), astfel putându-se aprecia că transformarea continuă reprezintă soluţia adaptării cu succes la un mediu schimbător. Cu toate acestea în cazul structurilor organizaţionale mari, mai ales al celor care şi-au dovedit eficienţa la un moment dat în timp, transformarea nu numai că poate intra în conflict cu inerenta interţie organizaţională, dar poate reprezenta şi o serioasă sursă de risc. O soluţie viabilă pentru depăşirea şi minimalizarea riscurilor generate de transformare o constituie determinarea şi înţelegerea trendurilor şi în consecinţă identificarea noilor caracteristici de mediu generate de acestea.

Cel mai important element de luat în considerare când discutăm despre necesitatea de transformare a capabilităţilor Organizatiei Tratatului Atlanticului de Nord (NATO) se referă la principalele caracteristici ale mediului de securitate în care aceste capabilităţi sunt destinate să opereze. În consecinţă atât NATO cât şi alte organizaţii internaţionale (IO) cu responsabilităţi în domeniul securităţii sunt preocupate de determinarea principalelor trenduri şi caracteristici ale mediului de securitate viitor, precum şi de impactul pe care acestea l-ar putea avea rolului de furnizor de securitate pe care aceste organizaţii îl au în principal.

O serie de studii eleborate de Comandamentul Aliat pentru Transformare (ACT)[1] alături de cele elaborate de OSCE, Comisia Europeană, Consiliul Naţional pentru Informaţii al S.U.A. şi alte organizaţii reliefează modificarea mediului de securitate la începutul secolului prezent, ceea ce generează o serie nouă de provocări şi ameninţări globale. Anumiţi factori cauzali prezentaţi de toate aceste studii nu numai că au un potenţial ridicat de a defini trendurile globale – motiv pentru care o parte au fost prezentaţi în Noul Concept Strategic al NATO adoptat de summit-ul de la Lisabona din 2010 – dar prezintă şi o relevanţă deosebită din perspectiva înţelegerii dinamicii mediului uman, după cum urmează:

- *Competiţia ideologiilor şi a perspectivelor geopolitice.* Acest aspect se referă la dezacordul, ostilitatea şi confruntarea generate de diferenţele culturale, religioase şi de valori sau a perspectivelor geopolitice diferite ale actorilor internaţionali. Modificarea situaţiei de securitate globale generează transferul de la certitudinea confruntării între superputeri spre incertitudinea interacţiunilor complexe dintre actorii statali şi non-statali.
- *Alocarea resurselor naturale*. Majoritatea studiilor care abordează acest subiect subliniază ca esenţiale aspectele referitoare la disponibilitatea, accesibilitatea, preţul şi competiţia pentru aceste resurse. Cu toate că se estimează că acestea vor continua să fie disponibile în cantităţi suficiente pentru a susţine atât creşterea populaţiei cât şi a economiei globale, nivelul de acces şi distibuţia acestor resurse vor fi inegale, manifestându-se prin anumite lipsuri la nivel local şi regional, ce pot provoca instabilitate socială şi dezacorduri între state, generând astfel surse de conflict.[2] Competiţia pentru resursele precum apa sau hrana este puţin probabil că va genera conflicte interstatale, însă ne putem aştepta la dispute interne sau inter-

[1] *The Multiple Futures Project* (MFP) (2009) şi *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-şi securiza accesul la aceste resurse vitale.[1]

- *Globalizarea*. Acest aspect se referă la nivelul de integrare funcţională şi al schimburilor comerciale ale economiilor naţionale şi regionale, iar toate documentele de referinţă, inclusiv cele militare[2], 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 ecuaţia integrării economice, modificând echilibrul de forţe la nivel global de la hegemonie la pluralism naţional. Datorită tendinţei de consolidare a poziţiei unor actori internaţionali în detrimentul celorlalţi generând tensiuni între identităţile naţionale şi cele de grup, globalizarea este legată în mod direct de competiţia perspectivelor geopolitice. Cu toate că în general globalizarea contribuie la o dezvoltare constantă a intereselor econmice comune între şi dintre state, nu s-ar putea afirma că ea reprezintă soluţia certă împotriva rivalităţilor şi suspiciunilor internaţionale.[3]
- *Complexitatea, impredictibilitatea şi incertitudinea.* Globalizarea, competiţia pentru resurse, competiţia ideologică şi tensiunile dintre structurile politice şi sociale combinate cu diferendele culturale, religioase şi ideologice pot genera alte aspecte cu impact deosebit asupra mediului de securitate, respectiv complexitatea, impredictibilitatea şi incertitudinea. Marea majoritate a studiilor menţionate subliniază faptul că mediul de securitate viitor va fi dominat de complexitate şi impredictibilitate, aspecte ce vor constitui o adevărată provocare la adresa solidarităţii aliaţilor, având în vedere faptul că unitatea de valori, partajarea sarcinilor şi anagjamentul faţă de deciziile comune reprezintă elementele cheie ale unei alianţe. Implicaţiile derivate din scenariile "viitorurilor multiple" sugerează că mediul de securitate va suferi o modificare continuă generată de evoluţii în domeniile politic, social, tehnologic şi militar ce nu pot fi prevăzute cu certitudine în prezent.
- *Factorul demografic*. Trendurile sociale şi demografice actuale vor avea un impact semnificativ asupra evoluţiei mediului de securitate amplificând potenţialul apariţiei şi intensitatea conflictelor intrastatale generate de actori non-statali.[4] Creşterea populaţiei globale poate avea efecte sociale semnificative cum ar fi extinderea urbanizării, adâncirea faliilor dintre clasele sociale, sărăcie, şomaj şi migraţie; toate acestea putând reprezenta surse de conflict. Diferenţele demografice semnificative dintre tările dezvoltate şi cele în curs de dezvoltare vor continua astfel că în timp ce statele dezvoltate se vor confrunta cu fenomenul de îmbătrânire şi scădere a populaţiei cele în curs de dezvoltare vor avea o populaţie din ce în ce mai tânără în continuă creştere, ce ar putea crea o serie de probleme majore din punctul de vedere al securităţii în situaţia în care această creştere nu este corelată cu nivelul de dezvoltare economică. Trendurile tehnologice, culturale şi economice au potenţialul de a alimenta tendinţele de negare a comunităţilor şi instituţiilor tradiţionale, mai ales în statele dezvoltate, iar pe măsură ce fracturarea societăţii

[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 Operaţii de Informaţii (noiembrie 2009) şi 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 ţări însăşi existenţa statului naţional poate fi pusă la îndoială.[1]

- *Tehnologia şi inovaţia.* Utilizarea tehnologiei a devenit un factor din ce în ce mai important al mediului de securitate şi se referă la ritmul exponenţial de creştere a inovaţiei tehnologice, evoluţia continuă a diferitelor tehnologii, precum şi gradul de diseminare şi nivelul de accesibilitate al acestora, ce conferă o marjă de acţiune tot mai largă atât pentru actorii non-statali cât şi pentru simplii indivizi. Proliferarea armelor de distrugere în masă, a armamentului pe bază de laser, a mijloacelor de război electronic, a nano- şi bio-tehnologiilor, precum şi a tehnologiilor spaţiale va avea un impact major asupra mediului de securitate.[2] Dependenţa tot mai mare a infrastructurilor critice de sistemele de reţele informatice corelată cu nivelul de accesibilitate a celor mai noi tehnologii în domeniu determină ca ameninţările informatice, respectiv securitatea cibernetică să devină probleme de interes major din punct de vedere al securităţii.
- *Aspectele privind mediul înconjurător.* Modificările climatice trebuie privite prin prisma efectelor semnificative pe termen lung cu impact asupra relaţiilor internaţionale deoarece aspecte precum criza tot mai pronunţată a resurselor de apă potabilă şi cererile tot mai mari de resurse energetice vor avea un impact tot mai pronunţat asupra mediului de securitate în zonele de interes ale NATO. Raportul din 2013 al Forumului Economic Mondial subliniază importanţa înţelegerii schimbărilor din domeniul energetic şi cele ale altor resurse naturale avertizând că aceste aspecte nu trebuie examinate doar din perspective cantitative şi de distribuţie 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 şi tensiunilor sociale, exacerbând şi mai mult potenţialul de instabilitate deja existent.

Caracteristicile operaţiilor viitoare ale NATO. Importanţa dimensiunii umane în conflictele militare

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

- *Mediul operaţional complex* reprezentat de anagajarea simultană a forţelor armate în întreg spectrul operaţional – aerian, terestru, maritim, cosmic şi cibernetic – în operaţii cu un ritm din ce în ce mai ridicat, în care mijloacele non-cinetice vor avea un rol tot mai important;
- *Operaţii multinaţionale întrunite cu caracter expediţionar*, care implică dezvoltarea unor capabilităţi expediţionare solide din partea NATO având în vedere că zonele de instabilitate cu risc major de conflict se află în afara teritoriului Alianţei;
- *Creşterea probabilităţii confruntării cu ameninţările hibride*[4], deoarece ameninţările 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 ameninţări de securitate generate de adversari ce au capabilitatea de a recurge adaptiv atât la mijloace convenţionale cât şi neconvenţionale pentru a-şi realiza obiectivele, după cum stipulează input-urile comandamentelor strategice cu privire la noul concept NATO privind contribuţia militară la contracararea ameninţărilor hibride. Principala caracteristică a acestui tip de ameninţări o reprezintă executarea unor combinaţii de acţiuni – convenţionale şi neconvenţionale – îndreptate împotriva unor obiective atât militare cât şi

hibridă caracterizată prin angajarea unor capabilităţi convenţionale, neregulate şi infracţionale integrate operaţional şi tactic până la cel mai mic nivel posibil, desfăşurate în special în mediul urban sau în acele zone în care Alianţa nu dispune de un sprijin adecvat;

- Confruntarea cu *adversari neconvenţionali dispersaţi* este o consecinţă directă a provocării generate de ameninţările hibride şi reprezintă o importantă schimbare de paradigmă de la conceptul tradiţional al confruntării între super-puteri unde inamicul este identificat ca actor statal spre interacţiuni cu grad de complexitate sporit între actori statali şi non-statali. Deoarece NATO şi-a demonstrat capabilitatea de a desfăşura operaţii convenţionale rapide şi eficiente, statele cu care se confruntă vor recurge tot mai mult la sprijinirea şi exploatarea unor subsituienţi (cum ar fi elemente teroriste sau infracţionale) capabili să genereze provocări şi ameninţări asimetrice, care să le permită să contracareze eficient interesele, obiectivele şi acţiunile Alianţei fără a se angaja în acţiuni directe, astfel că rolul acestui tip de adversari va deveni tot mai important în operaţiile militare viitoare;
- *Urbanizarea confruntării armate* este generată de trendurile de creştere demografică din ţările în curs de dezvoltare ce prevăd că până în anul 2025 mai mult de 60% din populaţia lumii va trăi în oraşe. Din perspectivă militară mediul urban ridică o serie de probleme deosebite datorită caracteristicilor specifice şi cerinţelor şi limitărilor pe care le impune: efective numeroase pentru desfăşurarea acţiunilor militare; limitări severe ale eficienţei puterii de foc; executarea manevrei într-un mediu de confruntare multidimensional; precum şi prezenţa în număr ridicat a populaţiei civile;
- *Populaţia – centru de greutate al operaţiilor* deoarece în viitor zonele de operaţii se vor suprapune tot mai mult cu zone dens locuite şi în consecinţă populaţia va deveni un element cheie al mediului operaţional, astfel că a câştiga sprijinul acesteia va reprezenta cerinţa de bază pentru obţinerea succesului;
- *Comprehensivitatea* este generată de experienţa operaţiilor recente care au demonstrat că forţele armate nu dispun de capabilităţile necesare pentru a gestiona exclusiv într-o manieră eficientă provocările generate de complexitatea operaţiilor de stabilitate şi reconstrucţie astfel că abordarea multidisciplinară şi intensificarea cooperarii interagenţii în cadrul acestui tip de operaţii devin imperios necesare.

Conflictele prezente relevă un nou tip de ameninţari asimetrice, inedite, subtile şi nedefinite, iar adversarii se amestecă şi se ascund în rândurile populaţiei locale, care în cele din urmă devine parte integrantă a mediului operaţional. În conflictele actuale ameninţările sunt disimulate în rândul populaţiei ceea ce sporeşte complexitatea şi incertitudinea operaţională prin obstrucţionarea identificării acestora, astfel că a câştiga sprijinul populaţiei devine un aspect esenţial pentru neutralizarea acestui tip de ameninţări asimetrice. Cu toate că populaţia civilă a reprezentat întotdeauna un element important al mediului operaţional, pe măsură ce adversarii mută intenţionat desfăşurarea conflictului în mijlocul acesteia, rolul populaţiei capătă o importanţă sporită, iar a-i câştiga sprijinul devine centrul de greutate al operaţiei atât pentru NATO cât şi pentru adversarii săi.

---

civile într-un mediu operaţional din ce în ce mai larg cuprinzând şi domenii imateriale, nelimitate din punct de vedere fizic cum ar fi cele financiar, cibernetic sau media. Acest tip de acţiuni sunt greu de atribuit unui anumit actor sau adversar, la fel cum este extreme de dificilă identificarea iniţiatorului lor, şi poate constitui rezultatul cooperării dintre state-sponsor, organizaţii teroriste sau infracţionale, guverne corupte sau indivizi.

Recunoaşterea importanţei aspectelor umane ca factor al confruntării armate nu este un fenomen nou, iar pe parcusrul istoriei o serie de personalităţi[1] şi instituţii[2] au fost preocupate de influenţarea acestor aspecte în sprijinul realizării obiectivelor proprii. Deşi cunoaşterea inamicului a constituit întotdeauna unul dintre principiile de bază ale confruntării militare, atât operaţiile militare cât şi decidenţii de securitate au avut adeseori de suferit datorită lipsei unei cunoaşteri aprofundate a unor culturi şi societăţi străine. Etnocentrismul, prejudecăţile şi asumările bazate pe modul de gândire propriu au avut consecinţe nefaste asupra unor conflicte militare cum ar fi ofensivele nord-vietnameze (1968 şi 1975), războiul sovieto-afgan (1979-1989), preluarea puterii de către şiiţi 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 cunoaşterea 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 operaţional actual s-a modificat fundamental în ultimii douăzeci de ani ca rezultat al globalizării şi 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 înţelegerea mediului uman şi a fi în măsură astfel să comunice mai eficient cu populaţia locală, autorităţi şi alţi actori din zona de operaţii pentru a-şi îndeplini cu succes misiunile.

Operaţiile recente din Kosovo, Afganistan şi Libia demonstrează că înţelegerea atât a mediului uman din zona de conflict cât şi a motivaţiilor populaţiei de a sprijini fie activ, fie pasiv oponenţii Alianţei sunt aspecte cheie ce trebuie luate în considerare pentru dezvoltarea capabilităţilor NATO. Lipsa cunoaşterii aspectelor umane poate avea consecinţe serioase şi nedorite, în timp ce, dimpotrivă, înţelegerea culturii adversarului poate face o diferenţiere pozitivă la toate nivelele: strategic, operativ şi tactic. (McFate, 2005, 44) Neînţelegerea aspectelor umane poate genera stabilirea unor obiective nerealiste la nivel strategic, dezvoltarea unei imagini publice negative la nivel operaţional şi punerea în pericol atât a trupelor proprii cât şi a populaţiei civile la nivel tactic. (McFate, 2005, 45)

Succesul operaţiilor viitoare va depinde de tot mai mult de integrarea în procesul de planificare militară a cunoştinţelor din domeniul ştiinţelor sociale ce au potenţialul de a facilita exploatarea la scară largă a aspectelor umane. În ciuda unor progrese moderate în ceea ce priveşte recunoaşterea importanţei acestor aspecte pentru operaţii, cum ar fi Strategia de Abordare Comprehensivă sau actualizarea procesului de planificare al operaţiilor, Alianţei nord-atlantice încă îi lipsesc programele, sistemele, modelele, personalul specializat şi structurile organizatorice adecvate pentru a putea contracara cu succes ameninţările prezente şi viitoare.

În lipsa unei surse centralizate de cunoştinţe şi analize cu privire la aspectele umane comunităţile militară şi politică, cărora aceste informaţii le sunt necesare în cea mai mare măsură, trebuie să se rezume la sursele proprii, insuficiente în cele mai multe situaţii. (McFate, 2005, 46) Cu toate acestea, dezvoltarea unor mecanisme eficiente de accesare într-o manieră oportună a cunoştinţelor şi informaţiilor, existente dispersat la diferite nivele în cadrul statelor membre, de către decidenţi şi planificatori, ar contribui la îmbunătăţirea semnificativă la nivelul NATO a gradului de înţelegere a dimensiunii umane a mediului operaţional.

[1] Sun Tzî 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 example Biroul de etnologie americană înfiinţat în timpul războaielor indiene (1865-1885) sub conducerea maiorului John Wesley Powell.

Aspectele umane ale mediului operaţional

Înţelegerea aspectelor umane ale mediului operaţional îşi are originea în sincopele cu care NATO s-a confruntat în operaţiile recente în ceea ce priveşte înţelegerea şi adaptarea la dimensiunea umană a teatrelor de operaţii în care a desfăşurat acţiuni militare. După cum rezultă din trendurile actuale şi în viitor preponderenţa operaţiilor Alianţei va consta în operaţii de răspuns la situaţii de criză non-articol 5 (NA5CRO) desfăşurate în afara teritoriului propriu, astfel că înţelegerea dimensiunii umane a mediului operaţional şi transformarea capabilităţilor acţionale în acest sens vor continua să reprezinte o prioritate pentru NATO în vederea executării cu succes a acestui tip de operaţii. Apreciem că reuşita unui astfel de demers depinde nemijlocit de identificarea unor soluţii concrete pentru sporirea cooperării şi coordonării acţiunilor Alianţei cu organizaţiile internaţionale, cu diferitele structuri guvernamentale din cadrul statelor membre, cu mediul academic şi think-tank-urile, precum şi cu diferite organizaţii neguvernamentale pe baza principiilor strategiei de abordare integrată.

În vederea realizării unei înţelegeri unitare a problematicii abordate apreciem că *aspectele umane ale mediului operaţional* reprezintă un set complex de elemente, factori, procese, interacţiuni şi percepţii dintr-o societate afectată de un nivel ridicat de violenţă ce au capacitatea nu numai de a influenţa operaţiile unor forţe armate ci chiar de a determina rezultatul final al conflictului. Aceste aspecte se referă la factorii psihologici, culturali şi sociali în relaţie cu contextul istoric, politic, instituţional, economic, militar şi legal generate de o situaţie de criză. Aspectele umane au o deosebită relevanţă pentru operaţiile de stabilitate şi reconstrucţie, de contrainsurgenţă, de menţinere/impunere a păcii, precum şi alte operaţii similare.

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

1. Motivaţia acţiunilor umane
   - Înţelegerea factorilor care generează acţiunile indivizilor contribuie la îmbunătăţirea relaţionării cu persoanele aparţinând unui civilizaţii sau culturi diferite;
   - Cunoaşterea faptului că satisfacerea nevoilor fundamentale tinde să reprezinte principala prioritate a indivizilor indiferent de cultura căreia îi aparţin vine în sprijinul inter-relaţionării culturale;
   - Observarea răspunsurilor comportamentale şi emoţionale la diferite situaţii conduce la identificarea motivaţiilor fundamentale ale acţiunilor umane;
   - Crearea unor nivele de aşteptare ridicate fără a fi şi satisfăcute generează situaţii conflictuale, chiar şi în cazul satisfacerii aşteptărilor de nivel inferior;
   - Normele morale au un rol important atât asupra manierei în care indivizii încearcă să îşi satisfacă nevoile fundamentale cât şi în ceea ce priveşte opţiunile comportamentale;
   - Observarea modului în care reţelele individuale se suprapun şi interacţionează poate revela potenţialul de cooperare sau conflict;
   - În cadrul unui grup sau al unei comunităţi indivizii au tendinţa de a recurge la acele decizii care minimalizează costurile personale şi maximizează recompensele materiale.
2. Înţelegerea mediului uman:
   - Înţelegerea acestui mediu favorizează şi managementul contactului iniţial cu o cultură diferită, dar şi procesul de adaptare la cultura respectivă;
   - Comunităţile locale reprezintă o sumă de grupuri umane cu nivele diferite de influenţă, motivate de factori naturali şi contextuali;

- Comunităţile umane trebuie analizate temporal din perspectiva dinamicii schimbării şi nu ca succesiune de imagini statice fără fundament;
- Odată cu desfăşurarea într-o anumită zonă forţele NATO devin un actor principal în cadrul respectivei comunităţi, iar succesul lor poate depinde de abilitatea de a trata cu respect opiniile membrilor acelei comunităţi, pe de o parte, iar pe de alta, de a furniza acele îmbunătăţiri ale situaţiei locale pe care comunitatea respectivă şi le doreşte;
- Înţelegerea răspunsurilor anterioare ale unei comunităţi la situaţiile conflictuale poate contribui la anticiparea reacţiilor la un nou conflict sau la o intervenţie a NATO;
- Crearea unei structuri de analiză a aspectelor umane poate furniza nivelul de cunoaştere necesar planificării în avans a potenţialelor operaţii viitoare;
- Integrarea metodelor de analiză specifice ştiinţelor umaniste şi sociale în procesul de analiză a informaţiilor asigură mijloacele necesare studierii eficiente a proceselor care determină atitudinile, credinţele şi 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 substanţial în portretizarea alianţei faţă de potenţialii interlocutori;
   - Înţelegerea modului în care populaţia locală îşi procură informaţiile şi adaptarea mesajelor la nivelul audienţei ţintă sunt elemente fundamentale ale unei comunicări eficiente;
   - "Competenţa inter-culturală" trebuie să constituie o cerinţă de bază pentru personalul militar şi civil destinat să interacţioneze cu reprezentanţii altor culturi;
   - Înţelegerea mediului cultural şi social, mai ales a sistemului social cu dinamica şi subsistemele sale specifice, este fundamentală pentru o comunicare inter-culturală constructivă.
4. Dinamica situaţiei locale:
   - Cu toate că înţelegerea acestei dinamici reprezintă o adevărată provocare, deopotrivă pentru forţele NATO dar şi pentru populaţia locală, ea este de importanţă critică pentru realizarea obiectivelor strategice ale misiunii;
   - Înţelegerea mecanismelor şi echilibrelor de putere constituie un element cheie pentru înţelegerea situaţiei locale;
   - Stabilirea unor obiective operaţionale adaptate la specificul situaţiei locale prin identificarea unui echilibru corespunzător între ceea ce se doreşte la nivel strategic, ceea ce poate fi acceptat la nivel local şi ceea ce se poate realiza de forţele desfăşurate în teren constituie cerinţa de bază pentru succesul unei operaţii;
   - Schimbările de situaţie trebuie gestionate luând în considerare faptul că şi o schimbare pozitivă generează sentimente de insecuritate, rezistenţă, teamă sau pierdere a identităţii.
5. Percepţia şi acceptarea operaţiilor NATO:
   - Legitimitatea constituie fundamentul acceptării prezenţei forţelor NATO de către populaţia locală;
   - NATO poate îşi poate îndeplini parţial obiectivele strategice fără a se angaja în acţiuni de luptă, doar prin influenţarea eficientă şi pozitivă a percepţiilor;
   - Aplicarea principiilor validate de experienţa ONU în operaţii de sprijinire a păcii poate îmbunătăţi substanţial performanţele NATO în executarea operaţiilor de stabilitate şi reconstrucţie;

- Angajamentul liderilor cheie alături de legătura şi mentoratul operaţional constituie domenii noi de acţiune în sprijinul îndeplinirii obiectivelor operaţionale;
- Strategia de informare publică şi comunicarea sunt elemente critice pentru realizarea obiectivelor la toate nivelele.

6. Determinarea atitudinilor faţă de operaţiile NATO:
   - Înţelegerea oportună a atitudinilor populaţiei faţă de acţiunile forţelor NATO poate contribui la îmbunătăţirea succesului operaţional;
   - Atitudinile sunt imput-uri deliberate ale intenţiilor şi comportamentului;
   - Pentru realizarea modificării comportamentale este necesară înţelegerea şi influenţarea convingerilor şi/sau atitudinilor individuale în direcţia dorită;
   - Analiza periodică a atitudinilor populaţiei poate veni în sprijinul procesului de planificare operaţională atât pe termen scurt cât şi pe termen lung;
   - Utilizarea mijloacelor tehnice moderne contribuie la îmbunătăţirea culegerii datelor specifice, precum şi la îmbunătăţirea analizei acestora.
7. Transformarea capabilităţilor NATO pentru a se adapta mai bine mediului uman:
   - Operaţiile recente au demonstrat că dimensiunea umană a mediului de acţiune reprezintă un element determinant al rezultatului unei operaţii militare ce impune transformarea capabilităţilor existente şi chiar dezvoltarea unor capabilităţi noi;
   - Înţelegerea aspectelor umane specifice zonei de operaţii este esenţială pentru planificarea unei operaţii reuşite;
   - Provocările generate de complexitatea mediului operaţional actual şi viitor impun dezvoltarea unui concept în acest domeniu şi implementarea aspectelor umane ca o nouă capabilitate integrată prin adaptarea modului de gândire; organizării; proceselor decizionale; tacticilor, tehnicilor şi procedurilor precum şi a programelor educaţionale şi de instruire;
   - Orice eventual program de transformare a capabilităţilor în acest domeniu trebuie să se bazeze pe principiile strategiei de abordare integrată şi să se axeze pe direcţiile de acţiune specifice Sistemului de dezvoltare a integrării a capabilităţilor întrunite[1]: DOTMLPFI (doctrină, organizare, instruire, asigurare materială, leadership, personal, facilităţi/infrastructură şi interoperabilitate);
   - Implementarea unui sistem de planificare operaţională integrată nu numai că ar permite NATO să îşi coordoneze acţiunile cu principalii actori internaţionali (organizaţii internaţionale şi neguvernamentale) încă din fazele premergătoare ale operaţiilor, dar ar facilita şi o mai bună integrare a resurselor umane şi materiale naţionale şi internaţionale, prevenind disfuncţionalităţile din interacţiunea civilo-militară;
   - Integrarea cunoştinţelor şi metodologiei specifice ştiinţelor sociale poate îmbunătăţi semnificativ maniera militară tradiţională de înţelegere a dimensiunii umane a mediului operaţional.

Premizele creării disciplinei SOCINT

Inteligența culturală este o teorie managerială și a psihologiei organizaționale care postulează fapul 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 culturali[1], 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, obieciurile, istoria, religia

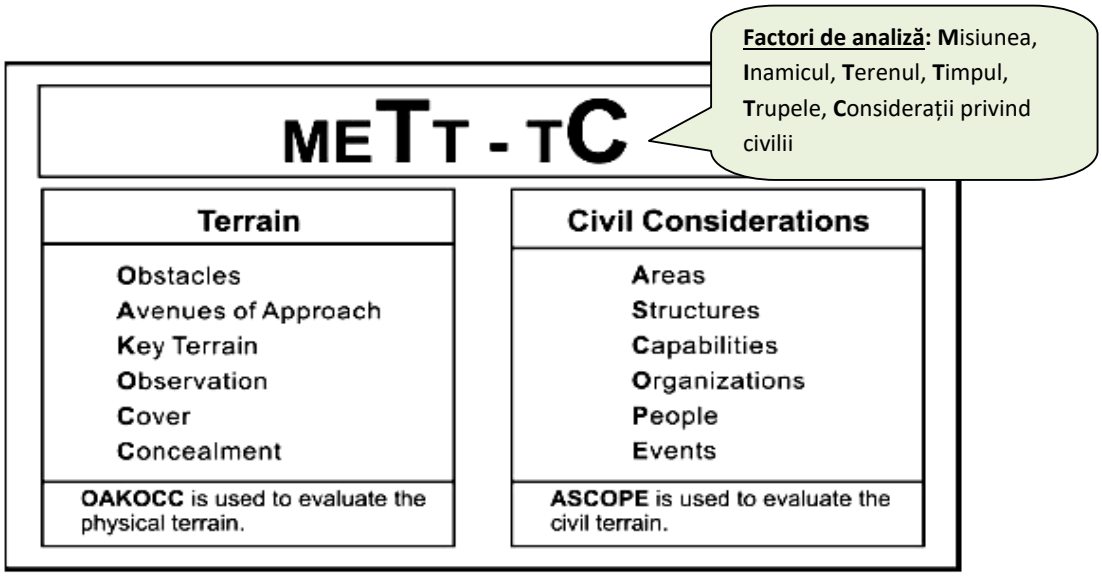


Figura 3.1 Factorii de analiză ai operației; ASCOPE – elemente de referință în formularea considerațiilor privind populația civilă *(FM 3-05.40 (FM 41-10) 2006, fig. 1-3, 1-4)*

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, Maliks, elders, Shura members, influential families	Builders, road contractors, local development councils	Media owners, mullahs, Maliks, elders, heads of families
E Events	Elections, Shurahs, Jirgas, provincial council meetings, speeches	Kinetic events, unit RIPs, 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 Intelligence[4].

Din 2012, HTS este promovat ca o capabilitate 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 capabilitate 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 capabilități (figura 3.3):

a. Capacitatea de a înțelege (capabilități de sprijin prin percepție și comprehensibilitate, în baza științelor sociale și comportamentale, a caracteristicilor și dinamicilor socioculturale în mediul operațional);
b. Detectarea (capabilități de descoperire, distingere și localizare a semnăturilor socioculturale relevante operațional prin colectarea, procesarea și analiza datelor comportamentale socioculturale);
c. Anticiparea (capabilități 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 (capabilități 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)

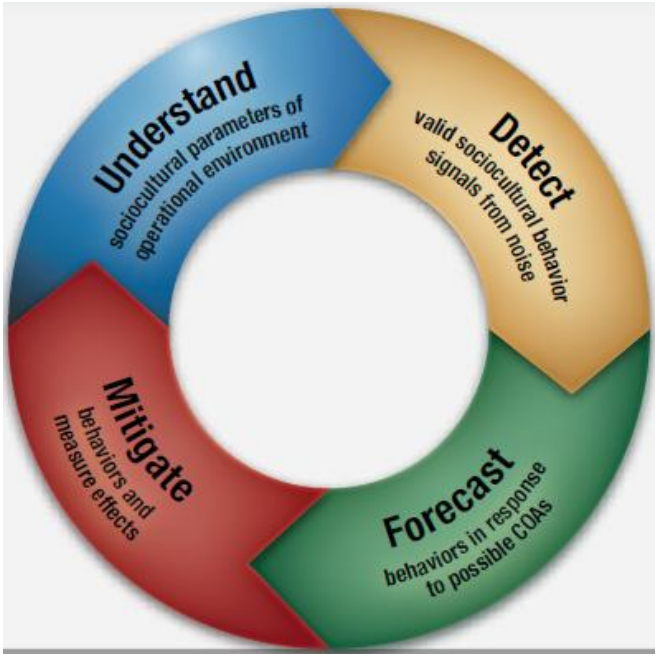


Figura 3.3 Cadrul domeniilor de capabilitate ale comportamentului sociocultural (Schmorrow, 2011)

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 umane[1] 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, sprijind 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 paradigmatice 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 specifice[2]. 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 (credințe, 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 daca 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 deosebit[1]);
- 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.

Algoritmul acțiunii socio-culturale presupune parcurgerea unor pași (identficarea 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 intreprinde 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.

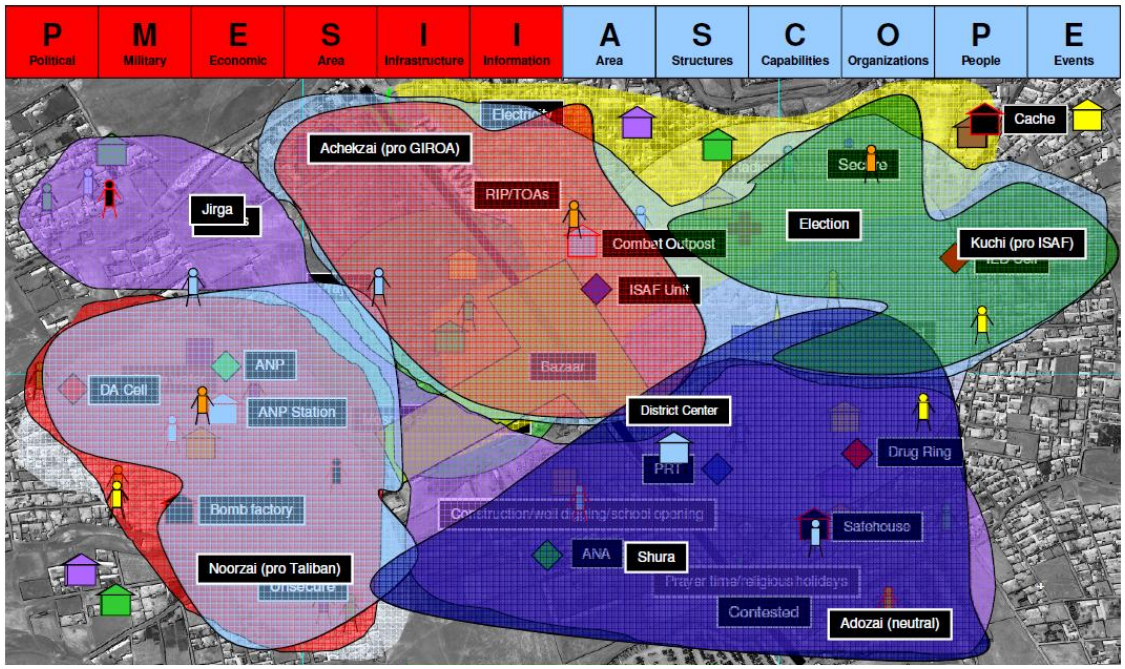


Figura 3.5 Pregătirea informațională a mediului operațional – overlay (după Doctrina contrainsurgență)

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 Combinate) 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 web[1] (figura 3.6).

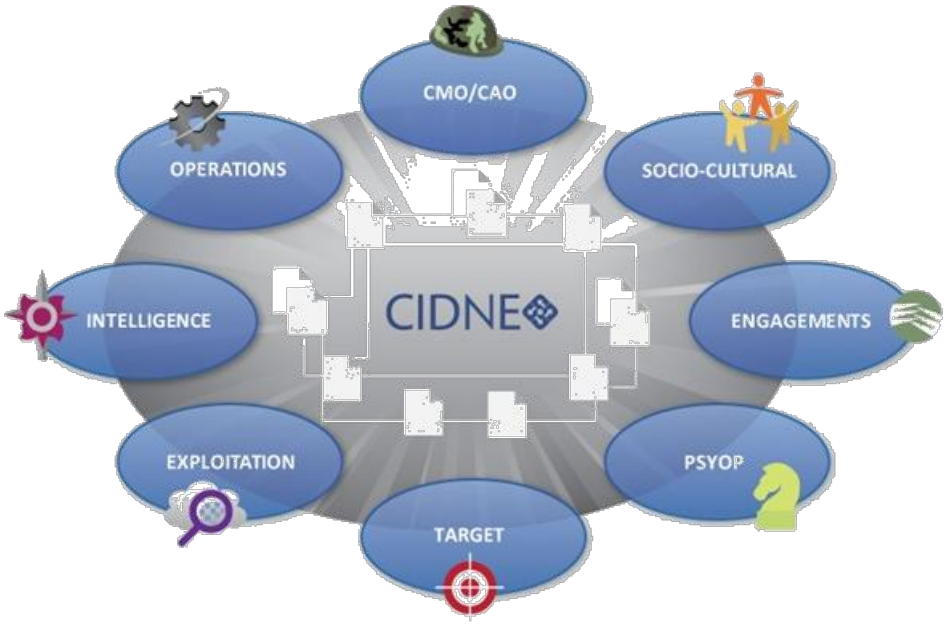


Figura 3.6 Platforma CIDNE – contributori (http://www.issinc.com/products/cidne/)

În ceea ce privește SOCINT, CIDNE asigură atât repozitorul achizițiilor senzorilor 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).

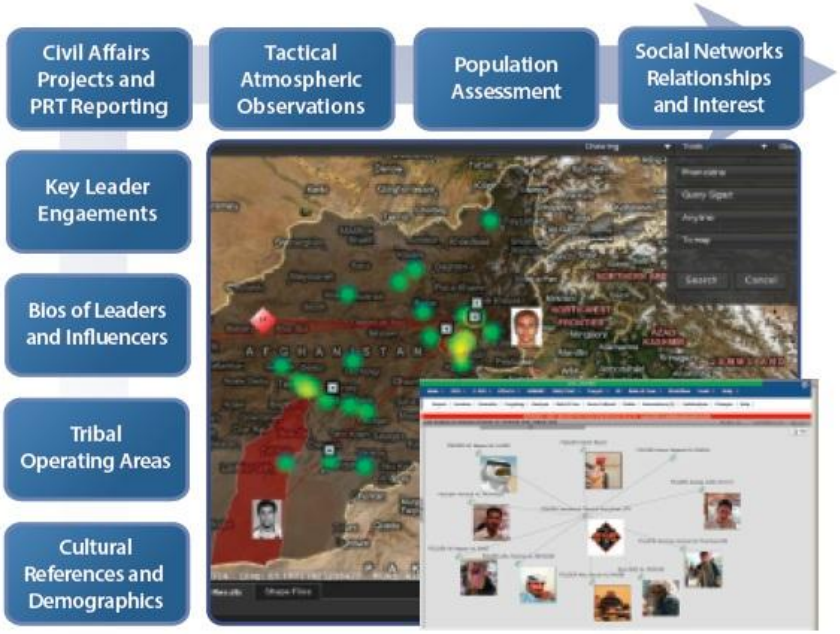


Figura 3.7 – Platforma CIDNE – vizualizarea rețelelor umane (http://www.issinc.com/products/cidne/)

[1] www.issinc.com

Concluzii

Instituţionalizarea consideraţiilor 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 capabilității 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=GetTRDoc.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*, în 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 persoaneși-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 Convenţia 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 informaţii în zona de operaţiuni a unui beligerant, cu intenţia de a le comunica părţii adverse*"[1], făcând totodată distincție față de unitățile de cercetare, încadrate cu militari în uniformă (nedeghizaţi), trimişi în recunoaştere în teritoriul inamic, în zona operaţiilor militare.

Protocolul I Adiţional la Convenţiile de la Geneva 1977[2] 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 acţionează 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 forţelor cărora le aparţine – fapt ce nu exclude urmărirea ulterioară în justiție pentru violări ale Dreptului Războiului (Johnson și alții, 2013).

În timp de conflict militar, spionii acţionează în cadrul unor misiuni acoperite sau clandestine, pentru a obţine informaţii cu caracter preponderent militar despre inamic (potenţial uman, starea moralului, dotare, amplasamente, planuri de operaţii etc.). În această situație, potrivit dreptului internaţional cutumiar şi convenţional, 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 garanţie 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 cetăţeni ai unui stat ori

[1]Convention (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

[2]Protocol 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 cetăţenie (în serviciul unui stat) care acţionează împotriva altui stat culegând date și informaţii secrete pe care le transmit agenţiilor de apartenenţă.

Avansul tehnologic fulminant din ultimele decenii, concretizat în diferite soluţii tehnice ştipuri 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 relevanţei culegerii de informaţii din surse umane. Disciplinele tehnice, GEOINT, IMINT, SIGINT, COMINT, ELINT, precum și fluxul informaţional specific societăţii bazate pe cunoaștere, ca sursă a OSINT, au prevalat ca fiind sigure din punct de vedere al protecţiei operatorilor, totodată furnizând date concrete, bazate pe suport real.

Cu toate acestea, evoluţia spectrului de ameninţări în lumea globalizată, precum și caracterul operaţiilor militare recente și actuale, au determinat ca informaţiile din surse umane (HUMINT) să revină în prim-planul interesului atât a serviciilor și agenţiilor statale din domeniul securităţii, cât și în mediul militar. Nivelul de utilizare al acestei capabilităţi 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 informaţii/ contrainformaţii în plan intern, sau serviciile de informaţii externe ale statelor, prin intermediul instituţiei atașaturii militare, dar și în mod acoperit, prin mijlocirea unor reţele de spionaj, în funcţie de interesele de securitate naţionale și opţiunile existente[1]. Riscurile rezultate din activitatea clandestină sunt deosebit de ridicate, naţiunile în cauză putând recurge la deportarea, închiderea sau chiar executarea spionilor capturaţi. În cazul imunităţilor diplomatice[2], persoanele implicate în acte de spionaj pot fi declarate ”persona non grata” și obligate să părăsească teritoriul ţării respective.

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

În cadru naţional se manifestă abordări diferenţiate în ce privește nivelul de clasificare a documentelor doctrinare referitoare la acest subiect, din raţiuni 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 HUMINT[3]) au un nivel de clasificare care nu permite accesul larg la consultarea acestora, primând principiile securităţii informaţiei (”nevoia de a cunoaște”); în schimb, manualul american FM 2-22.3, care detaliază aspecte specifice operaţiilor de colectare a informaţiilor din surse umane, este postat pe internet, fără restricţii de acces[4].

Și la nivel conceptual apar diferenţe notabile în ce privește structurile, funcţiunile și procedurile HUMINT. Școala anglo-saxonă de Intelligence include în spectrul HUMINT operaţiile cu sursele, întâlnirile cu persoanele oficiale, interogarea persoanelor reţinute,

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

[2]Decretul nr. 566/1968 pentru ratificarea Convenţiei cu privire la relaţiile 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%2FJurisdictie%2F2a.doc&ei=Wy4NU91dw73KA_OJgtAD&usg=AFQjCNEALWJhM17xAXPT34Mcp-VnYOcKag

[3]documentul este in curs de revizuire, sub noua denumire de ”Proceduri, tehnici si tactici HUMINT in NATO”

[4]FM 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 intervievarea civililor sau a propriului personal, în anumite circumstanțe (Beall, 2009).Doctrina franceză înglobează în HUMINT (în limba franceză ROHUM – renseignement d'originehumaine) 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 capabilității 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 cuprinde[1]:

- 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 capabilități. 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;
- Aparate 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
[2] FM 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 definitorii, 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).

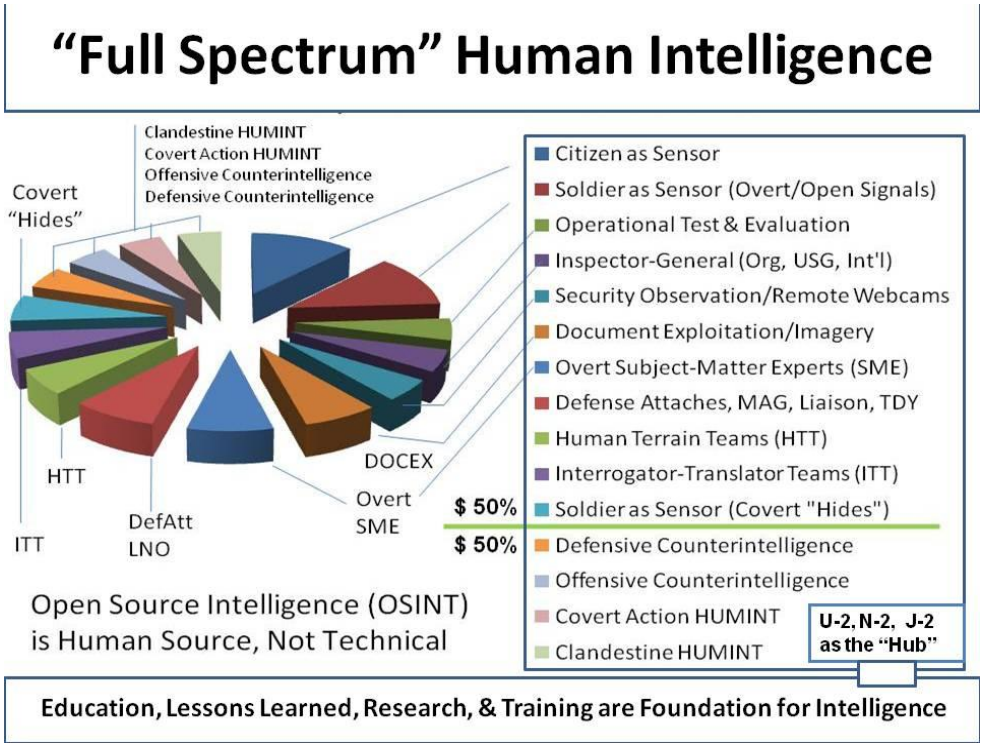


Figura 4.1 HUMINT într-o abordare comprehensivă (Steele, 2010)

Cadrul larg al dezvoltării capabilității HUMINT în NATO

Adaptarea Alianței la mediul de securitate este un process 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 2010[1] exprimă viziunea Alianţei și definește prioritățile sale în materie de securitate, identificând tipurile de operații ce fundamentează parametrii de dezvoltare a capabilităților militare ale Alianței[2] - proces reconfirmat la Summitul NATO din 2012 la Chicago[3].

[1] http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf
[2] Procesul de planificare a apărării în NATO se bazează pe Directiva Politică emisă în 2011, în vederea atingerii obiectivelor stabilite prin noul Concept Startegic
[3] http://www.nato.int/cps/en/natolive/official_texts_87593.htm?mode=pressrelease

Apărarea colectivă, managementul crizelor şi 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 (JISR[1]), 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 acţiunea coerentă a diferite tipuri de senzori de culegere a informaţiilor şi capacităţi de prelucrare şi diseminare a acestora, în toate domeniile acţionale.

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 acurateţea 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 imagerie 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

[1]Joint 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 SHAPE[1] 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 disicipline.

În cadrul fundamentării capabilității 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 informații[2], 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 aș menționa aici modul în care structurile HUMINT

[1] Supreme Headquarters Allied Powers Europe – statul major al Comandamentului Aliat pentru Operații
[2] Proiectul ”*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 capabilității 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 cunoștiințelor 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 colectivă[1], 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 aferentsunt 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).

[1]HCOE este gazda anuală a exercițiului NATO HUMINT ”Steadfast Indicator”

[2]HCOE 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 criterii de eficiență funcțională și răspunzând nevoilor de îmbunătățire a tuturor aspectelor definitorii.

O scurtă analiză SWOT[1] 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 pârghiile 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 curiculară 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 reperele curiculare 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.

[1]Strengths, 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 comonalitatea 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 reliefarea reperelor de suport în procesul de dezvoltare a capabilității 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 capabilități 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.

Relevanţa aspectelor umane ale mediului operaţional pentru HUMINT

Însăşi definiţia HUMINT ca şi *"capabilitate de culegere, procesare şi diseminare a informaţiilor din surse umane"* relevă nu doar conexiunea dintre structurile HUMINT şi dimensiunea umană a mediului operaţional, ci, mai mult, necesitatea imperioasă pentru o foarte bună înţelegere a mediului de acţiune – populaţia din zona de operaţii – ca premisă fundamentală pentru îndeplinirea cu succes a misiunilor specifice.

Astfel, o reflectare mai accentuată a aspectelor umane ale mediului operaţional în procesul de pregătire al structurilor HUMINT constând în aprofundarea înţelegerii impactului pe care factorii psihologici, culturali şi sociali în relaţie cu contextul istoric, politic, instituţional, economic, militar şi legal generate de o situaţie de criză îl au asupra desfăşurării operaţiilor militare ar avea ca o primă consecinţă îmbunătăţirea nivelului de competenţă inter-culturală al operatorilor – interfaţa structurilor de informaţii militare cu populaţia locală. Acest aspect s-ar concretiza în perfecţionarea capacităţii de comunicare şi relaţionare a operatorilor cu grupurile ţintă, conferindu-le astfel abilităţi sporite de dezvoltare a raporturilor interpersonale.

O altă îmbunătăţire generată de o mai bună cunoaştere a aspectelor umane s-ar manifesta în domeiul pregătirii premergătoare dislocării în teatrul de operaţii printr-o înţelegere aprofundată a particularităţilor specifice zonei respective de operaţii, mai ales în ceea ce priveşte caracteristicile populaţiei locale. În legătură cu aceast aspect trebuie menţionat faptul că una dintre concluziile pregnante rezultate din participarea personalului HCOE la activităţile de instruire a forţelor NATO organizate de Centrul de instrucţie a

forţelor întrunite[1] de la *Bydgoszcz*, Polonia, o reprezintă observaţia cvasi-generală a participanţilor de diferite naţionalităţi că nivelul de familiarizare culturală asigurat prin diferite forme de instruire – naţionale şi/sau multinaţionale – este insuficient în raport cu cerinţele impuse de realitatea din teatrele de operaţii. Ameliorarea calitativă şi cantitativă a pregătirii pe această linie contribuie semnificativ la familiarizarea corespunzătoare a personalului cu zona în care urmează să acţioneze; consecinţele directe ale acestui fapt concretizându-se atât în diminuarea efectelor şocului cultural cât şi în reducerea perioadei de adaptare la specificul zonei de operaţii şi creşterea eficienţei acţionale.

Din perspectivă acţională valorificarea cunoaşterii aspectelor umane ale mediului operaţional se poate concretiza prin creşterea nivelului de înţelegere a cererilor de informaţii pe această linie – a căror pondere este estimat a se amplifica direct proporţional cu importanţa tot mai crescută pe care comandamentele strategice şi operaţionale o acordă înţelegerii comprehensive a mediului operaţional – de către structurile HUMINT în vederea planificării, organizării, pregătirii şi executării misiunilor specifice de culegere, precum şi a analizei acestei categorii de informaţii.

Analiza operaţiilor recente desfăşurate de Alianţa 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, ştiinţific, cultural) şi implicit necesitatea dezvoltării capacităţii epistemologice a sistemului militar pentru a putea genera capabilităţi adecvate complexităţii unui mediu operaţional comprehensiv specific operaţiilor multinaţionale întrunite actuale.

Concluzii

Dezvoltarea capabilității 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 capabilității HUMINT nu este unul ușor; determinarea obiectivelor pe termen scurt, mediu și lung, a liniilor directoare, 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 suple, 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 capabilității, 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/rr/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, Marinel-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. POUCET, Emmanuel (2006) *Le renseignement de source humaine, espoirs et problemes*, în revista "Doctrine" N° 09
14. SIMION, Eduard (oordinator) (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 informaţionale 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 esenţiale pentru completarea şi îmbogăţirea cunoaşterii 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.

Funcţia analitică a OSINT (Intelligence din surse deschise/ Open Source Intelligence) este interpretabilă pe două paliere de referință: pe de o parte, susţinerea documentării necesare componentei operaţionale (Intelligence de bază), pe de altă parte dezvoltarea analizelor strategice referitoare la tendinţele de evoluţie a unor riscuri sau ameninţări pe termen mediu şi lung la adresa intereselor şi valorilor fundamentale ale statului şi societăţii.

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 raţiuni:

- ca punct de plecare al unei informări, când aduc un plus de valoare unei problematici 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 şi a întregi unele date/informații;
- pentru a valida informații din alte surse;
- pentru a adăuga criterii de ierarhizare a cunoaşterii;
- 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 uşor şi au un cost relativ redus în comparaţie cu cel necesar pentru obţinerea de informaţii 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, conferinţe, întâlniri internaţionale, organizaţii 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 desconspira 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 relevanți[1]:

[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 disiciplină de culegere a informațiilor[2].

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, exploatate și diseminate în timp oportun audienței adecvate, în scopul adresării unor cerințe specifice de Intelligence sau a unor cerințe de informare.

Schaurer și Störger observă necesitatea accesării în mod legal a informației public accesibile (Schaurer 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 elicita 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

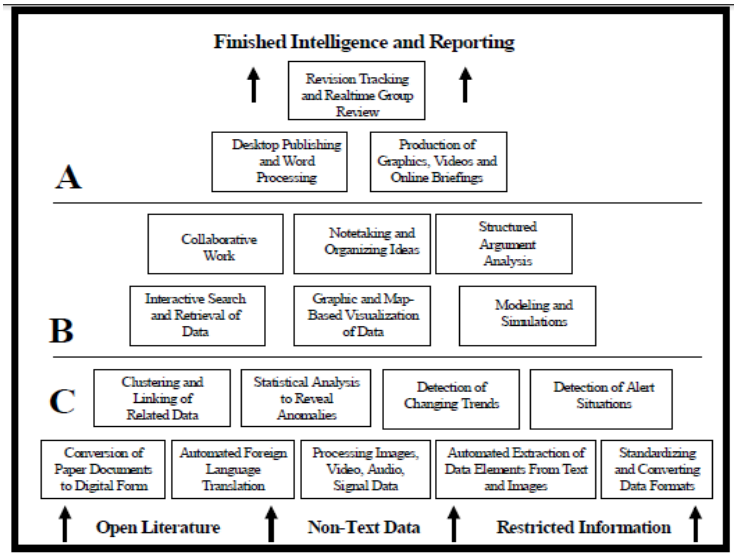


Figura 5.1 Elemente de software în ciclul OSINT (NATO Open Source Intelligence Handbook, 2001, fig. 6)

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

Informaţiile 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 (excepţie cele protejate de drepturi de copyright), nu sunt clasificate şi sunt obţinute pe căi legale. Din punct de vedere al modalităţilor 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 refolosire și redistribuire a acestora, precum și participarea neîngrădită la aceste resurse[1] - 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**” înțeleasă ca ”**surse** (*de informare*) **deschise** (*accesibile publicului*)” poate creea o serie de confunzii prin asocierea cu expresia ”**open source**” consacrată în comunitatea informaticienilor, unde se traduce prin programe a căror cod-sursă este public disponibil și modificabil[1]. 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 atribuitabile 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 şi afilierea participanţilor[1]; invocarea acestei clauze marchează trecerea de la informația publică din sursă deschisă la date din surse confidențiale).

În funcţie de suportul de difuzare, conţinut şi modul de diseminare, sursele deschise pot fi clasificate în două categorii:

C. clasice:

- *publicaţii periodice* (ziare şi reviste), agenţii de ştiri, cărţi (de specialitate, de telefoane, „Pagini aurii", monitorul oficial, anuare), materiale documentare (broşuri şi studii), hărţi şi fotografii;
- *literatura gri* – totalitatea materialelor care nu sunt disponibile prin intermediul canalelor tradiţionale (mass-media) de publicare, distribuţie sau control biografic. Sursele de literatură gri pot fi ONG-urile, instituţiile de învăţământ şi cercetare, companii comerciale, agenţii guvernamentale, mediul academic[2], asociaţii formale şi informale, cluburi etc. În această categorie se încadrează: documentare ştiinţifice şi tehnice, rapoarte guvernamentale, bugete, statistici demografice, audieri, dezbateri legislative, conferinţe de presă, discursuri, dar şi informaţiile din medii profesionale şi academice: conferinţe, simpozioane, documente elaborate de asociaţii profesionale, lucrări academice şi ale experţilor din diverse domenii. Principalele dificultăţi întâmpinate în exploatarea literaturii gri ține de faptul că este dificil de identificat şi procurat (nefiind la îndemâna publicului larg); intrarea în posesia literaturii gri este posibilă numai pe timpul unor evenimente, despre care culegătorul trebuie să aibă cunoştinţă şi 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 apariţiei etc.
- *transmisiile audio-video în eter* (radio şi televiziune).

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

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

Rolul Internetului şi *new media* în obţinerea OSINT

Din 1994, Internetul – o complexă rețea de rețele[3] – a luat amploare în lume, având un impact uimitor asupra tuturor aspectelor vieții. Internetul şi creşterea exponențială a numărului persoanelor cu acces la acesta aproape oriunde în lume, apariţia forumurilor de discuţii pe diferite subiecte, a reţelelor 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 responsabilităţii de către un editor şi circulată în afara circuitelor comerciale (ex. preprinturile, care conţin lucrări de cercetare, rapoarte tehnice etc., puse în circulaţie mai ales în spaţiile academice, pentru a face cunoscute ultimele noutăţi, ultimele gânduri, ultimele realizări, în beneficiul comunităţii ştiinţifice, 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 şi tehnologii de culegere, analiză şi diseminare a informaţiei la nivel global.

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

Deşi nu există o definiţie 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 şi distribuit prin reţele informatice sau totalitatea textelor, sunetelor, imaginilor şi elementelor grafice prelucrate pe computer şi 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 customizate 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 exemple[1]:

- **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 socializare[2]

Numărul imens de website-uri corporate/ personale, bloguri, forumuri publice, popularitatea fără precedent a reţelelor sociale (sute de milioane de conturi), dar şi creşterea exponenţială a conţinutului generat de utilizatori şi diversitatea limbilor şi a pachetelor în care este livrată informaţia 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 reacţie şi o încercare de adaptare la dinamica mediului online, fiind direct influenţate de noile tehnologii şi de rapiditatea cu care sunt preluate şi dezvoltate de utilizatori.

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

Dificultăţile întâmpinate în procesul de identificare şi validare a surselor sunt generate de caracteristicile Internetului şi facilităţile oferite de acest mediu, respectiv anonimatul relativ al utilizatorilor şi transmiterea virală a unor informaţii ce pot fi relevante.

Validarea poate îmbrăca două forme: verificarea informaţiei şi validarea sursei. Verificarea credibilității informației vehiculate în mediul online trebuie să aibă în vedere[1]:

- 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 informaţiilor prin transmiterea/ preluarea concomitentă a acestora pe diverse reţele de bloguri, forumuri, site-uri de ştiri şi 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 şi informaţiilor din mediul on-line necesară filtrarea conţinutului pentru a elimina informaţiile care se repetă; permisivitatea acestui mediu în privinţa preluării conţinutului, duce de multe ori la copierea şi postarea informațiilor fără menţionarea autorului, sau sub o formă modificată. În acest sens, se impune verificarea tuturor surselor de referinţă oferite, şi compararea materialelor pentru a identifica asemănările/ diferenţele 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 acoperă[2]:

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/)

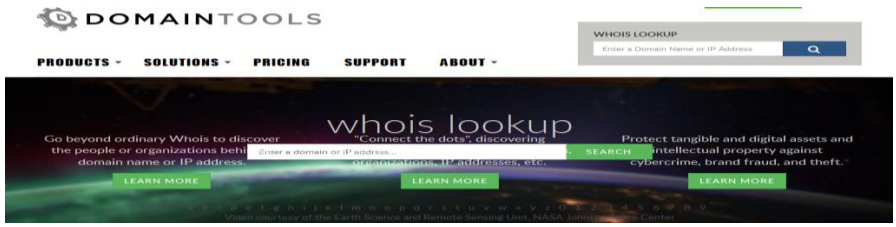


Figura 5.5 Pagina de căutare a aplicației WHOIS LOOKUP DOMAINTOOLS (http://whois.domaintools.com/)

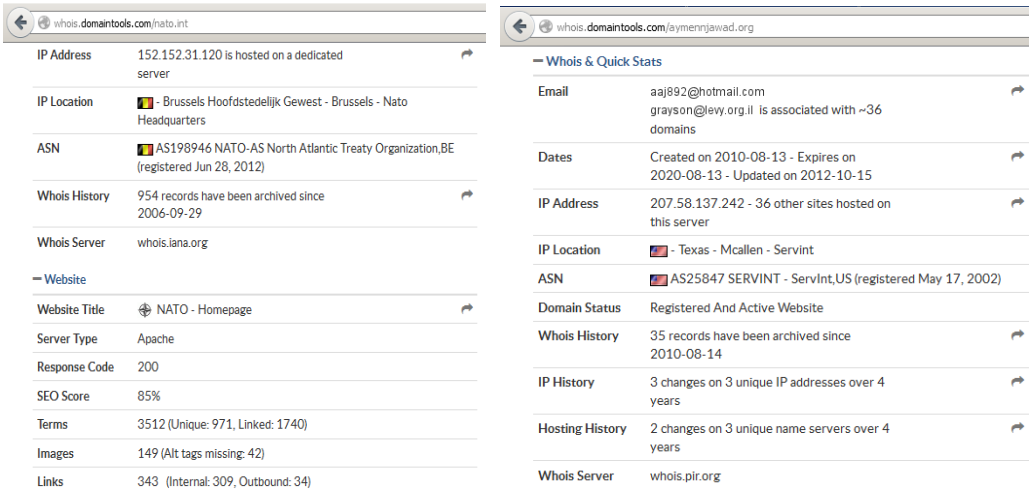


Figura 5.6 Date privind identitatea blogurilor, obținute prin aplicația WHOIS LOOKUP DOMAINTOOLS pentru blogurile de referință

[1] Blogul este un jurnal deschis publicului, publicat on-line, care oferă informaţii, 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 Explorer[1]); 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)

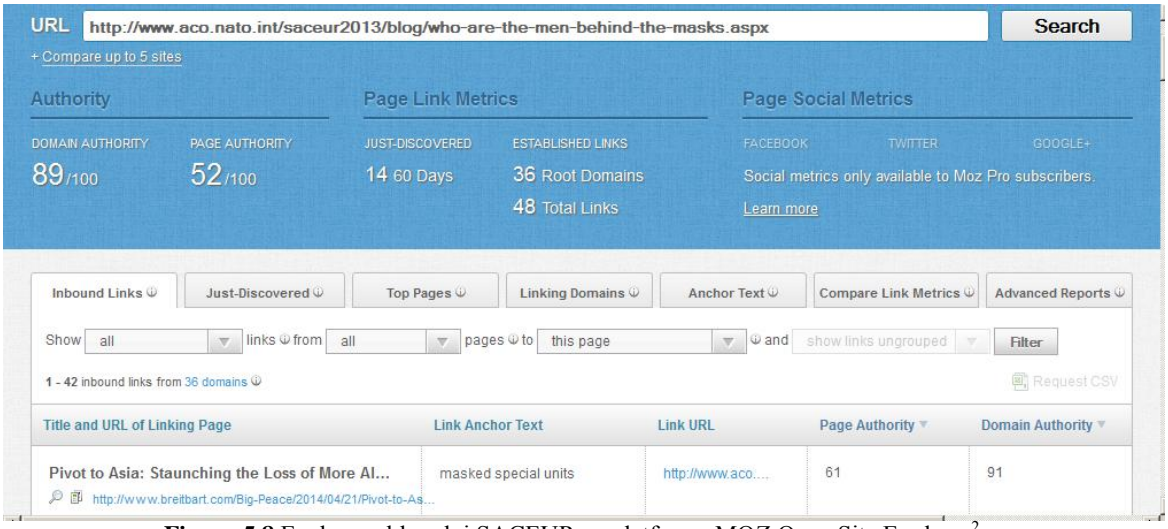


Figura 5.8 Evaluarea blogului SACEUR pe platforma MOZ Open Site Explorer[2]

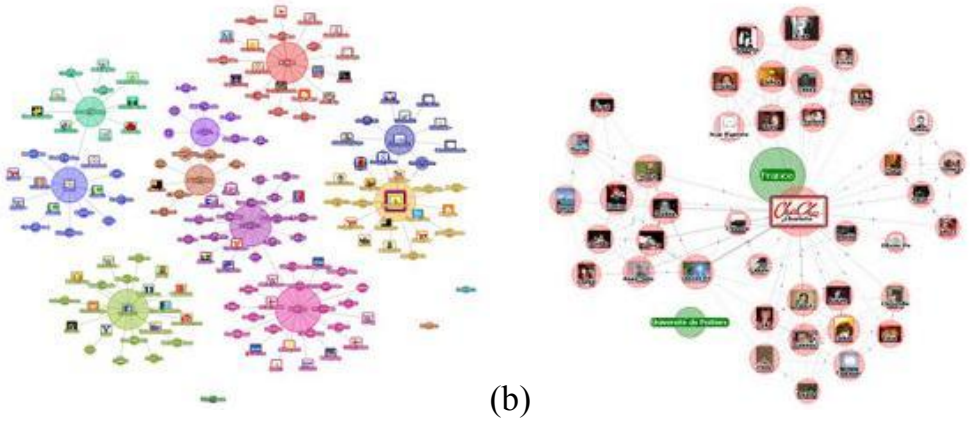
	http://www.aco.nato.int/saceur2013/blog/who-are-the-men-behind-the-masks.aspx	www.aymennjawad.org/blog/
Page Authority:	52	18
Page MozRank:	3.56	2.75
Page MozTrust:	5.03	4.86
Internal Equity-Passing Links:	1	2
External Equity-Passing Links:	45	0
Total Internal Links:	1	2
Total External Links:	47	0
Total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

[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 Navigator[2] - figura 5.10);



(a) (b)

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 Facebook[3]

d. etapa următoare privește modalitatea practică de sondare a gradului de recunoaștere a unui blog în cadrul comunității sale (contabilizarea trimiterilor/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.

Parcurgerea 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 necesare[4]. În mod specific, caracteristicile claselor rezultate în urma evaluării sunt definite de criterii de valoare ce se raportează la modalitatea de manifestare în spațiul virtual[5].

Pe de altă parte, conţinutul generat de utilizatorii reţelelor sociale presupune o monitorizare constantă a site-urilor de acest tip, precum şi interacţionarea cu aceştia pentru a fi acceptaţi/ invitaţi în grupurile personale. Similar, aplicaţiile de tip „Second life" (lumi virtuale) şi „Team Speak" (folosit pentru comunicarea online între membrii unei echipe de *gammeri*) oferă un mediu de relaţionare extrem de eficient şi 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 condiţiile "avalanşei

---

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 guidline 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

informaţionale". Arhitectura analist – server, distribuită după cerinţele informaţionale tot mai multe, reprezintă soluţia care răspunde cel mai bine nevoilor de prelucrare, analiză, producţie şi diseminare a informaţiilor.

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 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 deschise[2].

La nivelul Uniunii Europene (UE) putem menționa eforturile Centrului Întrunit de Cercetare al Comisiei UE (Joint Research Centre – JRC[3]), care prin instrumente ca: European Media Monitor (EMM) și OSINT Suite[4] 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 alerte[1]

Eforturile în cadrul NATO de a stabili cadrul general al capabilității 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 2002[1] 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 sprijinte 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 faptice, 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 (Schaurer 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 Canada[2].

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 militare[3].

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, informaţiile obţinute 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 obţinute 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 firmelor[1], 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 contractate[2]) 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 acestea[3]).

Accesul legal la baze de date se face ori făcând apel la repozitoare publice, ori prin intermediul a diferite companii specializate în constituirea și gestionarea acestora în interes comercial (precum Lexis-Nexis[4], D&B[5] 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 necunoscuți[6] sau baze de date ce listează persoane date în urmărire[7]. Mai mult, bibiotecile universităţilor 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 acestă 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 personal[2] și protecția vieții private în sectorul comunicațiilor electronice[3] 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 lege[4].

Concluzii

În actualul context geopolitic, potenţialul de valorificare şi capacitatea surselor deschise de a răspunde pe toate palierele de informare şi cunoaştere la nevoile beneficiarilor reliefează importanţa OSINT, care se dezvoltă odată cu evoluţia tehnologică şi a instrumentelor ce pot fi utilizate pentru a gestiona mijloacele de cunoaştere. Într-o societate a cunoaşterii în continuă transformare şi într-un mediu de securitate fluid şi dinamic, marcate de inovaţiile 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 guvernanțe 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 protecţie a datelor cu caracter personal reprezintă dreptul persoanei fizice de a-i fi apărate acele caracteristici care conduc la identificarea sa şi obligaţia corelativă a statului de a adopta măsuri adecvate pentru a asigura o protecţie eficientă. Prin date cu caracter personal se înţeleg acele informaţii 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, situaţia 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 si 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

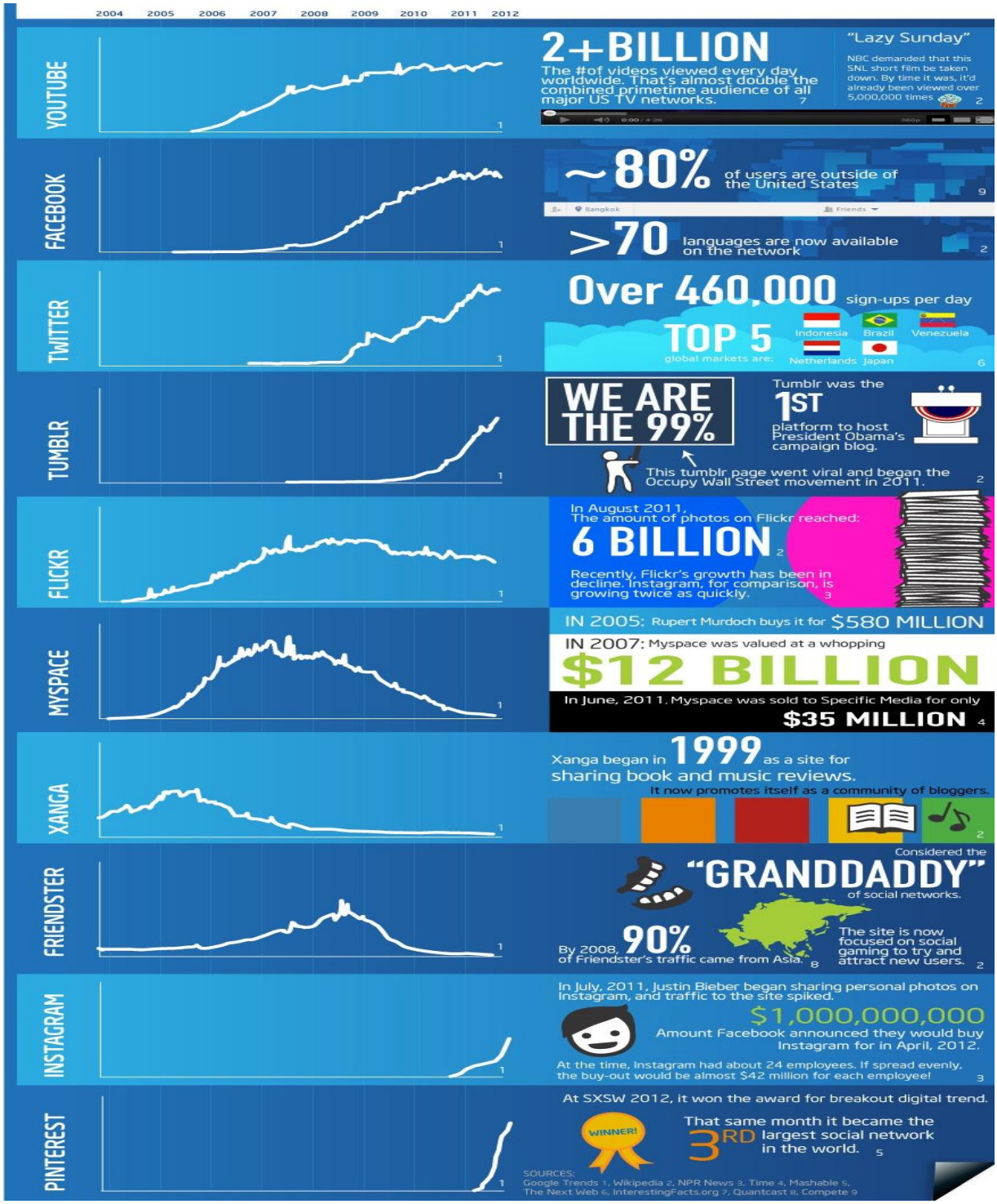
1. ***, *Aspecte privind etica profesională în lucrul cu informațiile din surse deschise*, în https://www.sri.ro/fisiere/studii/ETICA_SI_INTELLIGENCE.pdf
2. AHLQVIST, Toni, BACK, Asta, HALONEN, Minna, HEINONEN, Sirkka (2008) *Social Media Roadmaps*. *Exploring the futures triggered by social media*, 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%20OSINT%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 guidline 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 ştiinţifică*, 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 şi promovare pentru corporaţii*, 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.internetsociety.org/internet
38. http://www.lexisnexis.com
39. http://www.listafirme.ro/
40. http://www.media.utah.edu
41. http://www.mhhe.com/mayfieldpub/webtutor/judging.htm
42. http://www.namus.gov/;
43. http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%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 INFORMAŢIILOR ÎN CONTEXTUL GLOBALIZĂRII

Cerințe ale analizei de Intelligence în lumea globalizată

Activitatea de analiză a informaţiilor, etapă esenţială a ciclului Intelligence, este puternic solicitată ca urmare a schimbărilor pe care mediul de securitate le înregistrează, asociate cu reformularea priorităţilor în materie de cereri de Intelligence ale factorilor decizionali, în toate domeniile de interes. Sectoarele de referinţă exclusive îşi lărgesc în permanenţă aria de acoperire şi se întrepătrund, solicitând activitatea conjugată a unei largi palete de senzori/ operatori pentru a culege date şi informaţii din diferite medii, precum şi 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 greșeală strategică costisitoare, cu efecte asupra unui mare număr de națiuni[1].

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

- *dimensiunea militară,* carese referă la interacţiunea dintre capabilităţile armate ale statelor cu percepţiile statelor vizavi de intenţiile celorlalte;
- *dimensiunea politică,*careanalizează stabilitatea organizaţională a statelor, a sistemelor de guvernare şi a ideologiilor ce le conferă legitimitate;
- *dimensiunea economică,* ceinclude accesul la resurse şi la pieţele necesare menţinerii bunăstării şi puterii statului respectiv;
- *dimensiunea socială,*constând în sustenabilitatea identitară;
- *dimensiunea de mediu,*concentrată asupra biosferei ca sistem de suport al existenţei umane.

La rândul ei, doctrina britanică recunoaște ca și corespondente planurilor fizic, virtual și cognitiv ale abordărilor de Intelligence reprezentarea planurilor multiple definitorii 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** şi nu în prezicerea acestuia (Frățilă, 2008).

[1]Efectele 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

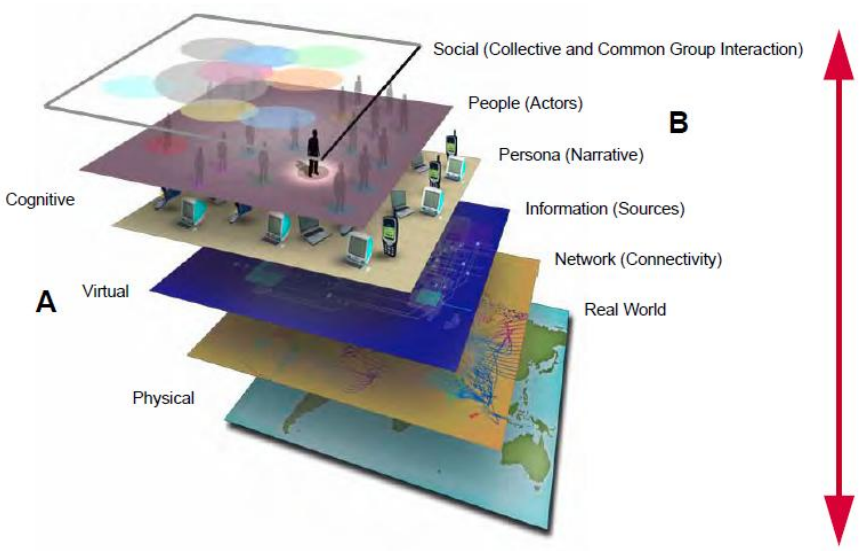


Figura 6.1 Domeniul informațional și câmpurile de analiză[1]

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

- oportunităţilor de a promova interesele statului prin mijloace diplomatice, militare şi economice, diplomaţie publică şi prin acţiuni acoperite;
- vulnerabilităţilor strategice şi tactice ale liderilor, partidelor şi grupărilor şi mişcărilor ostile statului;
- factorilor care pot fi influenţaţi;
- rezultatului probabil al cursului de acţiune adoptat;
- evaluarea punctelor forte şi 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 Naţională a Informaţiilor pentru Securitate (2004) stabilește o serie de principii în baza cărora activitatea de informaţii se desfășoară într-un stat de drept:

a. principiul legalităţii;
b. caracterul planificat şi sistematic al activităţii de informaţii;
c. ofensivitatea şi mobilitatea activităţii de informaţii;
d. anticiparea şi previzionarea;
e. obiectivitatea evaluărilor;
f. informarea exactă, corectă şi oportună a factorilor de decizie;
g. independenţa, neutralitatea şi echidistanţa 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

[1]The Development, Concepts and Doctrine Centre, UK Ministry of Defence, Joint Doctrine Publication 04 (JDP 04) (2010) *Understanding*, ShrivenhamSwindon, 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, cooperarea[1], conlucrarea[2] și colaborarea[3] intra și inter-instituțională, pe plan național sau internațional, este o cerință esențială.

Totodată, procesul analitic trebuie să asigure obiectivitatea[4] 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 internaţionale, 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 problematică 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 analiştii trebuie să le aibă în vedere menţionăm: (Frățilă, 2008, 165-166)

- căutarea sistematică a informaţiilor în toate sursele deschise şi exploatarea lor în toate tipurile de produse analitice;
- folosirea instrumentelor analitice ca sprijin şi nu ca suplinitor al efortului analitic;
- ne-discriminarea surselor (unele mai privilegiate decât altele) sau a metodelor analitice (analiştii trebuie să utilizeze, în mod constant, o gamă variată de instrumente, metode şi tehnici şi nici una dintre acestea nu trebuie privită ca excepţională 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 tradiţional - inductive bazate pe evidenţe;
- utilizarea mai largă a testelor de diagnoză a evidenţelor, ce permit îmbunătăţirea abilității de a confirma sau nega ipoteze;
- recursul la colaborare ca rutină şi nu excepţie; etc.

În baza acestor considerente, procesul de analiză cuprinde următoarele etape[1]:

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 tehnici[2].
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 disparate, 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 sensibile[1]. La nivelul analiștilor, judecata implică

[1]The 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

[2]tehnicile 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 informaţiile disponibile şi reprezintă principala modalitate de a îndepărta incertitudinea. Prin natura sa, judecata asigură ciclicitatea procesului de dezvoltare a cunoaşterii, permiţând tranziţia de la cunoscut la necunoscut şi din nou la cunoscut.

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

Logica situaţională, la rândul ei, implică generarea de ipoteze bazate pe elementele concrete ale situaţiei reale – progresiv, pe măsura cunoaşterii lor – limitată la un scenariu specific studiat în evoluţia sa temporală.

Teoria aplicată, o altă metodă de abordare analitică, se bazează pe aplicarea la realitate a modelelor desprinse din generalizări sugerate de experienţa acumulată, permiţând depistarea gradului de importanţă (semnificaţia) tendinţelor în cadrul evenimentelor studiate.

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

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

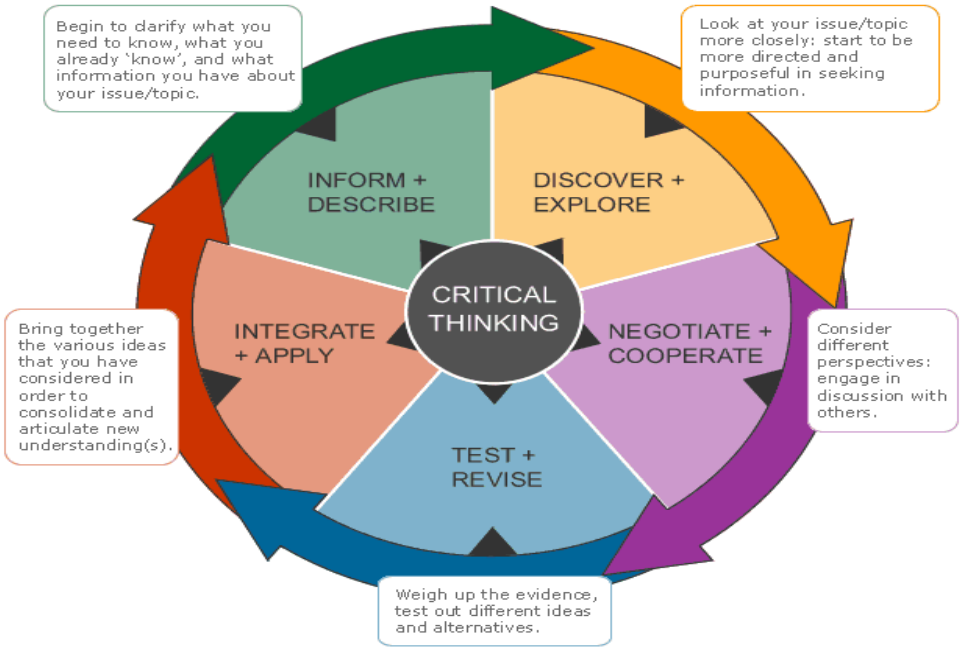


Figura 6.2 Procesul gândirii critice[2]

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 provin[1], 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 interese[2]).
- **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 asumpții 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:
    - **preconcepția proporționalității**, ce privește asumarea importanței date anumitor aspecte similare în culturi diferite;
    - **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

Secţiunea 7 - *Intelligence, Supraveghere şi Cercetare în cadrul Corpului Maritim* (Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise/MCISRE) a Conceptelor și programelor USMC pentru 2013[3] este subliniat faptul că procesul de analiză predictivă este esențial pentru proiecția forței expediționare.

---

[1] o 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”

[2] inabilitatea 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).

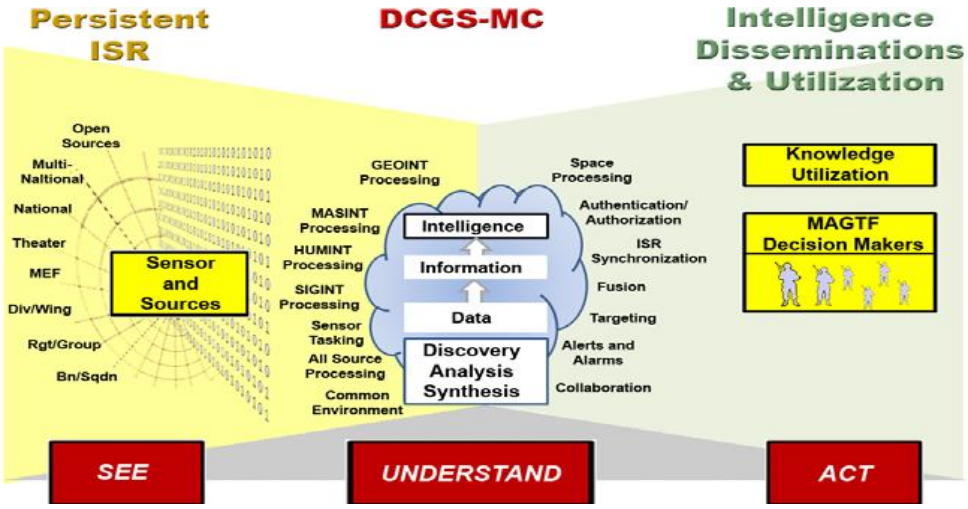


Figura 6.3 Rolul Intelligence în sprijinul operațiilor la nivel tactic[1]

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

1. **operațiile de succes reclamă o capabilitatea 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 şi Tehnici Structurate) ca spectru funcțional (procese 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 (SOCINT[3]) 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]Documentulfolosește conceptual de *Social Science Intelligence (SSI)/ Intelligence din ȘtiințeSociale*pentru a desemnaprodusele informative rezultate din analizaspecificădomeniilor de interes ale științelorsociale

importanță majoră și în cadrul operațiilor militare convenționale; SOCINT permite depășirea barierelor subiectivității în analiza factorului uman în folosirii baza unor proceduri și instrumente științifice consacrate în cadrul științelor sociale, toate acestea contribuind la mai buna 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 capabilităților 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 exponente 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 capabilitatea 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 Explozive 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 raportele 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, capabilitățile, 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 utilităţii produselor analitice, acestea trebuie să asigure înţelegerea materialului prezentat - cerinţă ce reclamă din partea analistului o bună cunoaştere a mecanismelor psihologice ale cognitivităţii umane[1].

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

- *insight* (înţelegerea cauzalităţii evenimentelor);
- *foresight* (identificarea-anticiparea cursurilor de acţiune 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.

IBMi2Intelligence Analysis Platform reprezintă o interfață analitică extensibilă, scalabilă, orientată spre serviciu, destinată furnizării organizațiilor beneficiare accesul la produse de Intelligence în conformitate cu nevoile acestora[2]. 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 rețelelorumane (prin colectarea, colarea și consolidarea datelor din multiple surse), în scopul asigurării vizualizăriişi 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*

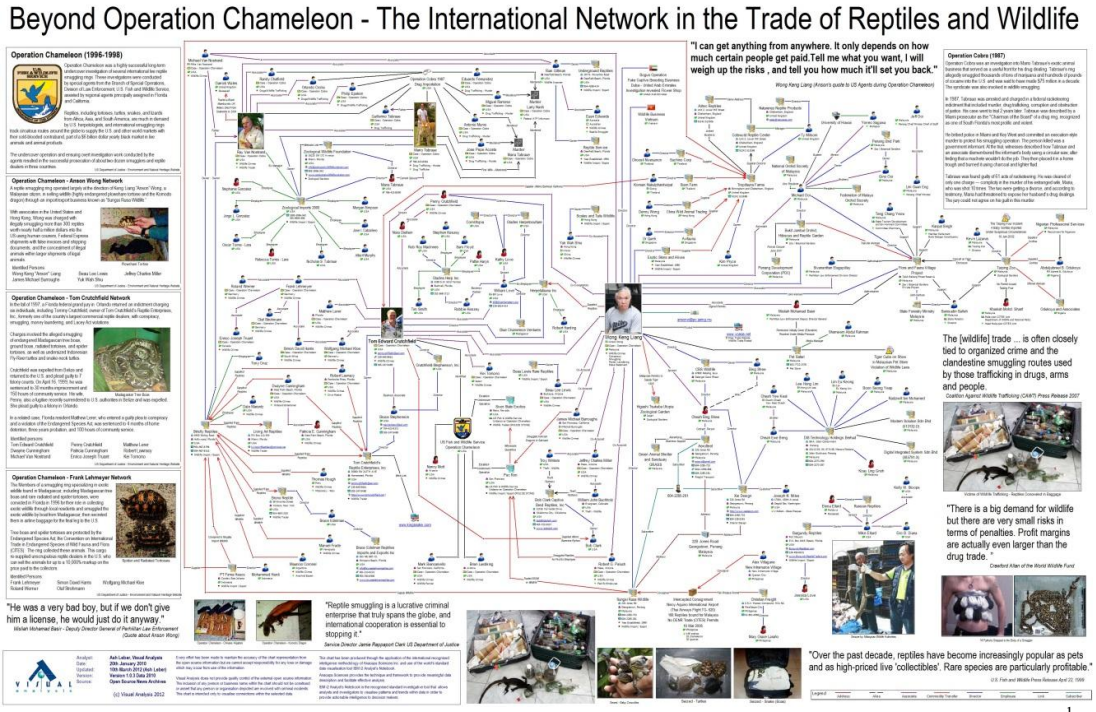


Figura 6.4 Diagramă i2 folosită în operația Cameleonul (demascarea unei rețele de traficanți de reptile)[1]

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.

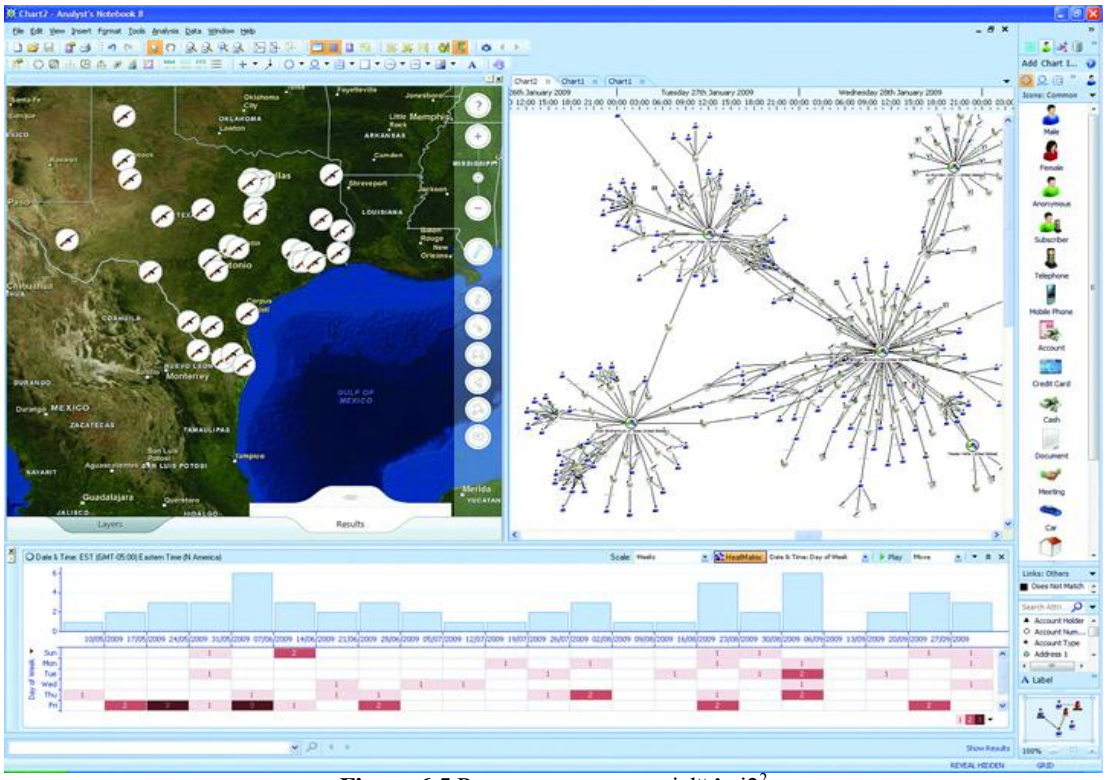


Figura 6.5 Reprezentare geospațială în i2[2]

[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 prindiagrame, hărți, tabele, fotografii, etc. Cerința de asigurare a colaborării cu alte sisteme este la rândul ei îndeplinită prin capabilitățile de interconectare securizată pe care programul le permite.

Concluzii

La nivel organizaţional, adaptarea la schimbările dictate de realitate nu este un proces natural, care survine de la sine. Schimbarea (transformarea) capabilității este un proces care trebuie bine gândit şi planificat, evaluat şi corectat în permanenţă (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 naţională a informaţiilor pentru securitate* (2004) Editura S.R.I. Bucureşti, 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 şi regional*, p. 97-107, în MOŞTOFLEI, Constantin (coordonator), Surse de instabilitate la nivel global şi regional. Implicaţii pentru România, A IV-a Sesiune anuală de comunicări ştiinţifice, Editura Universităţii Naţionale de Apărare, Bucureşti
4. BUZAN, Barry (2000) *Popoarele, statele şi teama. O agendă pentru studii de securitate internaţională în epoca de după Războiul Rece*, Editura Cartier, Chişinău
5. FRĂŢILĂ, Ovidiu Ilie (2008) *Capacitatea de adaptare a analizei de „Intelligence" - factor determinant în condiţiile evoluţiei actuale a mediului de securitate*, în MOŞTOFLEI, Constantin (coord.) (2008) Politici şi strategii în gestionarea conflictualităţii, Editura Universităţii Naţionale 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. NIŢU, Ionel (coordonator) (2011) *Ghidul analistului de intelligence: compendiu pentru analiştii debutanţi*, Editura Academiei Naţionale de Informaţii „Mihai Viteazul", Bucureşti
11. PÂRLOG, Adriean (2008) *Procesul de analiză de „intelligence", componentă a sistemului de securitate*, în MOŞTOFLEI, Constantin (coord.) (2008) Politici şi strategii în gestionarea conflictualităţii, Editura Universităţii Naţionale de Apărare „Carol I"
12. SARCINSCHI, Alexandra (2005) *Elemente noi în studiul securităţii naţionale şi internaţionale*, Editura Universităţii Naţionale de Apărare, Bucureşti, în http://cssas.unap.ro/ro/pdf_studii/elemente_noi_in_studiul_securitatii_nationale.pdf
13. ŞERBAN, Mihai (2008) *Unele aspecte referitoare la importanţa analizei în mediul intelligence*, în MOŞTOFLEI, Constantin (coord.) (2008) Politici şi strategii în gestionarea conflictualităţii, Editura Universităţii Naţionale 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 şi securitate* (note de curs), Iași

16. US Marine Corps, *Concepts and programs 2013*, America"s Expeditionary Force in Readiness, în 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 finaciară/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 capabilităților de prevenire, protecție și evoluție a proceselor subsumate acestora.

Sub imperiul globalizării, apărarea şi securitatea au încetat să mai fie apanajul construcţiei exclusive a statelor, indiferent de puterea şi de disponibilităţile 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 revoluţie în afacerile militare/ zona serviciilor de securitate, care nu este doar tehnologică şi informaţională, ci şi una de natură filozofică şi managerială, care presupune noi scopuri şi obiective politice pentru acţiunea militară sau civil-militară (abordarea comprehensivă), noi concepte strategice, operative, tactice precum şi 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 serviciispecifice (consultanță, avertizarea timpurie, logistica, protecția forței, Intelligence, etc.).

Apariția acestor capabilități 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 operaţiilor militare: planificarea şi instruirea trupelor, operaţiuni armate, culegerea de informaţii, interogarea deţinuţilor, analiza de Intelligence, servicii de protecţia forţei, etc (Klein, 2008).

Influențele în abordarea laturii lucrative a securității se regăsesc în ambele sensuri, atunci când facem o comparație între nivelurile de capabilități 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 funcţionar 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 birocrației 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 intreprinderi 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 customizate, 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 Expo[1], Expoziţia şi Conferinţa pe tema Forţelor din Operaţiunile Speciale – SOFEX/Special Operations Forces Exhibition and Conference[2], etc.). Conexiunile pe care liderii acestor firme le au la nivel guvernamental sau în cadrul sectorului formal de securitate (de unde majoritatea provin[3]) 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 prelucare, 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.counterterrorexpo.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 recunoaşteri, 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 responsabilității[2]; 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 intreprind și complianța angajaților cu coduri etice stricte, care să elimine posibilitatea oricărui abuz la adresa drepturilor omului[3]. 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 mercenar[4]:

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

[2] a se vedeascandalulBlackwaterînIrak (Scahill, 2009)

[3] Un rol important în coordonarea activităţilor de lobby la nivel internaţional pentru implicarea firmelor militare private în acţiuni de menţinere a păcii, îl are asociaţia comercială a acestor firme, I.P.O.A. (Asociaţia Internaţională pentru Operaţiuni de Pace). I.P.O.A. se prezintă ca o organizaţie alcătuită din „cele mai profesioniste companii”, care își desfășoară activitatea în baza unui cod de comportament redactat „cu ajutorul a zeci de organizaţii internaţionale şi non-guvernamentale, avocaţi ai drepturilor omului şi oameni de ştiinţă” şi care acţionează în „industria de pace şi 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 private[2], a treia întrunire a acestuia fiind programată în iulie 2014[3]. Draftul Convenției limitează atribuțiile și responsabilitățilr 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 atributabil 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, furnizînd 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 Intelligence[5]:

- 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 SUA[6]. 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/
[6] http://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 insituții (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 șiASI 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 – Hakluyt[1] și Pelorus[2]. 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 Group[3] 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 Services[4] 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 clienților[2] 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 International[3] 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 Kroll[4] 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 Terrogence[5] 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 exploatării 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 lahttp://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 şimetodologice politicilor naţionale, 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/
[2] Subscriși online sau contractanți ai serviciilor de consultanță
[3] http://www.smithbrandon.com/
[4] www.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 cheie[1]:

- 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);
- capabilități 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 şi sistematizată şi analiza informaţiilor provenind din zonele de criză în scopul:

a) anticipării escaladării unui conflict violent,
b) dezvoltării de răspunsuri strategice la crizele respective şi
c) prezentării opţiunilor 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 şi Colectarea de Informaţii – ORCI la ONU, inițiativele UNOCHA – Biroul Naţiunilor 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 BMZ[3], 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 Swisspeace[4]);
- sistemele de generaţia a treia, cu sediul în zona de conflict, unde se desfăşoară atât monitorizarea cât şi analiza; activitatea de colectare a datelor implică societatea civilă şi administraţia regională şi au legături cu mecanisme instituţionale de răspuns (ex.

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

[2] R. 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 şi Cooperare (1997); Raportul final al Comisiei Carnegie pentru Prevenirea Conflictelor Mortale (1997); Raportul Brahimi (2000); Declaraţia de la Khartoum la nivel sub-regional a şefilor 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).

[3] BundesministeriumfürwirtschaftlicheZusammenarbeit (Ministerul FederalpentruCooperareEconomică)

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

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

cărora 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 Fragilităţii 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 aș 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 regulatoare și metodologiile de lucru (Blitt, 2005).

Intelligence în competiția economică (*Competitive Intelligence*)

Dezvoltarea unui mediu de afaceri concurenţial şi 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 neexploatate ale clienţilor, 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 competitțional, 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*, cunoștiințele în materie fiind ulterior dezvoltate de CraigFleisher[2], Babette Bensoussan[3], Leonard Fuld[4] 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 Europa[5].

Crearea în 1986 a Societății Profesioniștilor în Intelligence Competițional, devenită ulterior asociația Profesioniștilor în Intelligence Strategic și Competițional (The Strategic and Competitive Intelligence Professionals - SCIP[6]), 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 capabilitățile, vulnerabilitățile și intențiile competitorilor în afaceri, reprezintând 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 domeniu[7], recunsocută de SCIP.

Activitatea de Intelligence competitțional 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 industriale[8].

Spionajul indistrial/ 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/een/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 profesiuni;
- 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 şi a intruziunii clandestine în reţelele de date confidențiale ale firmelor, până la modalități de protecție fizică în asigurarea secretului comercial[2] 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 secundară[3].

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

[1] www.scip.org

[2] constituie secret comercial informaţia care, în totalitate sau în conexarea exactă a elementelor acesteia, nu este în general cunoscută sau nu este uşor accesibilă persoanelor din mediul care se ocupă în mod obişnuit cu acest gen de informaţie şi care dobândeşte o valoare comercială prin faptul că este secretă, iar deţinătorul a luat măsuri rezonabile, ţinând seama de circumstanţe, pentru a fi menţinută în regim de secret; protecţia secretului comercial operează atâta timp cât condiţiile enunţate anterior sunt îndeplinite (Legea nr.11 din 29 ianuarie 1991 privind combaterea concurenţei neloiale)

[3] http://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 unorfirme 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 şi psihologice ale intervenţiilor externe, disponibilitatea imediată a pârghiilor 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 tutror resorturilor ce definesc activitatea companiilor din acest sector:

- tradiția istorică a mercenariatului ca intreprindere 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 trebuiesc 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 perspective[1]), valorificarea oportunităților de practică, asigurarea resurselor necesare proceselor specifice în condițiile extinderii şi multiplicării activităţilor necesare pentru a face faţă noilor forme de manifestare a ameninţărilor 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 influenţeze capacitatea de menţinere și dezvoltare a standardelor operaţionale şi a culturii organizaţionale 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 Iinternational 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 atribuţii informative şi experţii din domeniul securității naţionale, în cadrul unor programe guvernamentale, propunând și soluții de optimizare a formării culturii de intelligence a decidenților politici prin implicarea nemijlocită a Comunității Naţionale de Informaţii (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 internaţională şi forţele 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 securităţii şi relaţiilor internaţionale în contextul globalizării*, în Coordonator: dr. Constantin MOŞTOFLEI, *Politici şi strategii în gestionarea conflictualităţii* (Sesiunea anuală de comunicări ştiinţifice cu participare internaţională a Centrului de Studii Strategice de Apărare şi Securitate, 20-21 noiembrie 2008, București - vol. 5 *Despre orizontala şi verticala securităţii*), Editura Universităţii Naţionale 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, Laurenţiu S. (2009) *Noi actori şi tendinţe pe piaţa securităţii*, în MOŞTOFLEI, Constantin (coord.), Perspective ale securităţii şi apărării în Europa, Editura Universităţii Naţionale 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 şocului: naşterea capitalismului dezastrelor*, Editura Vellant, Bucureşti
15. Legea nr.11 din 29 ianuarie 1991 privind combaterea concurenţei 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 MOŞTOFLEI, Constantin (coord.), Perspective ale securităţii şi apărării în Europa, Editura Universităţii Naţionale 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. ROSENBACH, 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 şi platforme OSINT pentru avertizare timpurie, monitorizare şi analiză*, în MOŞTOFLEI, Constantin (coord.), Perspective ale securităţii şi apărării în Europa, Editura Universităţii Naţionale de Apărare „Carol I", București
26. UNGUREANU, Adriana (2009) *Revoluţia în afacerile militare, sursă de securitate în zonele cu potenţial conflictual*, în MOŞTOFLEI, Constantin (coord.), Perspective ale securităţii şi apărării în Europa, Editura Universităţii Naţionale 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/een/Newsletter%2010.pdf
39. http://www.colectivodeabogados.org/PRIVATE-SECURITY-TRANSNATIONAL
40. http://www.controlrisks.com/
41. http://www.counterterrorexpo.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.terrogence.com/
55. http://www.un.org/documents/ga/res/44/a44r034.htm
56. https://www.boundless.com/marketing/consumer-marketing/technology-to-assist-market-research/competitive-intelligence/
57. www.kroll.com
58. www.scip.org

CAPITOLUL 8. CONTRAINFORMAŢIILE ŞI SPECTRUL AMENINŢĂRILOR LA ADRESA SECURITĂŢII

Counterintelligence/ contrainformaţii – delimitări conceptuale

Subiectul reprezentat de *counterintelligence* porneşte, în mod necesar, de la clarificarea acestei noţiuni şi a termenilor asociaţi. În acest sens, vom folosi în continuare termenul *contrainformaţii* ca traducere directă a noţiunii *counterintelligence*, abreviat ca CI.

Dicţionarul WEBSTER defineşte conceptul contrainformaţiilor ca *activitate organizată a unui serviciu de informaţii desfăşurată cu scopul de a bloca sursele de informaţii ale inamicului, de a îl induce în eroare, a preveni sabotajele şi a culege informaţii politice şi militare*.[1]

Definirea termenului ”contrainformaţii” în spaţiul noţional al limbii române este legată de noţiunea de ”contraspionaj”; astfel, DEX 98 defineşte contrainformaţia (contrainformaţii) ca *serviciu de stat însărcinat cu urmărirea şi combaterea spionajului* şi contraspionajul ca *activitate de urmărire şi de contracarare a actelor de spionaj şi de descoperire şi prindere a spionilor* (dar şi ca *serviciu special care desfăşoară activitatea de contraspionaj*).[2]

În SUA, contrainformaţiile se referă la *informaţiile colectate şi activităţile desfăşurate în vederea protejării împotriva spionajului, a altor activităţi din spectrul intelligence, a sabotajelor sau asasinatelor executate de - sau în numele unei - puteri străine, organizaţii sau persoane, ori activităţi de terorism internaţional, fără a include programe de securitate şi protecţie fizică a persoanelor, documentelor sau comunicaţiilor*.[3]

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

Raportul Comisiei Church prezentat în senatul SUA consideră contraspionajul ca parte ofensivă[4] a CI (acţiunea *ofensivă* a CI fiind detaliată într-un glosar de specialitate SUA din 2006 ca penetrare a grupurilor adverse şi inducerea în eroare a acestora[5], exclusiv orientat împotriva spionilor/ surselor umane ale acestora şi având ca scop afectarea eficienţei lor prin manipulare sau disruperea operaţiilor de spionaj[6]).

În completare, acelaşi glosar clasifică CI *defensiv* ca totalitatea acţiunilor menite să protejeze informaţiile vitale privind securitatea naţională împotriva intrării în posesia lor sau a manipulării acestora de către organizaţiile/ operaţiile 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 acţional de destructurarea reţelelor clandestine şi prevenirea (ca măsură a succesului) a atacurilor teroriste, cibernetice, etc.

Directiva Departamentului Canadian pentru Apărare Naţională distinge tot două categorii funcţionale ale disciplinei CI[1]:

- pe de o parte *contrainformaţii* (”counter-intelligence/ contre-ingérence”[2]), focalizate asupra identificării şi contracarării ameninţărilor din partea serviciilor secrete ostile, a indivizilor sau organizaţiilor ostile angajate în spectrul activităţilor TESSOC[3] la adresa personalului, proprietăţii şi informaţiei forţelor proprii;
- pe de altă parte *informaţii pentru securitate* (”security intelligence/ renseignement de sécurité”), constând în colectarea şi prelucrarea de date şi informaţii privind identitatea, capabilităţile şi intenţiile serviciilor de intelligence ostile angajate în activităţi din spectrul TESSOC (furnizând intelligence ca fază pregătitoare a CI ofensiv).

Definţia NATO dată CI face trimitere la activităţile care urmăresc identificarea şi contracararea ameninţărilor la adresa securităţii reprezentate de serviciile de informaţii, organizaţiile sau indivizii ostili angajaţi în acţiuni de spionaj, sabotaj, subversiune sau terorism (AAP-6, 2-C-16, 2014). Această definiţie introduce acronimul ”TESS” (*Terrorism, Espionage, Sabotage, Subversion*) ca indicator al domeniilor de interes din perspectiva CI în NATO, aspecte care le vom aborda ulterior.

Contrainformaţii – contraspionaj; activităţi specifice mediului militar

Serviciile de CI sunt, de regulă, distinct organizate în cadrul comunităţilor de intelligence. Structuri specializate de contrainformaţii se regăsesc la nivelul tuturor entităţilor implicate în activitatea de garantare a securităţii naţionale, în primul rând datorită expunerii acestora la activitatea de spionaj a structurilor adverse, interesate de resursele şi potenţialul de acţiune al acestora. Aceste structuri interne funcţionează atât la nivel naţional, cât şi în cadrul operaţiilor externe ale entităţilor pe care le deservesc. Exemple de servicii centrale cu atribuţiuni de contrainformaţii sunt Biroul Federal de Investigaţii (FBI) în SUA, Serviciul de Securitate (MI5) în Marea Britanie, Serviciul Federal de Securitate (FSB) al Federaţiei Ruse, iar în România – Serviciul Român de Informaţii (SRI).

CI trebuie abordate la toate nivelurile de referinţă – strategic, operaţional şi tactic. La nivel strategic-operaţional, această disciplină facilitează asigurarea protecţiei intereselor guvernamentale (de stat) – indiferent de domeniul de manifestare a acestora (influenţă politică, economie şi bunăstare, putere militară, etc.).

În NATO, instituţia ce serveşte interesele strategice de protecţie contrainformativă este Comandamentul Aliat pentru Contrainformaţii (Allied Command Counter Intelligence – ACCI), reprezentat la nivelul structurilor de comandă ale NATO, precum şi în comandamentele operaţiilor Alianţei. La nivel operaţional – tactic, atribuţiile specifice sunt coordonate de către structura de Intelligence din cadrul statului major al operaţiei, prin intermediul secţiunii cunoscută ca ”2X”, responsabilă de coordonarea HUMINT, CI[4] şi, 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 securitate[1], urmărind ca finalitate obiective de protecţia forţei.

Structurile militare naţionale beneficiază de capabilităţi CI (organice sau în sprijin) reprezentate de diferite structuri, în funcţie de eşalonul de referinţă.

În mediul militar, responsabilitatea în domeniul contrainformaţiilor se adresează atât elementelor specializate, cât şi 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 forţelor adverse şi activităţile acestora.

Acţiunile de contracarare a structurilor de Intelligence ale adversarului îmbracă diferite forme – CI fiind o funcţiune multidisciplinară şi nu un apanaj exclusiv al acţiunii agenţilor speciali (cum este de cele mai multe ori înţeleasă).

La acest nivel, acţiunile CI sunt legate de capacităţile de lovire a sistemelor tehnice de colectare a informaţiilor, pe platforme terestre şi aeriene (SIGINT, IMINT, MASINT, etc.), procedurile/ programele informatice de contracarare a spionajului cibernetic sau acţiunea forţelor şi mijloacelor special desemnate să nimicească mijloacele de cercetare/ supraveghere ale forţelor adverse.

În succesiunea etapelor şi fazelor operaţiilor militare, funcţiunile Intelligence se traduc în următoarele sarcini de bază (FM 34-60, 1995):

a. furnizarea de indicatori şi avertizări;
b. sprijinirea pregătirii informative a mediului operaţional întrunit;
c. sprijinirea producţiei de scenarii de dezvoltare situaţională;
d. sprijinirea activităţii de achiziţionare a ţintelor;
e. dezvoltarea de intelligence pentru protecţia forţei;
f. executarea de evaluări ale rezultatelor operaţiilor/ acţiunilor/ loviturilor (BDA).

În acest cadru (după manualul Armatei SUA pentru CI, FM 34-60, ediţia 1995, figura 1-1), funcţiunile CI variază în funcţie de eşalon şi de tipul operaţiei desfăşurate, cuprinzând activităţi din spectrul:

- **investigaţiilor** (privind securitatea personalului, cazuri de trădare, spionaj, subversiune, revoltă, sabotaj direcţionat de servicii străine, terorism, asasinat, dezertare, detenţie, absenţă nejustificată, violări deliberate ale politicilor de securitate, suicid sau tentativă de suicid, penetrări de natură tehnică);
- **sprijinul operaţiilor** şi **protecţia forţei** (prin operaţii speciale CI, protecţia forţei în diferite faze şi etape ale operaţiei, protecţia forţei în operaţiile cu surse, asistenţă şi consiliere, legătură, sprijin tehnic, verificări ale respectării acordurilor/ tratatelor, contracararea acţiunilor ISR inamice, simularea acţiunilor adversarului – ”*red cell*”, acţiuni de acoperire a agenţilor, etc.);
- **colectarea de date şi informaţii** (identificarea şi validarea cerinţelor, colectarea de date, debriefing şi interogare, etc.);
- **analiză, sinteză, producţie** (dezvoltarea şi gestionarea de baze de date privind forţele proprii şi ameninţările, evaluări privind vulnerabilităţile şi ameninţările, identificarea prezenţei şi acţiunilor entităţilor ISR adversare, formularea de recomandări privind contramăsurile de securitate, evaluarea contramăsurilor, etc.).

  Acestora, Manualul pentru Intelligence al Forţelor Terestre ale SUA (Army FM 2-0, Intelligence, 2010), adaugă în spectrul activităţilor specifice CI şi serviciile funcţionale şi 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 funcţionare a CI este strâns legată de procedurile de securitate existente la nivelul structurilor proprii, aplicate la nivelul securităţii personalului, a informaţiilor, securitatea fizică, securitatea operaţiilor şi a informaţiilor.

TESS – terorismul, spionajul, sabotajul şi subversiunea ca subiecte de interes pentru serviciile de contrainformaţii militare

Terorismul

Terorismul a apărut ca subiect politic la nivelul Ligii Naţiunilor din 1934, însă fără să fi întrunit până azi consensul în ce priveşte definirea unitară, comprehensivă, ancorată în principii de legalitate şi urmărind prosecuţia faptelor de terorism, în ciuda multiplelor instrumente legale sectoriale elaborate începând cu 1963 pentru amendarea şi prevenirea acestora.[1] În accepţiunea ONU, terorismul este descris ca reprezentând ”acte criminale ce intenţionează sau sunt calculate să provoace stare de teroare în cadrul publicului general, a unui grup de persoane sau la adresa persoanelor private (...) indiferent de consideraţiile 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 ameninţarea cu folosirea forţei sau a violenţei în mod ilegal împotriva indivizilor sau a proprietăţii în încercarea de a presa sau intimida guverne sau societăţi în vederea atingerii unor obiective de natură politică, religioasă sau ideologică” (AAP-6, 2-T-5, 2014)

Legat de acesta, Alianţa 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 şi a dezvoltărilor ulterioare ale fenomenului.

Interesul din perspectiva informaţiilor militare în ce priveşte terorismul se leagă atât de rolurile identificate ale apărării împotriva acestui flagel (măsurile defensive antiteroriste, managementul consecinţelor şi reducerea efectelor actelor teroriste, măsurile ofensive contrateroriste şi cooperarea militară)[3], cât şi de o funcţiune consacrată tuturor operaţiilor militare – protecţia forţei[4] – care, în contextul apărării împotriva terorismului, se confruntă cu un spectru de ameninţări mult mai nuanţat şi imprevizibil.

În funcţie de caracteristicile mediului operaţional, tipurile de ameninţări teroriste la adresa forţei şi instalaţiilor proprii (când ne adresăm mediului militar), probabilitatea de producere şi impactul acestora sunt variabile în timp şi spaţiu, solicitând eforturi deosebite la nivel de colectare a datelor şi informaţiilor relevante (indicatori şi avertizări privind ţinta, momentul acţiunii, modul de operare, efectele scontate, etc.), precum şi în palierul de analiză CI, angrenând totdată schimbul de informaţii cu alte agenţii/ structuri.

Spionajul

Este de notat faptul că logica funcţionării activităţii de spionaj se concentrează asupra accesării (directe sau prin intermediul unor interpuşi, persoane cu acces corespunzător la informaţiile de interes) a unor date şi informaţii secrete de ordin politic, militar, de securitate, tehnologic sau economic. Obiectivul final al acestei activităţi 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

influenţarea unei decizii strategice, promovarea ilegală a intereselor proprii în detrimentul celor ale statului şi ale partenerilor săi sau provocarea de agresiuni informaţionale.[1]

Serviciul britanic MI-5 defineşte spionajul în mod bivalent, ca *proces ce implică folosirea de surse umane (agenţi) sau mijloace tehnice pentru obţinerea de informaţii ce nu sunt, în mod normal, publice,* alături de *influenţarea factorilor de decizie şi a formatorilor de opinie în beneficiul intereselor unei puteri străine.*[2] Acest al doilea aspect îl reprezintă tocmai finalitatea activităţii de spionaj; informaţiile secrete vin în completarea celor disponibile din surse deschise - a căror culegere şi prelucrare reprezintă o activitate de rutină pentru o serie de funcţionari (diplomaţi, ataşaţi militari sau economici, etc.) însărcinaţi cu monitorizarea diferitor aspecte ale vieţii socio-economice, politice, ş.a.m.d. - şi sprijină luarea deciziilor la nivel guvernamental, menite să contureze politica externă şi relaţiile internaţionale, sau să asigure anumite avantaje (competiţionale) în domeniile de interes.

Informaţiile clasificate deţin acest caracter datorită importanţei pe care o au pentru securitatea naţională şi care, datorită nivelurilor de importanţă şi consecinţelor care s-ar produce ca urmare a dezvăluirii sau diseminării neautorizate, trebuie să fie protejate. În baza evaluării informaţiei raportat la aceste două criterii, statele sau organizaţiile internaţionale îşi stabilesc taxonomii specifice, în cadrul cărora se reglementează şi cerinţele specifice de securitate aplcabile.

În România, Legea nr. 182 din 12 aprilie 2002 privind protecţia informaţiilor clasificate[3] prevede o serie de standarde naţionale obligatorii, în concordanţă cu criteriile şi recomandările NATO în acest domeniu. Conform acestei legi (art. 15), *clasele de secretizare* a datelor şi informaţiilor sunt: **secrete de stat** (care privesc securitatea naţională, prin a căror divulgare se pot prejudicia siguranţa naţională şi apărarea ţării) şi **secrete de serviciu** (informaţiile a căror divulgare este de natură să determine prejudicii unei persoane juridice de drept public sau privat). În continuare, *nivelurile de secretizare* sunt atribuie informaţiilor clasificate din clasa secrete de stat, distingând categoriile (Legea 182/2002, art.15, litera ”f”):

- **strict secret de importanţă deosebită** - informaţiile a căror divulgare neautorizată este de natură să producă daune de o gravitate excepţională securităţii naţionale;
- **strict secret** - informaţiile a căror divulgare neautorizată este de natură să producă daune grave securităţii naţionale;
- **secret** - informaţiile a căror divulgare neautorizată este de natură să producă daune securităţii naţionale.

În NATO sunt considerate patru niveluri de clasificare a securităţii: [4] [5]

a) COSMIC TOP SECRET (CTS), pentru informaţii a căror divulgare neautorizată ar cauza organizaţiei pagube excepţional de grave;
b) NATO SECRET (NS), pentru informaţii a căror divulgare neautorizată ar cauza pagube serioase organizaţiei;
c) NATO CONFIDENTIAL (NC), pentru informaţii a căror divulgare neautorizată ar afecta interesele organizaţiei;

[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=0CEIQFjAF&url=http%3A%2F%2Fwww.secnav.navy.mil%2Fdusnp%2FSecurity%2FInformation%2FDocuments%2Fintro-natosecuritybrief.pdf&ei=WKzrVLf1DOvXyQOruIKgBw&usg=AFQjCNFzhNqyeDeZwKRY8wgWcUJqkrfILg&bvm=bv.86475890,d.bGQ

d) NATO RESTRICTED (NR), pentru informaţii a căror divulgare neautorizată ar fi dezavantajoasă intereselor organizaţiei.

Revenind la tema spionajului, putem identifica o serie de priorităţi în ce priveşte informaţiile secrete vizate de către serviciile de spionaj, începând cu cele din domeniul militar şi politic, precum şi secretele industriale. Art. 17 din Legea nr. 182/2002 prezintă succint elementele de interes din categoria informaţiilor secrete de stat.

Raportat la modalităţile 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 priveşte tehnicile de spionaj şi lucrul cu agenţii, acţionând sub acoperire (cu sau fără protecţie diplomatică)[1];
- agenţii[2] - surse umane ce acţionează în mod acoperit şi furnizează, în mod clandestin, în baza poziţiei lor şi a relaţiilor de încredere prestabilite, informaţii către ofiţerii de intelligence; agenţii au o instruire de bază în tehnici de spionaj şi pot avea diferite motivaţii personale (inclusiv pecuniare) pentru desfăşurarea acestei activităţi.

Culegerea informaţiilor secrete se poate face printr-o largă varietate de metode, făcând apel la tehnologii de ultimă oră din domeniul comunicaţiilor (mijloace de interceptare, transmitere de date, înregistrare optică, acustică, sau a altor semnale, etc.) şi exploatând vulnerabilităţile de securitate ale organizaţiilor/ entităţilor spionate. Dezvoltarea spaţiului cibernetic oferă, din acest punct de vedere, oportunităţi extraordinare.

Sabotajul

În sens larg, sabotajul este definit ca fiind distrugerea, avarierea sau obstrucţionarea deliberată a unui sistem (instalaţii şi echipamente, activităţi, lucrări de infrastructură, servicii, etc.), în special pentru obţinerea unui avantaj politic sau militar[3], ca urmare a finalităţii reprezentate de împiedicarea bunului mers (eficienţei) al unei activităţi, în special frânarea desfăşurării normale a unui proces de producţie[4].

Acţiunea de sabotaj cade în sarcina celor numiţi, 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 consecinţelor actelor de care se fac responsabile). Dincolo de distrugerea fizică – ca metodă de acţiune pe care o implică sabotajul, obiectivul urmărit poate fi obţinut de sabotor şi prin exploatarea aşa numitului ”element uman”: oportunităţilor de luare a unor decizii greşite (care să disrupă activitatea lucrativă – ex. promovarea incompetenţilor în posturi cheie, fragmentarea activităţii prin convocarea de şedinţe în momente critice, etc.) şi convingerea altora de a le urma, sau adoptarea unor atitudini necooperante (ex. inflamarea situaţiei la locul de muncă cu efecte directe asupra productivităţii).[5]

Un exemplu de act de sabotaj, comis prin intermediul virusului STUXNET, este distrugerea unei părţi din echipamentul industrial al complexului nuclear iranian de la Natanz (Langner, 2013); alte exemple recente pot fi enumerate, comune situaţiilor de criză sau război, cum ar fi: pasivitatea şi neglijenţa forţelor de ordine ucrainene pe timpul revoltelor din oraşul

[1] Acțiunea în acest sens ce presupune asumarea unei false identități fiind practicată, 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 2014[1] sau distrugerea parţială prin acte de sabotaj a unor poduri de cale ferată în Ucraina, în martie 2015[2]. Sabotajul face parte din arsenalul de proceduri asimetrice ce pot fi utilizate în cazul unui război hibrid, după cum o arată acţiunile Rusiei în estul Ucrainei.

Subversiunea

NATO defineşte subversiunea[3] ca acţiune având ca scop slăbirea forţei militare, a puterii economice sau voinţei politice a unei ţări[4] prin subminarea moralului, a loialităţii cetăţenilor 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 forţă militară, regulamentele de specialitate ale armatei SUA menţionează în spectrul subversiunii şi acţiunea de încurajare activă a personalului militar sau civil în ce priveşte violarea legilor, nerespectarea ordinelor sau reglementărilor legale sau disruperea activităţilor militare cu intenţia expresă de a interfera cu (sau a afecta) loialitatea, moralul sau disciplina forţei (US CI Glossary, p. GL-82, 2011). În acest sens, toate actele ce contravin intereselor structurilor autorităţii şi nu se încadrează în categoriile: trădare, incitare la revoltă, sabotaj sau spionaj sunt considerate activitate subversivă (JP 1-02).

Avantajele oferite de acţiunile subversive sunt legate de riscul, costurile şi dificultatea relativ scăzută raportat la efectele urmărite; cu toate acestea, strategiile ce stau la baza acţiunilor subversive necesită reţele umane şi conexiuni bine stabilite în organizaţiile/ societăţile ţintă, precum şi o evaluare complexă a aspectelor sociale, politice, economice, culturale, religioase, etnice, istorice, etc. caracteristice acestora. Acţiunea propriu-zisă poate fi realizată prin pârghii de putere politică (infiltrarea şi manipularea partidelor), manipulare prin mass-media, infiltrarea instituţiilor şi structurilor din domeniul securităţii şi al apărării – de unde şi interesul pe care îl suscită pentru contrainformaţiile militare.

Alte subiecte de interes pentru disciplina contrainformaţiilor militare

Crima organizată

În România[5], Legea 39/ 2003 privind prevenirea şi combaterea criminalităţii organizate, publicată în Monitorul Oficial nr. 50 din 29.01.2003[6] (având ca bază Convenţia ONU împotriva criminalităţii transnaţionale organizate[7]), defineşte în capitolul I, art. 2, **grupul infracţional organizat** ca fiind grupul structurat, format din trei sau mai multe persoane, care există pentru *o perioadă şi acţionează 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, *Convenţie a naţiunilor unite împotriva criminalităţii transnaţionale 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 ***infracţiuni grave***[1]*, pentru a obţine direct sau indirect un beneficiu financiar sau alt beneficiu material* (totodată, nu constituie grup infracţional organizat grupul format ocazional în scopul comiterii imediate a uneia sau mai multor infracţiuni şi care nu are continuitate sau o structură determinată ori roluri prestabilite pentru membrii săi în cadrul grupului).

Infracţiunile grave, în contextul acţiunii structurate, capătă un interes deosebit din punct de vedere al securităţii din cauza impactului pe care acţiunile respective îl au la nivelul societăţii, prin penetrarea unor domenii esenţiale funcţionării statului (ex. crearea de riscuri sistemice prin fraudare masivă, asociată cu coruperea reprezentanţilor puterii) şi dezvoltarea lor la dimensiuni şi grade de complexitate comparabile cu cele corporatiste[2], într-o multitudine de modele acţionale (Miclea, 2004).

În mediul militar, acţiunile complexe pe care criminalitatea organizată le presupune, coordonarea şi relaţiile dintre membrii reţelelor criminale (naţionale sau transnaţionale), obiectivele lor, precum şi conexiunile membrilor forţelor proprii cu elemente de crimă organizată (percepute ca vulnerabilităţi) devin subiecte de interes pentru serviciile de contrainformaţii.

Ameninţările din interior ("insider threat")

Capabilitatea şi activitatea de Intelligence nu este vulnerabilă doar în faţa unor factori externi, ci şi a ameninţărilor venite din interior – contabilizate la nivel de vulnerabilităţi exploatate prin activităţi ca subversiunea, trădarea, scurgerile de informaţii secrete, infiltrarea elementelor ostile.

Pericolul din interior ("*insider threat*") este reprezentat de indivizi aparţinând organizaţiei – actuali sau foşti angajaţi, contractori, asociaţi – cu acces la zone sensibile şi informaţii secrete pe care le exploatează în interes personal sau al unei terţe entităţi (organizaţii sau chiar ţări), afectând interesele propriei organizaţiei sau chiar securitatea naţională (de la furtul unor date privind proprietatea intelectuală/ spionaj economic până la sabotaj şi crimă).

În acest caz, efortul contrainformativ este focalizat asupra unor aspecte privind:[3]

- *factorii personali* (motive sau situaţii ce determină o astfel de acţiune îndreptată împotriva propriei organizaţii – cum ar fi: nevoia de bani, dorinţa de răzbunare, frustrarea la locul de muncă, conflictul ideologic sau de loialitate, spiritul de aventură, vulnerabilitatea la şantaj, comportament compulsiv etc.), asociaţi unor *indicatori de comportament* de natură să trezească suspiciuni cu privire la activitatea suspectului (accesarea unor documente care nu ţin de necesitatea profesională; prezenţa (neaprobată) la lucru în afara programului normal; nerespectarea politcilor de

[1] **infracţiunea gravă** este infracţiunea care face parte din una dintre următoarele categorii: omor, omor calificat, omor deosebit de grav; lipsire de libertate în mod ilegal; sclavie; şantaj; infracţiuni contra patrimoniului, care au produs consecinţe deosebit de grave; infracţiuni privitoare la nerespectarea regimului armelor şi muniţiilor, materiilor explozive, materialelor nucleare sau al altor materii radioactive; falsificare de monede sau de alte valori; divulgarea secretului economic, concurenţa neloială, nerespectarea dispoziţiilor privind operaţii de import sau export, deturnarea de fonduri, nerespectarea dispoziţiilor privind importul de deşeuri şi reziduuri; proxenetismul; infracţiuni privind jocurile de noroc; infracţiuni privind traficul de droguri sau precursori; infracţiuni privind traficul de persoane şi infracţiuni în legătură cu traficul de persoane; traficul de migranţi; spălarea banilor; infracţiuni de corupţie, infracţiunile asimilate acestora, precum şi infracţiunile în legătură directă cu infracţiunile de corupţie; contrabanda, evaziunea fiscală, alte infracţiuni financiare; bancruta frauduloasă; infracţiuni săvârşite prin intermediul sistemelor şi reţelelor informatice sau de comunicaţii; traficul de ţesuturi sau organe umane; orice altă infracţiune pentru care legea prevede pedeapsa închisorii, al cărei minim special este de cel puţin 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 organizaţiei; contacte cu străini care nu sunt raportate; călătorii scurte şi dese în afara ţării, fără o motivaţie credibilă; afişarea unei bunăstări nejustificate de câştigurile materiale; interes deosebit în ce priveşte alţi colegi; manifestarea îngrijorării cu privire la posibilitatea de a fi supravegheaţi, etc.);

- *factorii organizaţionali* (percepţia relaxată asupra riscurilor şi vulnerabilităţilor; deficienţe privind politicile de securitate, managementul informaţiilor, instruirea angajaţilor; practici de lucru neadecvate, care duc la o presiune a timpului asupra anagajaţilor şi la eludarea unor aspecte privind securitatea, etc.).

Noţiunile ”*insider threat*” sau ”*green on blue*” sunt în mod comun folosite în operaţiile militare (NATO) pentru a desemna militari ai ţării gazdă, aflaţi în relaţii de cooperare cu forţele 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).

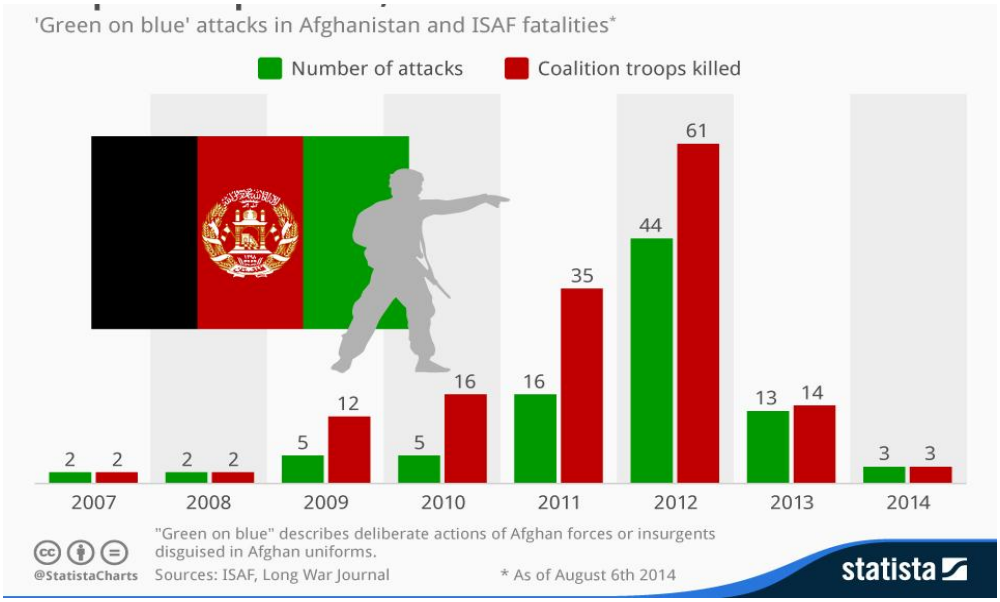


Figura 1.8 Evoluţia incidentelor de tip ”*green on blue*” (atacuri ale militarilor afgani asupra militarilor din cadrul coaliţiei) în misiunea ISAF. Numărul de atacuri este reprezentat pe coloanele verzi, iar numărul de victime pe coloanele roşii.[1]

Dincolo de spectrul de ameninţări TESSOC, acest tip de atacuri sunt de o importanţă deosebită pentru protecţia (şi moralul) forţei, reclamând acţiuni complexe de prevenire.[2]

Ameninţările cibernetice

Interesul tot mai mare al CI pentru acţiunile în mediul cibernetic este legitimat de o creştere exponenţială a dependenţei funcţionale a sistemelor de securitate organizaţionale/ naţionale de suportul informatic, asociat creşterii progresive a numărului de atacuri cibernetice sau utilizare a spaţiului cibernetic în sprijinul unor acţiuni 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=JJJlVdegAer7ygPbooHABQ&ved=0CBsQFjAB&usg=AFQjCNGNuG1z_1dsst-BPey0XROzU3jNag

Avantajele acţiunii în mediul cibernetic ţin de costurile relativ scăzute raportat la volumul de date accesibil (şi valoarea acestora)/ impactul acţiunii ostile, în condiţii de siguranţă fizică şi posibilitatea de acţiune cu identitatea disimulată a operatorului, indiferent dacă acţionează în interes personal, în numele unui grup (activist/ criminal/ terorist) sau al unui stat.

Acţiunile ostile în mediul cibernetic pot reprezenta un risc la adresa securităţii statului, a sistemului socio-economic, a bunei funcţionări a unor organizaţii din domenii vitale, etc., de aceea eforturile CI sunt îndreptate spre identificarea atacatorului, stabilirea procedurilor folosite, contracararea acţiunilor de spionaj cibernetic, determinarea structurilor implicate (componenta operaţională), ş.a.m.d. – alunecând către o supraspecializare ce fac acest domeniu distinct în spectrul capabilităţilor structurilor de securitate (a se vedea capitolul referitor la Intelligence în mediul cibernetic).

Concluzii

Este important de subliniat faptul că activitatea CI se desfăşoară într-un cadru normat, legitim; în general, obiectivul de securitate al activităţilor CI vizează protecţia a trei elemente fundamentale la nivel de organizaţie: personalul, instalaţiile şi operaţiile proprii.

Parte din atributele ”pasive” ale disciplinei CI se leagă atât de documentarea şi cunoaşterea ameninţărilor şi a elementelor legate de acestea – surse posibile (organizaţii, indivizi), locaţii, etc., precum şi de sensibilizarea şi educarea personalului structurilor protejate cu privire la riscurile de securitate la care pot fi expuşi. În partea acţională, monitorizarea persoanelor cu vulnerabilităţi în ce priveşte spectrul TESSOC urmăreşte aspecte legate de fundamentarea motivaţională a deciziei acestora de implicare în astfel de acţiuni[1].

Contracararea mijloacelor tehnice ce pot fi utilizate în reţele de spionaj (senzori SIGINT, IMINT, MASINT) se bazează pe identificarea vulnerabilităţilor propriilor sisteme/ elemente, furnizarea de soluţii de securitate (inclusiv măsuri de mascare pasivă şi activă) şi monitorizarea acestora.

Pentru asigurarea protecţiei corespunzătoare în domeniul surselor deschise, cenzurarea informaţiei (pusă în balanţă de libertatea de exprimare specifică societăţilor democratice) reprezintă o măsură de prevenire a scurgerii de date şi informaţii de valoare. Clasificarea documentelor în funcţie de valoarea datelor şi informaţiilor pe care le conţin şi a impactului pe care publicarea acestora l-ar avea asupra capabilităţilor proprii reprezintă o practică aproape universală, parte a măsurilor generale de protecţie a informaţiei – 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. ***, *Dicţionarul explicativ al limbii române* (ediţia a II-a revăzută şi 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&rct=j&frm=1&q=&esrc=s&sa=U&ei=JJJlVdegAer7ygPbooHABQ&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 şi combaterea criminalităţii organizate
27. Legea nr. 182 din 12 aprilie 2002 privind protecţia informaţiilor clasificate
28. LOWENTHAL, M. (2003) *Intelligence: From secrets to policy*, Washington, DC, CQ Press
29. MARCU, Florin (2000) *Marele dicţionar de neologisme*, Editura Saeculum
30. 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=0CEIQFjAF&url=http%3A%2F%2Fwww.secnav.navy.mil%2Fdusnp%2FSecurity%2FInformation%2FDocuments%2Fintro-natosecuritybrief.pdf&ei=WKzrVLf1DOvXyQOruIKgBw&usg=AFQjCNFzhNqyeDeZwKRY8wgWcUJqkrfILg&bvm=bv.86475890,d.bGQ
31. MICLEA Damian (2004) *Combaterea crimei organizate – evoluţie, tipologii, legislaţie, particularităţi*, Editura Ministerului Administraţiei şi Internelor, Bucureşti
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. Organizaţia Naţiunilor Unite, *Convenţie a naţiunilor unite împotriva criminalităţii transnaţionale 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 şi noi ierarhii ale statelor definesc imaginea unei lumi în continuă schimbare, în care principiile dreptului internațional sunt aplicate selectiv, puterea militară întrând 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 Pace[1]), în colaborare cu revista „Foreign Policy", publică un index anual denumit „The Failed States Index" (Topul statelor eşuate), în care stabileşte (fără pretenţii de exhaustivitate, dar de o manieră tot mai complexă în timp) ierarhia statelor ce alunecă spre colaps structural. Lista face referinţă exclusivă la state suverane, determinate de apartenenţa 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 societăţile democratice, asigurând un proces de analiză, cercetare, proces decizional şi evaluare politică pluralist şi cuantificabil (Nakamura, 2002), până la minimalizarea credibilităţii lor în lumina servituţii unor scopuri dictate de sponsori[2]. În mod evident, există o aliniere (mai mult sau mai puţin declarată) a acestor instituţii politice la anumite perspective ideologice sau la promovarea unor interese private, fapt ce poate altera demersul ştiinţific 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 eşuat" sau „pseudo-stat" – ca expresie a unei stări alterate a puterii de stat – şi promovarea lor în limbajul politic internaţional 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 suveranităţii naţionale 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 salvgardării securității umane).

Cazul Libiei, unde perspectiva unui dezastru umanitar a generat intervenția militară a comunităţii internaţionale, nu a găsit aceeași rezonanță într-o situație de criză similară[3] (a se vedea situaţia Siriei, în cazul căreia o rezoluţie a Consiliului de Securitate al ONU a fost blocat în repetate ori de Rusia şi 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 economică[4] sau stabilitatea financiară[5], Banca Mondială[6] - 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 rezoluţiilor ONU care reclamă intervenţia militară de către organizaţii regionale cu relevanţă 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 umană[1], etc.) cât și la nivel informal, de către organizații neguvernamentale (ex. Fitch – în domeniul financiar și al asigurărilor[2], fundația Heritage – cu Indexul Libertății Economice[3], 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, existenţa entităţilor statale nefuncţionale este un fapt cert şi considerăm de interes a observa cum funcţionează balanţa dintre factorii de dezechilibru interni şi externi în procesul manifestării evoluţiei lor spaţio-temporale.

Deși central pentru subiectul dezbătut, conceptul de stat "eşuat" este doar o inovaţie lingvistică şi 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 mutaţiile suferite de capabilităţile puse în slujba ameninţărilor, care s-au modificat radical.

Fragilitatea nu constituie un pericol doar pentru statul în cauză, ci reprezintă o ameninţare pentru progresul şi stabilitatea altor state, care depind într-un fel sau altul de aceste entităţi sau se găsesc în situaţii care suferă comparaţii, mai ales în condiţiile 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 inducţie şi sugestie, care definesc state sau guverne prezentând simptome ale unei existenţe ce nu se încadrează în uzanţele general acceptate şi după care un stat se manifestă sau fiinţează în cadrul comunităţii internaţionale ca: „eşuat" (*failed state*), „în colaps" (collapsed state), „escroc" sau „bandit" (*rogue state*), „pseudo-stat" (*pseudo-state*) sau chiar „stat terorist".

Definirea conceptului de stat eşuat comportă mai multe sisteme de referinţă (Thürer, 1999):

Abordarea din punct de vedere politic şi legal se concretizează în trei elemente: aspectul geografic şi teritorial (criza ca implozie, asociată cu probleme interne, dar incluzând şi impactul extern incidental), aspectul politic (colapsul intern al legii şi ordinii datorat prăbuşirii structurilor responsabile – mai degrabă decât cel generat de acţiunile unor facţiuni care urmăresc întărirea propriei poziţii sau chiar uzurparea celei de stat) şi aspectul funcţional (absenţa structurilor capabile să reprezinte statul la nivel internaţional şi, pe de altă parte, să recepteze influenţele lumii exterioare).

Tributar contextului istoric şi de dezvoltare, observăm că statele considerate ca „eşuate" aparţin eminamente lumii a treia şi au fost afectate de trei factori geopolitici: sfârşitul Războiului Rece (şi implicit al suportului masiv primit de regimurile ideologice artificiale ţinute în funcţie de către superputerile lumii; absenţa sponsorizărilor acestora a permis întărirea puterii facţiunilor rivale, iar statele au început să îşi piardă legitimitatea şi autoritatea, reducându-se la valoarea de alt grup în conflict cu celelalte), moştenirea regimurilor colonialiste (care au durat suficient de mult pentru a distruge structurile sociale tradiţionale, dar nu suficient de mult pentru a le înlocui cu structurile constituţionale occidentale şi a le da identitatea unui nou stat – de aici autoritate bazată pe dominanţa 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/

poliţienească şi nu pe legitimitate, loialitatea redusă a populaţiei şi divizarea acesteia[1]) şi procesele generale de modernizare care au încurajat mobilitatea socială şi geografică, dar fără a fi contrabalansată de procese de construcţie naţională capabile să plaseze statul pe un fundament solid, oferindu-i capabilitatea de a gestiona integrarea pieţei şi schimbul şi fluxul liber de capital. În viziune critică neo-imperialistă (Liu, 2005), aceasta se traduce în transformarea statelor client slăbite, cu drepturi de suveranitate restricţionate, în capete de pod ale pieţei statului puternic în expansiunea sa generală, detaşând securitatea economică de funcţiunile 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 esenţei guvernării (inexistenţa sau inabilitatea de exerciţiu a organelor de lege şi ordine) şi brutalitatea şi intensitatea violenţei folosite (a se vedea situaţia din Liberia).

Subsumând, observăm mai mulţi indicatori care determină catalogarea unui stat ca fiind „eşuat", printre aceştia regăsindu-se:

- un stat al cărui guvern central este atât de slab sau ineficient încât deţine un control efectiv redus asupra celei mai mari părţi a teritoriului său, după cum vom arăta în cadrul acestui capitol, şi varianta în care – în condiţiile păstrării controlului – supune structura statală intereselor private, în serviciul unei clientele bogate ce îşi 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 (absenţa unui sistem universal de protecţie a sănătăţii; sistem de învăţământ primar public rezervat copiilor săraci disfuncţional);
- corupţie şi criminalitate larg răspândite;
- existenţa refugiaţilor şi a dislocărilor involuntare de populaţie;
- declin economic accentuat în condiţiile unei infrastructuri economice care clachează în a asigura venituri şi bunăstare în mod echitabil şi merge până la foamete şi lipsa de hrană pentru populaţia săracă în timp ce în economie persistă surplusuri de hrană;
- interacţiuni inexistente sau ratate cu alte state.

Putem considera că un stat supravieţuieşte atâta timp cât işi menţine monopolul asupra uzului legitim al violenţei în cadrul propriilor frontiere. Când acest fapt nu mai este efectiv (în faţa prezenţei „lorzilor războiului", a miliţiilor rebele sau elementelor teroriste), existenţa propriu zisă a statului devine îndoielnică iar acesta întruneşte premizele încadrării în categoria statelor eşuate.

Dificultatea în a determina gradul de menţinere a unui astfel de monopol asupra uzului legitim al forţei (care include şi problema definirii legitimităţii) nu este clar conturată. Pornind de la premiza că doar un stat deţine mijloacele de producţie necesare asigurării instrumentelor violenţei fizice, nu se pune problema legitimităţii în ce priveşte obţinerea 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 eşuate 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 in aceste state a constat intr-o serie de strategii de subordonare si asimilare care tind sa maximizeze resentimentele grupurilor submise – etnic, religios, etc. Rezultatul final il constituie o profunda polarizare, bazata pe deziluzie si insatisfactii legate de stat atat din partea populatiei, cat si a elitelor locale. A se vedea pe larg in: 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, in http://www.globalpolicy.org/nations/sovereign/failed/2003/12failedcollapsedstates.pdf

unor astfel de funcţiuni de către grupuri de interes special. Această categorie de state deţin o putere militară/ poliţienească dezvoltată şi promovează interesele economice înguste ale unei mici clase de cetăţeni, în timp ce sacrifică marea masă a populaţiei ca victime ale unei pieţe esuate.

Termenul de „stat eşuat" este de asemenea folosit în sensul în care un stat se dovedeşte a fi ineficient, incapabil să aplice în mod uniform legea din cauza unei rate înalte a criminalităţii, corupţiei politice extreme, pieţei negre supradimensionate, birocraţiei impenetrabile, ineficienţei juridice, interferenţelor militare în politică, împrejurărilor culturale în care lideri tradiţionali reclamă mai multă putere decât cea statală asupra unei anumite zone, dar nu intră în competiţie cu statul.

Centrul de Cercetare a Crizelor Statale[1] defineşte „statul eşuat" ca o variantă a „colapsului statal" - stat care nu mai este în măsură să îşi exercite securitatea de bază şi funcţiunile de dezvoltare şi nu deţine un control efectiv asupra teritoriilor şi frontierelor sale. Un stat eşuat nu mai este în măsură să asigure condiţiile propriei existenţe. Această idee este utilizată în modalităţi contradictorii în comunitatea politică, existând o tendinţă de a eticheta un stat cu slabe performanţe ca fiind „eşuat", 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 esenţa sa arbitrar, contestabil şi încărcat din punct de vedere ideologic. Conceptul îşi găseşte originea în adoptarea sa de către britanici în India, pe timpul perioadei coloniale. În anii `60 – `70, mai mulţi autori au utilizat termeni similari pentru a descrie anumite state cu comportament neconform cu normele internaţionale. În accepţiunea sa de azi, conceptul de "stat bandit" se conturează în anii `80, când se vorbea şi de "state teroriste" şi "în afara legii". În 1986, preşedintele 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 puţin interes. La acea vreme, Anthony Lake, consilierul preşedintelui 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 sfârşitului războiului rece. Folosirea conceptului s-a răspândit rapid în sânul Congresului şi în media americană. Pe lista statelor bandit se regăseau: Coreea de Nord, Siria, Libia, Iranul, Irakul, Sudanul şi Cuba. În contextul multiplicării criticilor legate de folosirea acestui termen, a fost retras de către administraţia Clinton din discursul său oficial şi înlocuit cu cel de «*state of concerns*» (state care provoacă îngrijorări), revenind în planul discuţiilor după evenimentele din 11 septembrie 2001.

O altă sintagmă folosită este noţiunea de pseudo-stat, definită ca acea entitate care nu este fondată decât pe legături personale, de clan sau tribale şi pentru care, în viziunea S.U.A., Convenţiile de la Geneva nu se justifică a fi aplicate[2]. Acesta este cazul Afganistanului, unde prizonierii făcuţi de forţele americane nu s-au bucurat de statutul de prizonieri de război, determinând apariţia unei noi categorii de deţinuţi, cu regim special – cei „suspecţi de terorism".

Topul statelor eşuate; premizele colapsului şi metodologia de cercetare aplicată

Nu vom insista asupra realităţilor particulare care au determinat prezenţa în partea superioară a clasamentului a anumitor state; există o vastă disponibilitate de informaţii 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, in http://www.voltairenet.org/article16092.html

metodologiei folosite pentru a putea determina scorurile şi a stabili clasamentul statelor în topul susceptibilităţii de eşuare.

Instrumentul de lucru a fost denumit „Conflict Assessment System Tool" (CAST) – Complex de Sisteme de Evaluare a Conflictului. Pe lângă notarea a 12 indicatori[1] sociali, economici şi politico – militari pe care îi vom detalia în cadrul acestui capitol, alte etape cuprind evaluarea capabilităţilor a cinci instituţii de stat considerate esenţiale pentru sustenabilitatea securităţii, identificarea factorilor idiosincratici şi a surprizelor, precum şi plasarea ţărilor pe o hartă a conflictelor care să arate istoricul riscurilor la care acestea sunt supuse.

Notarea este bazată pe un scor obţinut în urma analizei indicatorilor de vulnerabilitate a statelor: patru în domeniul social, doi economici şi şase politici, cu un rating cuprins de la 0 la 10, 10 semnificând „cel mai puţin stabil". Indicatorii nu sunt concepuţi să prezică momentul în care statele analizate riscă să se confunte cu violenţe 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 populaţiei relativ la posibilităţile de asigurare cu hrană şi alte resurse vitale. Presiunea izvorâtă din patternurile sociale şi delimitările fizice, incluzând disputele de frontieră, deţinerea sau ocuparea de terenuri, acces la căile de transport, controlul locaţiilor cu semnificaţie religioasă sau istorică şi riscul producerii unor pericole environmentale.

2. Deplasări masive de refugiaţi sau de persoane dislocate: împrăştierea forţată a largi comunităţi ca rezultat al violenţelor directe, a represiunilor, lipsei hranei, bolilor, lipsei apei potabile, competiţiei pentru terenuri şi tulburărilor care pot să le antreneze în spirala unor mari probleme umanitare şi de securitate, atât în cadrul propriei ţări cât şi între state.

3. Neajunsul reprezentat de perpetuarea grupărilor care caută răzbunare în virtutea unor nedreptăţi recente sau mai vechi, chiar datând secole în urmă, incluzând atrocităţi, persecuţii sau represiuni trăite de marea masă sau de grupuri particulare în relaţia cu statul sau cu alte grupări dominante. Aceste atitudini revanşarde pot să aibă la origini şi excluderea politică instituţionalizată, putând căpăta forme de responsabilizare publică în cadrul retoricii politice naţionaliste lansate în critici aduse grupărilor considerate a fi responsabile.

4. Emigrare cronică şi susţinută: atât exodul creierelor, alimentat de emigraţia profesioniştilor, intelectualilor şi dizidenţilor politici, cât şi emigraţia voluntară a reprezentanţilor clasei mijlocii. Creşterea comunităţilor în exil/ expatriate sunt de asemenea folosite ca parte ale acestui indicator.

b. Indicatori economici

5. Dezvoltarea economică inegală determinată de inegalităţile de grup ori de inechităţile percepute în educaţie, muncă şi statut economic. De asemenea, include măsurile nivelurilor sărăciei la nivel de grup, rata de mortalitate infantilă, nivelurile de educaţie.

6. Declinul economic accentuat/ sever, care este măsurat ca progresie a declinului economic al societăţii ca întreg (folosindu-se în acest sens: venitul brut per capita, PIB, datoriile, rata de mortalitate a copiilor, nivelurile de sărăcie, eşecurile în afaceri) şi vizează în egală măsură evoluţia preţurilor, schimburile, investiţii străine sau plata datoriilor. Este urmărit colapsul sau devalizarea monedei naţionale şi creşterile pe care le înregistrează economia subterană, incluzând traficul de droguri, armament, minerale rare, precum şi expedierile de capital. Un alt reper îl constituie neplata de către stat a salariilor către funcţionarii publici, către forţele armate sau a altor obligaţii financiare către proprii cetăţeni, cum ar fi plata pensiilor.

[1] Apud http://en.wikipedia.org/wiki/Failed_state

c. Indicatori politici interni

7. Criminalizarea şi/ sau delegitimarea statului: corupţie şi profitorism al elitelor conducătoare, rezistenţă la transparenţă, politica financiară, reprezentarea politică. Reperul include orice pierdere a încrederii populaţiei pe scară largă în procesele şi instituţiile statului.

8. Deteriorarea progresivă a serviciilor publice: o dispariţie a funcţiunilor de bază ale statului care serveau populaţiei, incluzând lipsa protecţiei acesteia faţă de terorism şi violenţă şi asigurarea serviciilor esenţiale în domeniile: sănătate, educaţie, igienă, transport public. De asemenea, folosirea aparatului de stat în folosul agenţiilor subordonate elitelor conducătoare, cum ar fi forţele de securitate, stafful prezidenţial, banca centrală, serviciul diplomatic, vămile şi agenţiile de colectare a taxelor şi impozitelor.

9. Violarea pe scară largă a drepturilor omului: emergenţa unor reguli autoritariste, dictatoriale sau militare în care instituţiile şi procesele constituţionale şi democratice sunt suspendate sau manipulate. Mai sunt cuantificate: izbucniri ale violenţei de inspiraţie politică împotriva civililor nevinovaţi; un număr crescut de prizonieri politici sau dizidenţi cărora li se refuză un proces echitabil, în concordanţă cu practicile şi normele internaţionale; orice abuz asupra drepturilor legale, politice şi sociale, incluzându-le pe cele ale indivizilor, grupurilor sau instituţiilor culturale.

10. Aparatul de securitate ca „stat în stat": emergenţa elitelor sau a „gărzilor pretoriene" care opereaza fără a fi supuse pedepsei; emergenţa miliţiilor private sponsorizate sau sprijinite de stat în vederea terorizării oponenţilor politici, a celor suspectaţi ca fiind „inamici" sau a civililor care simpatizează opoziţia; o „armată în cadrul armatei", care serveşte interesele unei clici militare sau politice dominante; emergenţa miliţiilor rivale, forţelor de gherilă sau armatelor private în acţiuni armate sau campanii violente împotriva forţelor de securitate a statului.

11. Ridicarea elitelor facţionalizate, focalizându-se asupra fragmentării elitelor conducătoare şi a instituţiilor statului pe linia intereselor de grup. Este urmărit orice uz al retoricii politice naţionaliste de către elitele conducătoare, adeseori în termeni iredentişti sau de solidaritate comunitară.

Nu numai realităţile 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 importanţă 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 evidenţia o metodologie în acest sens (similară CAST):

- angajări militare sau paramilitare în afacerile interne ale statului aflat în situaţie de risc;
- acţiuni ale unor armate externe, state, grupuri de identitate sau entităţi care afectează balanţa internă a puterii ori rezoluţia unui conflict;
- intervenţii ale unor donori (în mod special daca există o tendinţă către dependenţa exclusivă de sprijin străin[1]) sau existenţa 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 şi al înfometării[1].

[1] Ajutorul internaţional nu reuşeşte să depăşească 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 si 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 stat[2].

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 SWOT[3]

Observăm din cele prezentate că afişarea consistentă a grijilor legate de statele eşuate au apărut în politica internaţională după 1990, odată cu aplicarea principiului Westfalian al suveranităţii[4] în funcţie de alte criterii decât cele consacrate până atunci. Promotorul acestei noi terminologii - diplomaţia americană – s-a lansat în paralel în găsirea de soluţii pentru nou identificatele provocări la adresa dinamicii de securitate globală.

În 1994, vicepreşedintele SUA Al Gore stabilea instituţia "State Failure Task Force" (Stohl şi Stohl, 2001), compusă dintr-un grup de distinşi academicieni care aveau ca sarcină, în cooperare cu agenţiile guvernamentale, să analizeze factorii care duc la colapsul statal şi să dezvolte scheme de acţiune pentru contracararea acestora. Ulterior, politica preşedintelui Clinton faţă de aceste state s-a bazat pe trei componente: acţiunea asupra cauzelor destabilizatoare din statele eşuate, promovarea securităţii colective şi a capacităţii de reacţie corelate cu nevoile (bazată pe ONU şi NATO) şi angajarea în diplomaţia preventivă.

---

[1] Datele în acest sens sunt îngrijorătoare: 73 milioane de persoane din 78 de ţări 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 ţări şi îşi are originile în: cererea tot mai mare de alimente (în special în ţările beneficiare ale boom-ului economic, China şi India), folosirea biocombustibilor, nivelul tot mai scăzut al stocurilor mondiale de hrană, speculaţiile de pe piaţă, creşterea preţurilor la combustibili şi a cheltuielilor de producţie agricolă, modificările climatice şi restricţiile de export (Pomeroy, f.a.). Şeful FMI a avertizat că înfometarea în masă poate duce la război şi dezechilibre macroeconomice care să afecteze naţiunile 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] Strenghts, 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 teritorialităţii şi suveranităţii statelor. În interiorul frontierelor, ordinea este de apanajul autorităţilor statale, deţinătoare ale monopolului violenţei legitime, în timp ce viaţa internaţională este caracterizată de anarhie.

În aprilie 2000, Comisia de Securitate Naţională a S.U.A. (cunoscută şi sub denumirea Hart – Rudman, de la numele componenţilor) a elaborat un raport ce sublinia şase obiective-cheie de securitate naţională a S.U.A. pentru primul sfert al secolului XXI. Comisia recomanda ca primă reacţie în relaţia cu entităţi statale eşuate folosirea diplomaţiei preventive, incluzând apelul la iniţiative politice şi economice. În caz de insucces, SUA trebuiau să fie pregătite să acţioneze militar în cooperare cu alte naţiuni în situaţii caracterizate de următoarele criterii (Stohl şi Stohl, 2001):

- când state aliate/ prietene ale SUA erau în pericol;
- când apărea pericolul folosirii de arme de distrugere în masă care să afecteze populaţia civilă;
- când accesul sistemului economic global la resurse critice este pus în pericol;
- când un regim îşi demonstrează intenţia de a aduce atingeri serioase intereselor SUA;
- în caz de genocid.

Comisia a considerat că existenţa premizelor unui singur factor din cei amintiţi este suficient pentru a justifica o intervenţie militară. În consecinţă, pe lângă statele care într-adevar suferă de tare politice, sociale, economice ce le deviază de la cursul normal al existenţei, adâncindu-le în crize care duc, inevitabil, la catastrofe umanitare, există şi state puse în poziţia ori de a nu fi suficient de puternice (sau hotărâte) în a-şi gestiona problemele interne – şi de aici a risca neacceptarea lor ca fiind suverane de către alte state, fie să fie etichetate ca state eşuate pentru violarea drepturilor omului în încercarea lor de a-şi menţine securitatea internă. Această postură a războiului care nu se naşte din puterea statului, ci din slăbiciunea sa (Pouligny, 2000), poate justifica intervenţiile peste frontiere din motive legate de drepturile omului sau din raţiuni economice, în special când opţiunea intervenţiei aparţine exclusiv statelor puternice care, în baza forţei lor militare, îşi arogă privilegiul de a defini standardele drepturilor omului şi echităţii economice (Liu, 2005).

În virtutea acestor considerente, deşi algoritmul şi logica analizei CAST sunt îmbietoare ca demers ştiinţific[1], ideea în sine de a realiza un „top" al statelor eşuate forţează etica relaţiilor internaţionale şi stigmatizează oarecum întregul pe care statul îl reprezintă. Nu se pune problema aici de formalism şi curtoazie proprii limbajului diplomatic. A spune despre un stat că este eşuat induce ideea de ireversibilitate a fenomenului şi conferă o senzaţie de întrunire a tuturor tarelor abordate în cadrul sistemelor de referinţă anterior trecute în revistă.

Comentariile legate de acest subiect vădesc o stare de confuzie; accesând forumurile de discuţii pe Internet având acest topic, observăm – pe lângă frustrarea unor participanţi, cetăţeni ai unor state listate în partea superioară a clasamentului, intervenţii care demonstrează scoaterea din context a unor indicatori, nuanţarea unor abordări, apelul la evenimente mai mult sau mai puţin relevante, şi – peste toate acestea – tendinţa 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 existenţei

[1] După cum evidenţiază cercetătorii din cadrul celor două think-tankuri americane, metodologia CAST, permanent revizuită şi perfecţionată cu concursul unor experţi şi agenţii din toate sectoarele de interes, prezentând garanţia folosirii surselor alternative de informare, se constituie, în principiu, într-un instrument complex şi viabil de analiză a stării generale a unui stat. În sprijinul acestei afirmaţii vine faptul că această metodologie este folosită de guverne ale mai multor state, printre alte instrumente de analiză, pentru a obţine avertizări timpurii şi a desemna strategiile de asistenţă economică care pot reduce potenţialul pentru conflict şi să promoveze dezvoltarea în statele fragile. Uzul militar al CAST se regăseşte în întărirea avertizărilor punctuale, perfecţionarea gradului de pregătire şi aplicarea de strategii de evaluare a succesului în operaţiuni de stabilitate şi pace. Sectorul privat foloseşte această metodologie pentru a calcula riscurile politice pentru oportunităţile de investiţii. Organizaţiile multinaţionale şi un segment al altor entităţi găsesc acest instrument util pentru modelare şi simularea de scenarii, managementul organizaţiilor complexe şi pentru evaluarea riscurilor conflictuale. Educatorii îl folosesc pentru a antrena studenţii în analiza problemelor aferente stărilor de război şi pace prin mixarea tehnicilor specifice tehnologiei informaţiilor cu ştiinţele sociale. Finalmente, ţările implicate în testare folosesc CAST pentru autoevaluare cu criterii obiective în căutarea reperelor propriei stabilităţi şi performanţe.

sale istorice, este însă forţat a supune aceluiaşi complex de sisteme de referinţă state cu fundamente istorice şi culturale radical diferite. Acest fapt poate alimenta şovinismul şi se constituie în argumente ce justifică intervenţionismul.

În plus, apare întrebarea privind independenţa de opinie şi neutralitatea instituţiilor care au întocmit acest index[1]. Legat de aceasta, fragilitatea credibilităţii unui astfel de top se învârte în posibilitatea influenţării scorului în sensul dictat de anumite interese. În virtutea raţiunilor 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 aşa zis „generale" ale eşuării pot fi recompensate cu o poziţie favorabilă pe listă în funcţie de atitudinea pe care o au faţă de superputere şi de serviciile pe care le aduc acesteia.

Cu rezerva acestor obiecţii considerăm, totuşi, 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 situaţiei unui anumit stat, mai ales în condiţiile în care se apelează la corelarea datelor statistice cu informaţii valide legate de specificul evoluţiei istorice şi a valenţelor culturale care definesc profilul respectivei entităţi.

Cu cât factorii de decizie avizaţi pot anticipa, monitoriza şi măsura problemele, cu atât mai mult pot fi prevenite căderi violente, proteja civilii aflaţi în zone de conflict şi promova refacerea şi recuperarea. În acelaşi timp, politicienii trebuie să se concentreze în construirea capacităţii instituţionale a statului slăbit, în principal a celor cinci instituţii de bază: cea militară, poliţia, serviciile civile, sistemul de justiţie şi conducerea. Politicile în acest sens trebuie ajustate nevoilor concrete ale statului, monitorizate şi evaluate permanent, ajustate în funcţie de necesităţi, toate acestea între reperele unei tot mai necesare ştiinţe a reclădirii statale.

În ce priveşte termenul de "stat eşuat", sugestivitatea sa l-a consacrat în limbajul profan, dar şi cel ştiinţific. 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 eşuate, dorim să atragem atenţia asupra realităţilor de strictă actualitate care zugrăvesc spectacolul sumbru al scenelor de violenţă din anumite zone fierbinţi ale globului, precum şi perspectivele oferite de consecinţele 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 instituţie specializată în diagnoza şi evoluţia conflictelor asociate statelor slăbite şi a reacţiilor de politică externă la astfel de fenomene, organizaţia asumându-şi rolul de a promova conceptul de securitate sustenabilă şi a cultiva abilitatea societăţilor de a-şi rezolva problemele în mod paşnic, fără o prezenţă militară sau administrativă străină (http://www.fundforpeace.org/publications/annual/ar2006.pdf). "Foreign Policy" este o revistă de politică, economie şi relaţii internaţionale care a fost lansată în 1970 în S.U.A. şi este editată de think-tankul The Carnegie Endowment for International Peace (CEIP), în mod formal o organizaţie non-profit privată, care îşi asumă non-partizanatul, în practică puternic asociată cu United States Department of State, mulţi dintre preşedinţii SUA, numeroase grupuri de afaceri străine private şi liderii partidelor politice mari din SUA (http://en.wikipedia.org/wiki/Carnegie_Endowment_for_International_Peace). A se vedea în acest sens şi lista cu sponsorii care finanţează 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 autodefineşte ca promotoare a unui angajament global activ al S.U.A. şi caută să contureze formule de exercitare a unui leadership pozitiv şi constructiv al acestora la nivel global.

1. BĂHNĂREANU, Cristian (2005) *Puterea militară în secolul XXI. Modalităţi de realizare şi manifestare a puterii militare în societatea democratică românească*, Editura Universităţii Naţionale de Apărare, Bucureşti
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 şi de securitate*, Editura Centrului Tehnic – Editorial al Armatei, Bucureşti
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 EŞUATE 2013[1]

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	Dijbouti	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

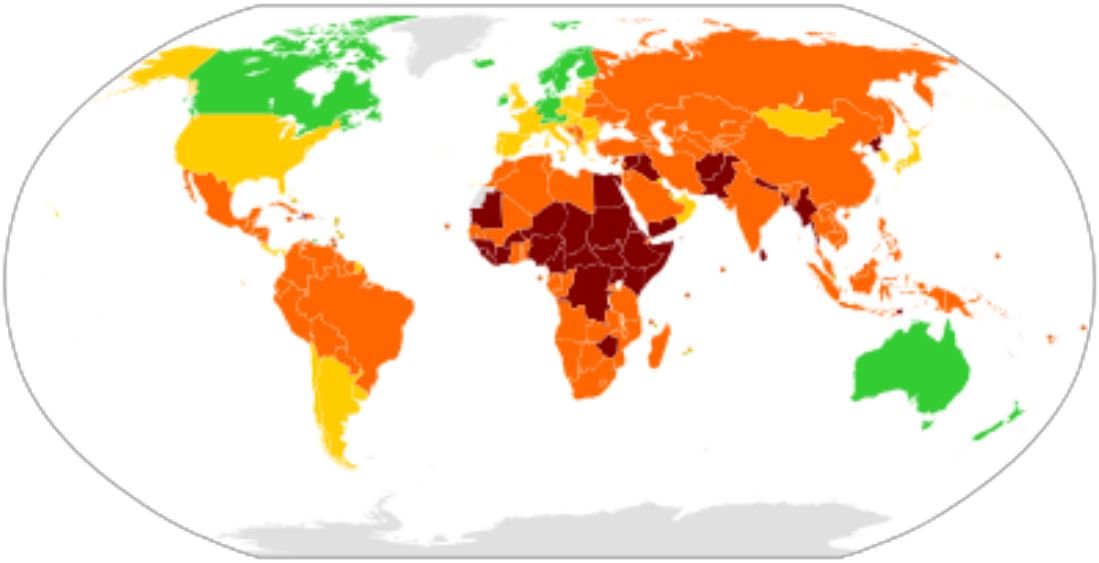
65	Tanzania	8.6	6.8	6.0	6.4	6.4	6.8	6.2	8.8	6.2	5.5	5.7	7.7	81.1
66	China	8.1	6.1	8.3	5.0	8.0	3.6	8.1	6.8	9.4	6.5	7.2	3.8	80.9
67	Israel/West Bank	6.2	7.4	9.8	3.2	7.5	3.7	6.7	5.9	7.6	7.1	8.1	7.7	80.8
67	Fiji	5.2	3.8	7.3	7.0	7.4	7.3	8.8	4.9	7.3	7.0	7.9	6.9	80.8
67	Bolivia	6.9	4.0	7.1	6.4	8.9	6.2	7.2	6.8	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

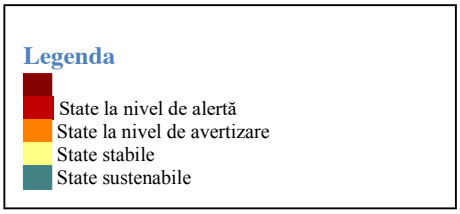
99	Gabon	6.8	5.6	3.3	5.5	7.3	5.2	7.6	7.0	6.8	5.4	7.1	5.4	72.9
101	Cuba	6.6	5.3	4.8	6.3	5.9	5.2	6.5	4.7	7.5	6.3	6.9	6.7	72.8
102	Saudi Arabia	5.5	5.2	7.4	3.1	6.4	3.6	7.8	4.0	8.9	7.2	8.0	5.6	72.7
103	Peru	5.9	4.7	7.0	6.1	7.8	4.1	7.1	6.4	5.0	7.0	6.7	4.5	72.3
104	Paraguay	6.1	2.4	6.5	4.9	8.6	5.1	7.9	6.1	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

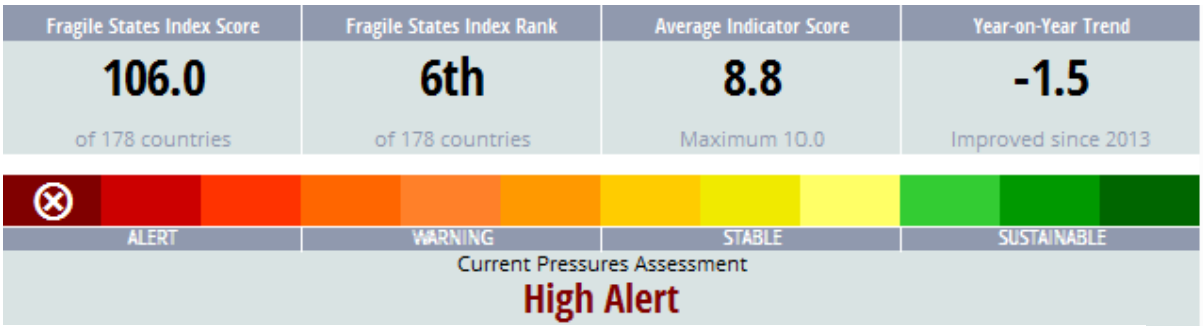
ANEXA NR. 2 – PLANIGLOB – TOPUL STATELOR EŞUATE 2013[1]



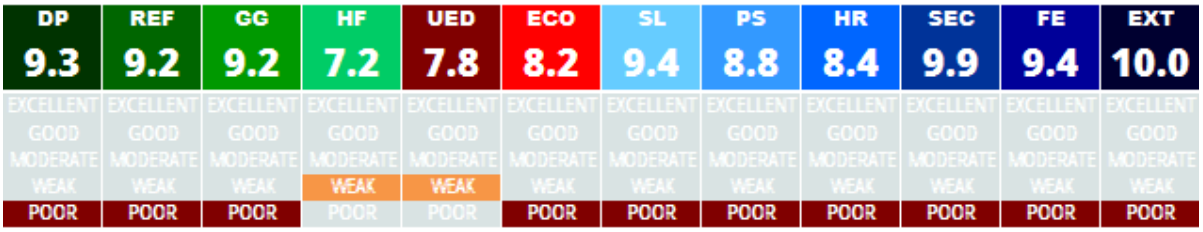


[1] http://ffp.statesindex.org/rankings-2013-sortable

ANEXA NR. 3 – OPȚIUNI DE VIZUALIZARE ALE CAST - AFGANISTAN[1]



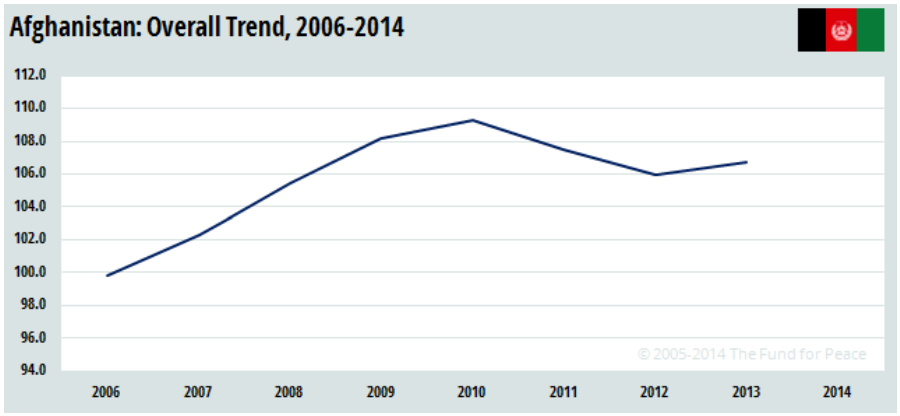
Indicator-by-Indicator in 2014

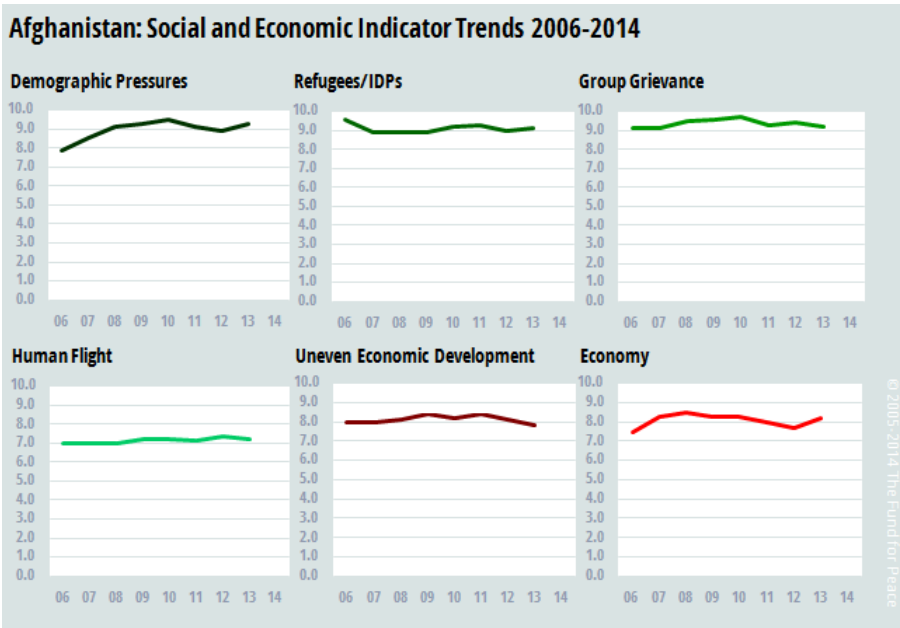


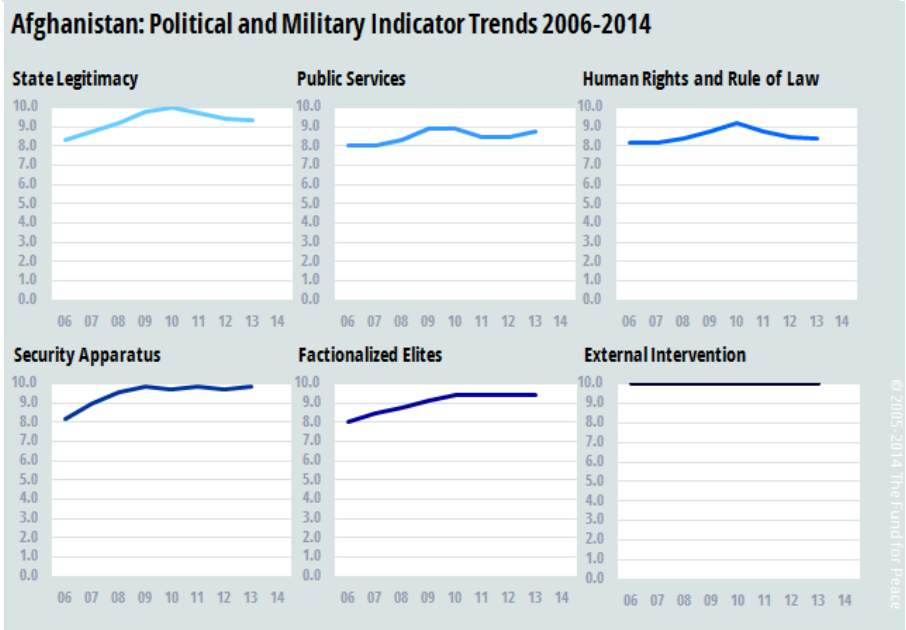
Year-on-Year Trend Since 2013

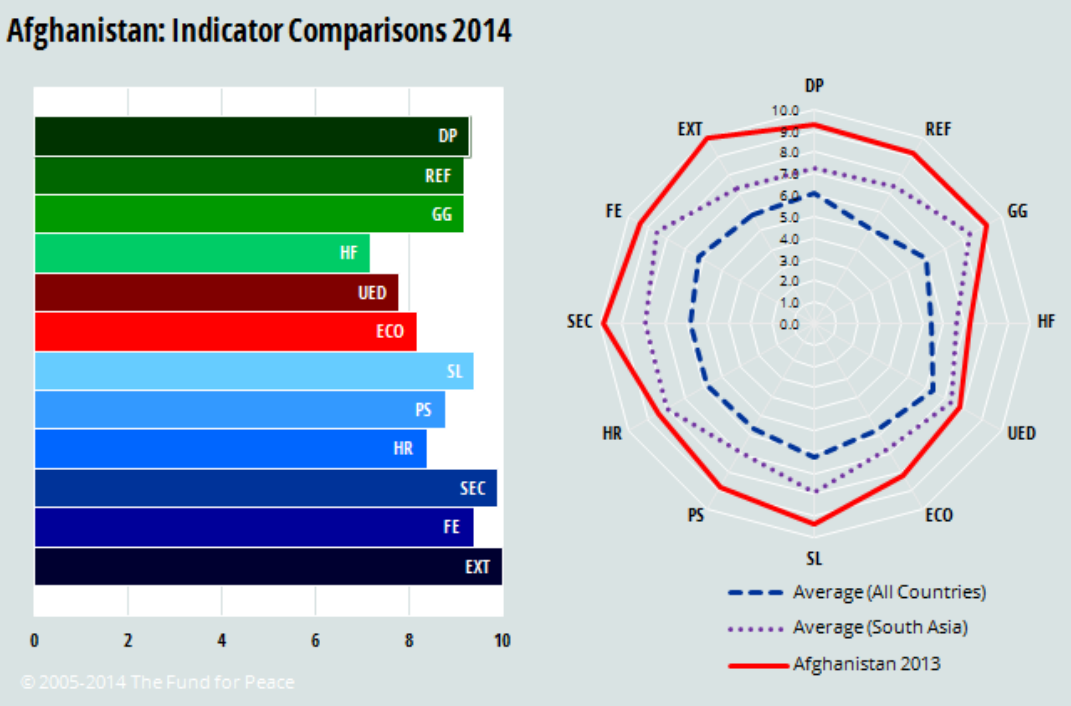
Five Year Trend Since 2009

[1] http://ffp.statesindex.org/afghanistan


Afghanistan: Overall Trend, 2006-2014
112.0
110.0
108.0
106.0
104.0
102.0
100.0
98.0
96.0
94.0
2006
2007
2008
2009
2010
2011
2012
2013
2014
© 2005-2014 The Fund for Peace


Afghanistan: Social and Economic Indicator Trends 2006-2014
Demographic Pressures
Refugees/IDPs
Group Grievance
Human Flight
Uneven Economic Development
Economy
© 2005-2014 The Fund for Peace


Afghanistan: Political and Military Indicator Trends 2006-2014
State Legitimacy
Public Services
Human Rights and Rule of Law
Security Apparatus
Factionalized Elites
External Intervention
© 2005-2014 The Fund for Peace


Afghanistan: Indicator Comparisons 2014
DP
REF
GG
HF
UED
ECO
SL
PS
HR
SEC
FE
EXT
0
2
4
6
8
10
© 2005-2014 The Fund for Peace
DP
REF
GG
HF
UED
ECO
SL
PS
HR
SEC
FE
EXT
10.0
9.0
8.0
7.0
6.0
5.0
4.0
3.0
2.0
1.0
0.0
Average (All Countries)
Average (South Asia)
Afghanistan 2013

CAPITOLUL 10. CENTRUL DE EXCELENŢĂ 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 capabilităților 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 Excelenţă 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 capabilităților NATO în condițiile reorganizării structurii de comandă militară a Alianţei şi 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 Excelenţă – MCM 236-03[1] – națiunile sunt încurajate să înființeze, într-un cadru stabilit şi în anumite condiţii, centre de excelenţă, instituții definite ca „entităţi naţionale sau multi-naţionale capabile să ofere expertiză şi experienţă recunoscută în sprijinul Alianţei, în special în sprijinul transformării". Centrele de Excelenţă sunt organizaţii militare internaţionale, în conformitate cuprevederile 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 competiţia cu capabilităţi 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. Acreditarea[2] Centrelor de Excelență presupune ca programul de lucru al acestora să fie în concordanţă 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 şi politicile de securitate ale NATO.

Înființarea reţelei Centrelor de Excelenţă NATO are multiple semnificaţii, atât pentru NATO, cât şi pentru naţiunile participante. Pe de o parte, Centrele gestionează proiecte și programe în sprijinul dezvoltării capabilităţilor existente,în ce privește managementul lecțiilor învățate/ bunelor practici, activitatea de analiză, dezvoltare conceptuală și standardizare, asigurând totodatăoportunităţi deosebite pentru procesul de educare şi instruire în NATO; pe de altă parte, participarea națiunilor la Centrele de Excelență, dincolo de contribuția asumată, are raţiuni şi interese bine justificate, avantajele imediate incluzând: asigurarea implementării viziunii şi reprezentării intereselor naţionale în produsele specifice, asigurarea accesului nemijlocit la dezvoltările de ultimă oră în domeniul funcţional şi la produsele specifice ale centrului, în condiții preferențiale. În plus, pe lângă vizibilitatea internațională şi la nivelul Alianţei, relația cu partenerii din cadrul Centrului permite dezvoltarea de proiecte comune, facilitând interacțiunile bilaterale şi multilaterale între naţiunile participante.

Funcţionarea centrelor de excelenţă acoperă, parţial sau în totalitate, o gamă largă de responsabilităţi ce se regăsesc în:

- sprijinirea forţelor NATO în vederea îmbunătăţirii capabilităţilor de planificare, pregătire şi conducere a operaţiilor;
- experimentarea, validarea şi implementarea unor noi concepte, tehnici, tactici şi proceduri, rezultate din procese de cercetare ştiinţifică sau ca bune practici/ lecţii învăţate din operaţii sau exerciţii;
- sprijinirea inovaţiei, a cercetării tehnice şi tehnologice în domeniile de responabilitate;
- furnizarea de produse şi servicii specifice procesului de standardizare (doctrine, standarde, proceduri, instrumente de evaluare, etc.), în sprijinind cerinţelor de interoperabilitate;
- asigurarea de expertiză pentru structurile NATO şi statele partenere;
- conturarea cadrului educaţional şi de instruire, individuală şi colectivă, în ariile funcţionale asumate.

[1]Conceptul Comitetului Militar pentru Centrele de Excelenţă NATO, din 04 decembrie 2003

[2] Condițiile necesare în acest sens sunt cuprinse în IMSM 0416-04, Criteriile de Acreditare pentru Centrele de Excelenţă 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 capabilităților 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 – trebuiesă fie mutual, iar inițiativa trebuie să găsească rezonanță la nivelul a cât mai multe națiuni care să se alăture proiectului.

În ce privește capabilitatea HUMINT în NATO, Grupul de Coordonare pentru Intelligence al Autorităţilor Militare NATO (NATO Military Authorities Intelligence Coordination Group - NMAICG) a identificat deficienţe în funcţionalitatea culegerii de informații din surse umane, fapt ce necesita o abordare coerentă şi structurată din partea naţiunilor aliate.

La acea dată, Armata Română îşi afirmase deja un corp de cadre experimentat, în condiţiile dezvoltării unor capabilităţi de lucru în comun cu structurile militare NATO în diferite teatre de operaţii (Kosovo, Bosnia, ulterior Irak şi Afganistan) şi dispunând de serviciile Direcţiei Generale de Informaţii a Apărării (DGIA), structură care s-a caracterizat prin viziune şi flexibilitate în prefigurarea şi construcţia unor capacități naţionale specifice, manifestând o prezenţă activă în cadrul grupurilor de coordonare şi a demersurilor lucrative în sfera informaţiilor militare în NATO[1].

Performanţele obţinute, profesionalismul recunoscut, interesul şi determinarea manifestate de către DGIA şi structurile subordonate în domeniul HUMINT au justificat angajamentul României în a se constitui ca naţiune-cadru a unui Centru de Excelenţă NATO cu obiect de activitate în domeniul informaţiilor din surse umane, candidatură acceptată de către NATO. Acestui demers i-a urmat un proces intens de pregătire a fundamentelor legale de înfiinţare a Centrului[2], precum şi negocierea participării la proiect a altor naţiuni NATO.

Documentele de bază elaborate în acest sens au fost: *Conceptul Centrului de Excelenţă*, care detaliază misiunea şi sarcinile asumate, precum şi viziunea privind dezvoltarea instituţiei ca pivot al transformării HUMINT în NATO, şi *Memorandumurile de Înţelegere Funcţional* şi *Operaţional*, care prevăd modalitatea concretă de funcţionare a Centrului. Acestea au fost semnate de către ACT, România şi primul grup de naţiuni participante – Grecia, Slovenia, Turcia şi Ungaria, la 16 decembrie 2009, la Norfolk/ SUA. Ulterior, acestora li s-a adăugat Slovacia, Polonia, Cehia şi SUA, procesul fiind în continuare deschis altor state membre NATO.

Centrul a fost înfiinţat în Oradea, în cadrul unei vechi cazărmi (foto 10.1) care a beneficiat de renovare completă, facilităţile existente fiind aduse la standardele calitative necesare unei astfel de instituţii, prin contribuția exclusivă a României în calitatea sa de națiune gazdă. Pe lângă infrastructura militară la dispoziţie, la baza alegerii locaţiei au stat şi o serie de caracteristici ale municipiului: un cadru social relativ cosmopolit, permisiv, posibilităţi de acces facil (locaţia vestică, infrastructura de transport existentă), condiţii de viaţă la standarde ridicate, posibilităţi de integrare socio-culturală pentru personalul străin.

[1]Detalii privind nivelul de implicare al DGIA în sfera dezvoltării capabilităţilor specifice se regăsesc în ediţia aniversară a publicaţiei direcţiei (Direcţia Generală de Informaţii a Apărării, *Infosfera* (revistă de studii de securitate şi informaţii pentru apărare), Anul I, nr. 3/2009, Bucureşti)

[2]Având la bază Decizia nr. 12 din 26 Iunie 2008 a Parlamentului României privind înfiinţarea pe teritoriul României a Centrului de Excelenţă NATO

Foto 10.1 Centrul de Excelenţă NATO în domeniul HUMINT din Oradea – intrarea de protocol

Pornindu-se de la o capacitate operaţională iniţială, au fost puse bazele funcţionale şi, în baza evaluării comisiei ACT, Centrul a obţinut statutul de organizaţie militară internaţională (conform prevederilor Protocolului de la Paris din 1952)[1], afiliată NATO.

Inaugurarea oficială a Centrului a avut loc la data de 16 martie 2010 şi a fost onorată de prezenţa Preşedintelui României, Traian Băsescu, a ministrului Apărării Naţionale, Gabriel Oprea şi a Şefului Statului Major General, amiral Gheorghe Marin, iar din partea ACT - locţiitorul comandantului acestui comandament strategic, amiralul Luciano Zappata[2]. (foto 10.2)

Foto 10.2 Inaugurarea Centrului de Excelenţă NATO în domeniul HUMINT din Oradea (16 martie 2010). Trecerea în revistă a gărzii de onoare de către Preşedintele României

Prin caracterul lor de noutate, fiecare etapă şi fiecare aspect al procesului de înființare a instituției au fost o provocare în sine, indiferent de natura lor – funcțională sau operațională: asigurarea infrastructurii, complianţa cu normele de securitate NATO, armonizarea legislativă (naţional vs. internaţional/ NATO), selecţia personalului, negocierile cu statele partenere, politica de relaţii publice şi promovare, asigurarea sprijinului logistic necesar, programul investiţional şi bugetarea, relaţia cu autorităţile 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/basictxt/b520828a.htm

[2] De asemenea, la eveniment au participat ambasadori şi ataşaţi militari acreditaţi la Bucureşti, reprezentanţi ai naţiunilor sponsor, generali şi ofiţeri din conducerea Ministerului Apărării Naţionale, precum şi reprezentanţi ai conducerii administraţiei publice judeţene şi locale, marcând importanţa evenimentului atât pentru mediul militar, cât şi pentru cel civil.

stabilirea relaţiilor de lucru cu alte structuri naţionale sau internaţionale, dezvoltarea comunității de interes în NATO, etc. Prin natura poziţiei deţinute şi a gradului de implicare pe care aceasta a presupus-o (şi o presupune), corelarea determinărilor funcţionale şi operaţionale cu nevoile de dezvoltare şi transformare ale NATO, precum şi identificarea comprehensivă a dimensiunilor de impact social, cultural, economic şi administrativ pe care înfiinţarea unui astfel de centru o are pe plan local, s-au dezvoltat într-o logică naturală.

Acest fapt a presupus o interacţiune susţinută cu factori de răspundere pe plan naţional (factorii de decizie politici şi militari, reprezentanţi juridici, eşaloanele militare superioare, elemente de sprijin administrativ-logistic, etc.), responsabilii NATO cu privire la gestionarea reţelei de transformare a Alianţei (TNB), precum şi cu reprezentanţii naţionali ai ţărilor 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 Excelenţă NATO în domeniul HUMINT – un exemplu de eficiență instituțională

Misiunea Centrului de Excelenţă NATO în domeniul HUMINT este de a furniza un punct de referinţă unic în NATO în ce priveşte activităţile de educare şi instruire, dezvoltarea de politici şi proceduri standardizate şi sprijinirea Alianţei în procesul de conturare a evoluţiei capabilităţilor 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 şi aprobat de către Comitetul Director, urmărind îndeplinirea lor din perspectiva a patru piloni de referinţă (corespunzând domeniilor acţionale ale transformării în NATO):

- analiză şi lecţii învăţate;
- dezvoltare conceptuală şi experimentare;
- doctrină şi standardizare;
- educaţie şi instruire.

În mod concret, personalul Centrului este implicat în cursuri, exerciţii, seminarii, grupuri de lucru, managementul documentelor de standardizare, experimente, activităţi de analiză, proiecte de cercetare ştiinţifică, toate contribuind la conturarea imaginii unei instituţii complexe, la nivelul căreia energiile se concentrează în mod sinergic în vederea asigurării unui înalt nivel calitativ al produselor şi serviciilor asigurate în cadrul Alianţei.

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 NATO[1], gestionează activitatea Comunității de Interes NATO pentru lecții învățate și bune practici în domeniul HUMINT.

La atingerea unui nivel de excelenţă în prestaţia Centrului contribuie în mod decisiv şi baza de relaţionare largă pe care instituţia a construit-o şi consolidat-o în timp scurt, printr-o politică pro-activă, prin disponibilitatea de angajament şi prioritizarea judicioasă a resurselor, asigurându-şi prezenţa şi fiind reprezentat la nivelul principalelor entităţi decizionale şi acţionale în domeniul de interes.

Astfel, pe lângă structurile de coordonare din cadrul Comandamentelor Strategice ale Alianţei, au fost stabilite relaţii de lucru în primul rând cu naţiunile aliate, cu structuri din cadrul comandamentelor operaţionale, cu centre de instruire NATO şi cu alte centre de excelenţă a căror activitate se interconectează la diferite niveluri de interes.

Având în vedere faptul că procesele de reformă şi transformare reclamă viziune, performanţă şi deschidere, trebuie să se ţină cont şi de necesitatea multiplicării domeniilor de expertiză ale personalului, asigurarea accesului acestora la medii care promovează confruntările de idei, facilitează înţelegerea procesualităţii fenomenelor şi permit aprofundări multidimensionale ale problematicilor de interes. Deschiderea şi interrelaţionarea cu mediul academic, dezvoltarea de parteneriate cu universităţi, *think-tank*uri, institute de cercetare, ONGuri, în cadrul unor proiecte specifice, asigură premizele necesare unor astfel de ”achiziţii” în materie de cunoaştere şi 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

Figura 10.4 Poster de prezentare a Centrului de Excelenţă NATO în domeniul HUMINT, destinat expunerii în cadrul evenimentelor academice

Centrul de Excelenţă NATO în domeniul HUMINT – perspective de integrare instituţională

Integrarea instituţională reprezintă o adevărată provocare pentru orice organizaţie nou apărută, în orice mediu de referinţă. În acest sens, factorii manageriali ai instituţiei trebuie să gestioneze două direcţii funcţionale de integrare, una aparţinând de structura şi relaţiile interioare, iar cealaltă ţinând de integrarea externă într-un sistem - sau sisteme - funcţionale superioare (Simion, 2012).

În ce priveşte funcţionarea internă, principalele referinţe rezidă într-o ”construcţie” interdependentă de oameni, procese şi tehnologii (incluzând procedurile de lucru). Într-o abordare sistemică, intrările şi ieşirile (resurse şi proceduri vs. produs) este, de asemenea, contabilizată. În final, tipul organizaţiei şi scopul acesteia defineşte şi determină modul de abordare a analizei instituţionale.

Din punct de vedere funcţional, Centrul de Excelenţă NATO în domeniul HUMINT realizează un ciclu complet de procese menite să contribuie la activitatea de sprijin a dezvoltării capabilităţii HUMINT: de la culegerea şi procesarea de lecţii identificate şi asimilarea de bune practici, dezvoltarea şi experimentarea de noi concepte, transpunerea rezultatelor activităţii analitice şi de cercetare în politici, doctrine, proceduri şi, în final, transferul de cunoştinţe şi dezvoltarea de abilităţi prin intermediul activităţii de educare şi instruire.

Din punct de vedere al cadrului sistemic, subliniem o primă conexiune a organizaţiei cu entităţile externe. Organizaţiile fiind, în general, caracterizate de procese complexe, dinamice, orientate spre obiective, ne putem asuma raportul dintre ”intrări” (sarcinile internalizate şi asigurarea resurselor) vs. ”ieşiri” (produsul) ca o importantă caracteristică de integrare instituţională, atât în ce priveşte indicatorii calitativi, cât şi cei cantitativi. Din acest punct de vedere, putem marca un pas decisiv către integrarea instituţională la parametri maximali: în conformitate cu documentele sale constitutive, Centrul de Excelenţă NATO în domeniul HUMINT şi-a constituit propriul program de lucru în baza cererilor de suport ale Alianţei, centralizate de către structura directoare a Reţelei de Transformare, fiind totodată deschis cererilor particulare ale naţiunilor participante sau ale altor beneficiari din cadrul NATO. În ce priveşte resursele, toate piesele angrenajului – buget, personal, proceduri, reţele de interconectare, tehnologii, etc. sunt clar specificate în documentele constitutive, precum şi în legislaţia naţională (luând în considerare localizarea Centrului) şi asigurate astfel încât să contureze premisele necesare şi condiţiile optime desfăşurării activităţii specifice.

Pe de altă parte, pentru o mai bună înţelegere a adaptării organizaţiei la mediul de acţiune, teoria complexităţii ne oferă o perspectivă a unei sume de strategii şi structuri ce facilitează integrarea ”întregului” (organizaţia în sine) prin contabilizarea performanţelor conective ale substructurilor componente.

În consecinţă, pentru o organizaţie militară, unde independenţa de acţiune a sub-sistemelor componente este puternic limitată şi controlată de către reguli specifice, se impune o strategie adecvată care să potenţeze la maxim oportunităţile şi iniţiativele palierelor subordonate, succesul lor transpunându-se în succesul organizaţiei.

Asumându-ne suficientă flexibilitate la nivelul managementului Centrului de Excelenţă NATO în domeniul HUMINT şi o viziune clară privind rolul şi viitorul instituţiei, putem afirma că sub-structurile acestuia au fost astfel direcţionate încât să contribuie, atât individual cât şi în cadrul efortului comun, la realizarea racordării cu structurile relevante ale Alianţei; schema organizatorică a Centrului (figura 10.5) este ea însăşi concepută astfel încât să asigure o conectare specializată, corespondentă pilonilor transformării în NATO, cu branşele responsabile din cadrul comandamentelor strategice şi cele operaţionale, precum şi cu alte structuri aliate angrenate în procesul de dezvoltare a capabilităţilor militare ale Alianţei –

Centrul pentru Lupta Întrunită (Stawanger, Norvegia), Centrul de Instruire al Forţelor Întrunite (Bydgoszcz, Polonia), Centrul de Analiză Întrunită şi Lecţii Învăţate (Monsato, Portugalia), etc.

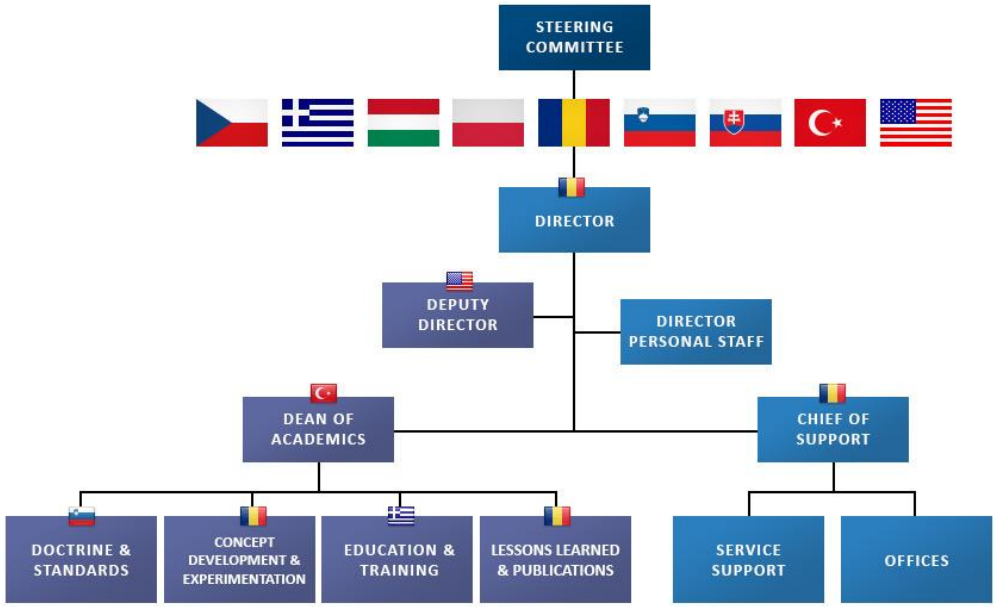


Figura 10.5 Organigrama Centrului de Excelenţă NATO în domeniul HUMINT
(http://www.natohcoe.org/en/organisational_chart/)

Din perspectiva dezvoltării obiectului de activitate a Centrului – capabilitatea HUMINT în NATO – unul dintre obiectivele prioritare ale instituţiei este constituirea unei comunităţi de interes în domeniul HUMINT care să se coaguleze în jurul Centrului de Excelenţă din Oradea, interesând structuri NATO, naţiuni şi alte organizaţii, şi având ca scop constituirea unui forum de dezbateri şi dezvoltarea de activităţi menite să asigure informarea reciprocă a participanţilor în legătură cu acţiuni, evenimente, evoluţii semnificative în domeniu (prin acţiuni formale ca: publicarea unui buletin informativ, gestionarea unei pagini web dedicate, organizarea de conferinţe şi 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 capabilității HUMINT în NATO:

- **2009:** HCOE devine gazda permanentă a exerciţiului NATO pentru HUMINT;
- **2010:** HCOE demarează procesul de instruire de specialitate, derulând până în 2015 peste 40 iteraţii a 5 cursuri de specialitate distincte;
- **2011:** directorul HCOE preia preşedinţia Grupului de lucru NATO pentru HUMINT (NHWG), ulterior şi a Grupului de lucru NATO pentru tehnologie HUMINT (NHTWG);
- **2011:** HCOE preia custodia Doctrinei NATO pentru HUMINT (AJP-2.3) şi a publicaţiei NATO pentru procedurile HUMINT (AIntP-5);
- **2013:** în cadrul procesului de reformare a politicilor de educaţie şi instruire în NATO şi alinierii la standardele civile (procesul Bologna), instituţiei noastre îi este conferit "*sigiliul calităţii*" de către autoritatea responsabilă (Joint Force Trainer) din cadrul Comandamentului Aliat pentru Transformare, ca recunoaştere a calităţii

infrastructurii, sistemelor, proceselor şi procedurilor de lucru, a managementului şi 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 educaţia şi instruirea în domeniul HUMINT în NATO.

Dincolo de aspectele funcționale legate de obiectul de activitate, Centrul de Excelenţă NATO în domeniul HUMINT s-a făcut remarcat în cadrul Reţelei de Transformare NATO ca o organizaţie pro-activă, participând la toate evenimentele importante din domeniul HUMINT sau legate de aspecte concrete ale conectării sale la pulsul Alianţei, fiind reprezentat în cadrul a diferite proiecte[1], grupuri şi ateliere de lucru, foruri de coordonare şi standardizare, etc.

Depăşind specificitatea câmpului de expertiză şi a ariei de interes a Centrului de Excelenţă din Oradea, dezvoltarea sa ca organizaţie bazată pe cunoaştere prin integrarea viziunii, politicii şi cerinţelor NATO în materie de management al cunoaşterii informaţiei, adoptate şi adaptate ca fundament al propriilor necesităţi de schimb de informaţii, reprezintă un element de maximă importanţă pentru integrarea instituţională completă.

Centrul de Excelenţă NATO în domeniul HUMINT – relevanţa locală, naţională şi regională. Consideraţii privind perspectivele de integrare instituţională multispectrală (socială, economică, culturală)

Din punct de vedere strategic, decizia politico-militară de poziţionare a României ca naţiune-cadru pentru dezvoltarea Centrului de Excelenţă NATO în domeniul HUMINT reflectă viziunea unui angajament coerent al ţării în angrenajul aranjamentelor de securitate asumate odată cu intrarea în Alianţa Nord-Atlantică, eveniment cu profunde semnificaţii 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 relaţiilor bilaterale în diferite domenii ale câmpului larg al securităţii şi creşterea nivelului de coeziune în asumarea obiectivelor promovate în cadrul NATO sau a unor iniţiative regionale.

La nivel naţional, Centrul de Excelenţă NATO în domeniul HUMINT reprezintă un adevărat paşaport de calitate al instituţiei Armatei Române, iar imaginea sa a fost folosită (alături de alte repere relevante[2]) ca argument al importanţei contribuţiei României la eforturile Alianţei în câmpul securităţii, într-un material video ("*What NATO means for us*" – "*Ce înseamnă NATO pentru noi*") parte a campaniei de diplomaţie publică a Alianţei[3]. 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 mândreşte şi prin intermediul cărora îşi asigură o poziţie relevantă în peisajul capabilităţilor NATO.

***

Dincolo de prestigiul internaţional şi de relevanţa politică pe care existenţa Centrului de Excelenţă o are în plan naţional, la nivel local se înmulţesc în mod semnificativ şi se diversifică implicaţiile legate de integrarea instituţională.

---

1 A se vedea, ca exemplu, contribuţia adusă în cadrul experimentului legat de dezvoltarea conceptului de Contracarare a Ameninţărilor Hibride (Counter Hybrid Threats) – în https://transnet.act.nato.int/WISE/CHTIPT/Newsletter/AprilNewsl/file/_WFS/CHT%20Newsletter%20-%20Edition%202%20-%20final.pdf

[2]Principalele realizări ale Armatei Române în relaţia cu NATO sunt prezentate sintetic de către ministrul Apărării Naţionale, Gabriel Oprea, în articolul "*Armata şi interesul naţional*" din revista Infosfera, Anul II, nr. 2/2010, p. 3-8

[3]http://www.mae.ro/en/node/6038

Încă de la înfiinţarea sa, Centrul de Excelenţă din Oradea a provocat imaginaţia populaţiei locale (şi nu numai). Descrierea sa ca „*centru de instruire pentru spionii NATO*" a prevalat în mass-media[1] - dar în timp relativ scurt latura spectaculoasă a acestei imagini s-a disipat, iar localnicii au realizat ce reprezintă cu adevărat Centrele de Excelenţă NATO (şi, în mod special, cel găzduit de oraşul de pe Crişul Repede).

În continuare, vom contura o serie de abordări pe care aspecte legate de integrarea funcţională a instituţiei pe plan local le determină.

În primul rând, în zona furnizării de servicii (fără a lua în considerare cheltuielile de mentenanţă aferente funcţionării cazărmii), străinii care intră în relaţii de lucru cu Centrul de Excelenţă (într-un număr considerabil, ca medie lunară) şi, totodată, profită de această oportunitate pentru a vizita Oradea (eventual şi împrejurimile) sunt excelenţi consumatori. Ei folosesc hoteluri de bună calitate, care furnizează servicii complexe, închiriază autoturisme, se bucură de zonele de relaxare (restaurante, pub-uri, staţiunile cu băi termale – Băile Felix şi 1 Mai) şi vizitează obiective culturale de interes.

În acest sens, Centrul este în permanenţă preocupat să contribuie la orientarea corectă a oaspeţilor săi, care devin şi oaspeţi ai oraşului. În cadrul activităţilor de lucru, instituţia asigură colaboratorilor prezentări generale ale locaţiei, oraşului şi zonelor înconjurătoare, face recomandări legate de specificul local, furnizează hărţi de buzunar, direcţionează oaspeţii în funcţie de intenţiile exprimate ale acestora, desfăşoară activităţi de însoţire/ ghidare în cadrul unor scurte tururi turistice la principalele obiective de interes. În acest sens, dispunând de o balanţă oarecum disproporţionată a timpului liber faţă de cel dedicat activităţilor profesionale în favoare acestora din urmă, ne bazăm pe referinţe caracterizate de calitate şi atractivitate; aceste trăsături vor constitui motive de promovare mai departe, în cercul apropiaţilor, a unor argumente menite să determine reîntoarcerea lor ca turişti, însoţiţi de familie şi prieteni.

Este evident faptul că sunt încă multe de făcut în ce priveşte potenţarea şi scoaterea în evidenţă a caracteristicilor culturale ale zonei (managementul şi marketingul profesionist al potenţialului turistic cu accent pe obiective şi evenimente culturale), conectarea acestora la alte evenimente, crearea de parteneriate reciproc avantajoase, a unui pachet de oferte care să asigure tururi de cunoaştere complexe[2]; ne orientăm, într-o primă fază, asupra disponibilităţii Muzeului "Ţării Crişurilor", a Muzeului Militar şi a Cetăţii Oradei (în proces de renovare), urmărindşi o valorificare superioară a diferite festivaluri, zile comemorative sau sărbători. În acest sens, parteneriatul cu organele administraţiei publice, factorii de răspundere instituţionali, organizaţii neguvernamentale ar fi mai mult decât util.

O promovare originală a obiceiurilor culinare locale are loc cu ocazia activităţilor specifice care întrunesc un număr mai mare de persoane, când hrănirea este asigurată în regim de catering, într-o concepţie care nu presupune doar simpla asigurare a hranei, ci constituie o excelentă oportunitate de a servi feluri de mâncare specifice zonei. Acest fapt este deosebit de apreciat de vizitatori, care ajung chair să înveţe denumirile în limba română a felurilor preferate. În acest sens, parteneriatul Centrului cu furnizorii de servicii în domeniul hrănirii reprezintă o caracteristică integraţională importantă în acest domeniu economic, asigurând predictibilitate, relaţii de colaborare îmbunătăţite şi o calitate constantă a prestaţiilor, în condiţii 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

[2] În general, Centrele de Excelenţă NATO nu acordă o atenţie deosebită acestui aspect, însă considerăm că o manifestare pro-activă în acest sens reprezintă nu numai o datorie faţă de comunitate, ci şi o oportunitate pentru scoaterea în evidenţă a ofertei socio-culturale a oraşului, fapt de maxima importanţă în evaluarea condiţiilor generale de trimitere la post a personalului civil.

Pornind de la necesitatea focalizării pe performanţă ca trăsătură a excelenţei, 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 experţi în câmpuri de interes comun întărind reciproc calitatea şi atractivitatea diferitelor evenimente în care instituţia este parte.

Un proiect de interes public, gestionat de Centrul de Excelență, este un demers finanţat de către structura NATO focalizată pe provocările emergente în materie de securitate (Emerging Security Challenges Division/ ESCD), intitulat "*Aspecte umane ale mediului operaţional*" (Human Aspects of the Operational Environment - HAOE). Centrul asigură directoratul proiectului şi nucleul de lucru de bază, colaborând cu experţi politici şi militari, consilieri culturali, antropologi, sociologi, istorici, specialişti în comunicare, reprezentanţi ai organizaţiilor neguvernamentale, etc. din străinătate şi din ţară[1].

Scopul proiectului este de a asigura suport pentru o mai bună înţelegere a caracteristicilor populaţiei din zonele de conflict şi să asigure fundamentul pentru un posibil concept major al NATO în acest domeniu. Studiul se concentrează la nivelul strategic şi operaţional, fără a exclude însă unele implicaţii la nivel tactic[2].

Acesta a reprezentat şi o excelentă oportunitate de a implica mediul academic militar prin organizarea unui atelier de lucru pe această temă în cadrul Conferinţei Internaţionale "The Knowledge – Based Organization/ KBO 2012", organizat de Academia Forţelor Terestre "Nicolae Bălcescu" din Sibiu.

Nevoia de performanţă în activitate îşi găseşte rezonanţa începând de la nivel individual. Personalul Centrului este activ implicat în dezvoltarea propriei pregătiri academice, urmând programe de masterat şi doctorat în diferite domenii (în acest caz, abordările interdisciplinare care antrenează domeniul fundamental al ştiinţelor militare şi informaţiilor, fiind în măsură să asigure spaţiul necesar contribuţiilor de valoare exploatabile în activitatea profesională). Totodată, aceştia participă la conferinţe, sesiuni de comunicări şi ateliere de lucru, proiecte de cercetare, etc., urmărind obiective de dezvoltare personală ce contribuie decisiv la creşterea capacităţii intelectuale, a volumului de cunoaştere şi expertiză şi, în cele din urmă, a calităţii prestaţiei profesionale. Principalele instituţii cu care se colaborează în acest sens sunt: Universitatea din Oradea, Academia Forţelor Terestre "Nicolae Bălcescu" din Sibiu, Colegiul Naţional de Apărare "Carol I" Bucureşti, Universitatea "Lucian Blaga" din Sibiu, Universitatea Națională pentru Intelligence (SUA).[3]

***

[1]În perioada 6-8 Septembrie 2011 a avut loc primul atelier de lucru, în Oradea, la care au participat 20 de experţi în domeniile de interes identificate reprezentând instituţii şi organizaţii de renume din diferite ţări NATO şi 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 Excelenţă 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.

[2]În acest sens, următoarele direcţii de analiză au fost considerate ca necesare: principalii factori motivatori ai acţiunilor umane; determinarea profilului comunităţii; comunicarea interculturală; dinamica situaţiei locale; percepţia şi acceptarea operaţiilor/misiunilor NATO; indicatori măsurabili ai atitudinii populaţiei privind operaţiile NATO; Aspectele Umane în Planificarea Operaţională.

[3]Toate Centrele de Excelenţă NATO abordează cu deosebită seriozitate relaţia cu mediul academic, datorită naturii activităţii lor predilect intelectuale, cu concretizare în sfera educării şi instruirii, dezvoltării conceptuale şi cercetării.

Există o serie întreagă de alte aspecte care pot fi abordate din perspectiva unei mai bune integrări în plan local, atât la nivel instituţional, cât şi la nivel social – având în vedere nevoile specifice ale personalului internaţional al Centrului. Pornind de la multiculturalismul zonei – un cadru excelent pentru adaptarea personalului străin şi a familiilor acestora cu un mediu social tolerant, pot fi lansate întrebări legate de capacitatea sistemului de învăţământ (şi reprezentarea sa la nivel local) de a asigura o ofertă cu adevărat utilă din punct de vedere al cerinţelor pieţei educaţionale.

Dacă învăţământul în limbile maghiară şi germană este bine reprezentat, ar trebui ca factorii de răspundere din domeniul educaţiei să realizeze şi nevoia de asigurare a acestor servicii în limba engleză, făcâd facilitatea de educaţie accesibilă unei plaje mult mai largi de clienţi (familiile investitorilor străini pe plan local, ale personalului străin aflat la post – cum e cazul Centrului de Excelenţă, dar şi elevilor şi studenţilor orădeni care urmăresc să îşi dezvolte competenţe care să le asigure succesul dezvoltării profesionale viitoare într-o luma caracterizată de uniformizarea generată de presiunile integraţioniste ale globalizării).

***

Concluzionăm că, pentru Oradea, înfiinţarea Centrului de Excelenţă reprezintă o oportunitate unică pentru promovarea sa în exterior, în spaţiul de interes NATO.

Municipiul capătă notorietate prin relaţiile de lucru pe care Centrul le derulează cu o multitudine de structuri NATO sau organizaţii naţionale şi internaţionale active în câmpul securităţii şi în mediul academic. Oradea (şi judeţul Bihor) sunt promovate cu ocazia tuturor evenimentelor găzduite de către Centru, dar şi de către delegaţii Centrului participanţi la diferite activităţi în afară. Mai mult, toate referirile la Centrul de Excelenţă NATO în domeniul HUMINT care se fac în comunitatea Alianţei Nord-Atlantice se leagă de oraşul gazdă - Oradea, detalii despre acesta fiind făcute cunoscute prin prezentări postate pe websiteul NATO şi pe pagina web a Centrului, toate cu scopul de a contribui la cunoaşterea sa pe plan internaţional.

Condiţionările de securitatea activităţilor specifice se transpun şi în planul relaţional al Centrului de Excelenţă NATO din Oradea, limitând interacţiunea în domeniul specific de expertiză la nivelul comunităţii de interes HUMINT din cadrul Alianţei. Cu toate acestea, instituţia nu este izolată de mediul civil, dezvoltând şi participând în mod activ la proiecte deschise publicului larg, promovând cultura de securitate a Alianţei Nord-Atlantice şi urmărind dezvoltarea prezenţei sale în comunitatea academică prin punerea în valoare a potenţialului uman de care dispune.

Concluzii

O abordare cuantificabilă a determinării în materie de securitate demonstrează că Alianţa Nord-Atlantică este una dintre organizaţiile cu cea mai mare deschidere în ce priveşte asumarea de responsabilităţi în câmpul de referinţă conceptual al securităţii. Nevoia de transformare[1] 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) şi, subsecvent, de căutarea rolului Alianţei în acest context, cât şi de noile provocări în materie de securitate.

[1]Transformarea, după cum o vede John J. Garstk, înseamnă o schimbare susţinută, coerentă, care urmăreşte realizarea obiectivului strategic de a crea sau menţine un avantaj în cadrul competiţiei sau de a anihila avantajul unui adversar nou sau deja existent. Conceptul este relevant pentru organizaţiile confruntate cu provocări şi oportunităţi care nu pot fi abordate în mod real prin metodologiile consacrate, pentru a putea aduce îmbunătăţiri incrementale organizaţiilor, proceselor, tehnologiilor, managementului resurselor umane şi modelelor de afaceri existente. (Garstk, 2005)

La nivelul Alianţei, transformarea constă, în fapt, într-o sumă de iniţiative lansate progresiv şi care se dezvoltă complementar (Bell, 2005), în corelaţie şi influenţându-se reciproc cu procesul de reformare a altor organizaţii relevante în câmpul securităţii. Transformarea în NATO a fost pozitiv influenţată de dezvoltarea Politicii Europene de Securitate şi Apărare; în acelaşi timp, forma şi eficacitatea viitoare a Organizaţiei Naţiunilor Unite sunt importante pentru NATO, deoarece mandatul ONU reprezintă, de multe ori, o precondiţie pentru ca mulţi dintre aliaţii europeni să ia în considerare folosirea forţei (Riecke, 2005).

În cadrul organizaţiei militare, transformarea implică schimbări la nivelul doctrinelor, organizării şi structurii forţelor, a activităţii de informaţii, instruirii, educaţiei şi achiziţiilor, managementului personalului şi programării bugetare; acestea devin domenii principale de aplicare a transformării în domeniul militar, care se reflectă, ca efort şi resurse, la nivelul tuturor naţiunilor aliate.

Este important de subliniat rolul pe care Conceptul Strategic adoptat la Summitul de la Lisabona, dar și recentele decizii determinate de provocările din flancul estic al Alianței îl joacă în procesul decizional al NATO, ca referinţă privind finalitatea efortului depus în slujba securităţii, promovând consensul transatlantic şi imaginea unei organizaţii transparente şi coerente. Direcţiile trasate prin Conceptul Strategic constituie un adevărat vector al orientării sarcinilor de transformare a structurilor şi capabilităţilor 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 capabilităţile Alianţei pentru implementarea acestor cerinţe sunt relativ limitate, în special în ce le privește pe cele legate de educaţie şi instruire, este de aşteptat ca rolul Centrelor de Excelenţă NATO să crească exponenţial, acestea având atât capacitatea, cât şi cadrul legal flexibil pentru a răspunde cererilor de sprijin adresate de comandamentele NATO în cadrul procesului de transformare.

Prin activitatea lor, Centrele de Excelenţă NATO caută să devină principalii agenţi ai transformării în ariile de expertiză care le corespund prin dezvoltarea, promovarea şi implementarea de politici, concepte şi noi strategii în scopul creşterii calitative a capabilităţilor operaţionale şi atingerii obiectivelor de interoperabilitate propuse.

Produsele Centrelor de Excelenţă sunt compliante cu scopul final al procesului de transformare în NATO: capabilităţi îmbunătăţite, interoperabilitate crescută şi întărirea valorilor comun împărtăşite, totul aliniat viziunii strategice şi politicilor de dezvoltare ale Alianţei, contribuind în mod plenar la programul ”Smart Defence”.

Este important să observăm că domeniile transformării în NATO vor purta, astfel, amprenta predilectă a naţiunilor înregimentate în cadrul centrelor. În această logică, o largă participare şi reprezentare în clubul centrelor de excelenţă va asigura o acceptabilitate şi legitimitate sporită a produselor acestora, constituindu-se, în egală măsură, într-o oportunitate care să permită manifestarea valorilor, experienţei acumulate, bunelor practici şi lecţiilor învăţate ale naţiunilor.

Pe lângă faptul că se constituie în adevăraţi ambasadori ai mesajului NATO în cadrul propriilor comunităţi de interes, sprijinind o mai bună aprofundare a viziunii şi rolului asumat de către Alianţă în plan internaţional, participarea naţiunilor la centrele de excelenţă este o şansă de manifestare a propriilor puncte forte şi de promovare a imaginii naţionale.

România beneficiază din plin de aceste oportunităţi, în calitate de naţiune cadru şi gazdă a Centrului de Excelenţă NATO în domeniul HUMINT. Prin calitatea produselor sale, centrul este un excepţional promotor al imaginii ţării şi instituţiei militare naţionale în primul rând în cadrul NATO, dar şi în plan internaţional lărgit. Mai mult, prezenţa centrului de excelenţă are semnificaţii deosebite şi pe plan local, poziţionarea sa în ansamblul instituţiilor

publice şi integrarea într-un cadru social specific generând o serie de abordări de real interes pentru o multitudine de actori.

Centrul de Excelenţă NATO HUMINT din Oradea reprezintă deja un model şi exemplu de urmat pentru iniţiative similare, naţionale sau aparţinând unor structuri instituţionale ale altor state. Abordarea structurată pe care o urmăreşte tema propusă poate deschide astfel de orizonturi şi pentru alte entităţi interesate, atât în ce priveşte gestionarea unei astfel de instituţii, cât şi stabilirea de relaţii în arii funcţionale de interes comun cu Centrele de Excelenţă 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/basictxt/b520828a.htm
2. BELL, Robert, (2005) *Fişa transformării NATO*, în http://www.nato.int/docu/review/2005/issue1/romanian/summaries.html
3. Conceptul Comitetului Militar pentru Centrele de Excelenţă NATO, din 04 decembrie 2003
4. Decizia nr. 12 din 26 Iunie 2008 a Parlamentului României privind înfiinţarea pe teritoriul României a Centrului de Excelenţă NATO
5. Direcţia Generală de Informaţii a Apărării, *Infosfera* (revistă de studii de securitate şi informaţii pentru apărare), Anul I, nr. 3/2009 și Anul II, nr. 2/2010, Bucureşti
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 Excelenţă 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/AprilNewsl/file/_WFS/CHT%20Newsletter%20-%20Edition%202%20-%20final.pdf
14. www.natohcoe.org

CAPITOLUL 11. INTELLIGENCE ŞI AMENINȚĂRILE DIN MEDIUL CIBERNETIC

Securitatea cibernetică – domeniu de referință pentru Intelligence în domeniul cibernetic

Tehnologiile digitale, sistemele informatice, bazele de date, conexiunile în reţele, Internetul, toate au devenit esenţiale vieţii moderne, devenind o extensie virtuală a acesteia, un spațiu de manifestare a tuturor aspectelor funcționale ale proceselor, evenimentelor, relaționărilor din toate domeniile.

Strategia de securitate cibernetică a României definește spațiul cibernetic ca *mediu virtual, generat de infrastructurile cibernetice, incluzând conţinutul informaţional procesat, stocat sau transmis, precum şi acţiunile derulate de utilizatori în acesta;* spațiul cibernetic se caracterizează prin lipsa frontierelor, dinamism şi anonimat, generând deopotrivă oportunităţi de dezvoltare a societăţii informaţionale bazate pe cunoaştere, dar şi riscuri la adresa funcţionării acesteia (la nivel individual, statal şi chiar cu manifestare transfrontalieră) *(Strategia de securitate cibernetică a României, 2013).*

Odată cu dezvoltarea spectrului cibernetic, vulnerabilităţile specifice (probleme tehnice, imperfecţiuni de software, sisteme de protecţie 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 cibernetice au devenit tot mai frecvente şi mai organizate, nivelul pagubelor în ce priveşte activitatea administraţiei de stat, afacerile, domeniul economic, transporturile şi reţelele de aprovizionare sau ameninţările asupra infrastructurii critice atingând cote înalte, în măsură să ameninţe prosperitatea, securitatea şi 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 cibernetice (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 şi reactive[1] prin care se asigură confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi nonrepudierea informaţiilor în format electronic, a resurselor şi serviciilor publice sau private, din spaţiul 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 reţelelor informatice şi de comandă, control şi comunicaţii ale Alianţei sau în dezvoltarea capacităţilor de răspuns la agresiunile cibernetice exercitate asupra statelor membre.

[1]Acesteainclud, întrealtele:politici, concepte, standardeşighiduri de securitate, managementulriscului, activităţi de instruireşiconştientizare, implementarea de soluţiitehnice de protejare a infrastructurilorcibernetice, managementulidentităţii, managementulconsecinţelor

Încă din anul 2000, Alianţa a recunoscut importanţa protecţiei infrastructurilor informatice critice împotriva atacurilor cibernetice, această problematică apărând pentru prima dată pe agenda summitului de la Praga din 2002 şi fiind reconfirmată în reuniunea de la Riga, în 2006.

Atacurile cibernetice asupra Estoniei, în aprilie şi mai 2007, au dus la executarea de evaluări privind locul şi rolul Alianţei 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 Bucureşti.

Conceptul Strategic NATO din 2010[1] a luat în considerare necesitatea ca Alianţa să-şi accelereze eforturile de prevenire, detectare şi apărare în domeniul cibernetic, precum şi sprijinirea refacerii rapide a ţărilor membre după astfel de atacuri. Aplicarea metodologiei procesului de planificare NATO în acest domeniu ar fi de natură să asigure coordonarea capabilităţilor naţionale de securitate cibernetică, asigurând un nivel superior de informare, avertizare şi răspuns în cadrul protecţiei cibernetice centralizate.

La 8 iunie 2011, NATO a aprobat o Politică revizuită privind Apărarea în Domeniul Cibernetic şi un Plan de Acţiune pentru implementarea acesteia, urmate de:[2]

- stabilirea elementelor critice ale capacităţii operaţionale depline a sistemului NATO de răspuns la incidente în reţelele 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 şefilor de state şi guverne, la summitul de la Chicago din mai 2012[4], de a îmbunătăţi nivelul de apărare cibernetică în cadrul Alianţei prin punerea în comun a reţelelor NATO sub protecţie centralizată[5] (responsabilitate preluată de către Agenţia NATO pentru Comunicaţii şi Informaţii - NCI, din iulie 2012) şi îmbunătăţirea parametrilor NCIRC;
- instalarea în aprilie 2013 a infrastructurii de bază pentru gestionarea apărării reţelelor şi a capabilităţii analitice la Centrul Tehnic al NCIRC în Mons, Belgia;
- în cadrul primei întâlniri a miniştrilor apărării din NATO dedicată exclusiv apărării cibernetice (la 4 iunie 2013) a fost stabilită crearea Echipelor de Reacţie Rapidă pentru protejarea sistemelor NATO în cadrul NCIRC, precum şi dezvoltarea procedurilor de sprijin şi asistenţă din partea NATO pentru naţiunile aliate ce solicită asistenţă în caz de atac cibernetic[6].
- 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 tuturor[7]; 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.

[1]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

[2]http://www.nato.int/cps/en/natolive/topics_78170.htm

[3]Centrul de coordonare a NCIRC se află la comandamentul NATO din Bruxelles

[4]http://www.nato.int/cps/en/natolive/events_84074.htm

[5]Infrastructura critică naţională rămâne o responsabilitate a naţiunii respective, care trebuie să îşi dezvolte propriile capacităţi de protecţie

[6]Sprijinul acordat se concretizează în schimbul de informaţii şi bune practici, executarea de exerciţii practice, asigurarea de expertiză, etc.

[7] http://www.nato.int/cps/en/natohq/official_texts_112964.htm

Eforturile NATO în domeniul apărării cibernetice sunt sprijinite în mod consistent de Centrul de Excelenţă NATO în domeniul Apărării Cibernetice prin Cooperare (Cooperative Cyber Defence Centre of Excellence - CCDCOE) din Estonia[1], în special în domeniul cercetării şi instruirii (figura 11.1).

Figura 11.1 Pagina web a Centrului de Excelenţă 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 guvernanța internetului (Klimburg, 2012).

Principalele activităţi privind apărarea cibernetică în NATO se referă la: asistarea naţiunilor aliate, integrarea apărării cibernetice în Procesul de Planificare a Apărării în NATO, dezvoltarea apărării cibernetice ca iniţiativă ”smart defence”, cercetare şi instruire (sprijinită consistent de CCDCOE), cooperarea cu naţiunile partenere, organizaţiile internaţionale, mediul academic şi industria de securitate[2], coordonarea şi ghidarea cu privire la măsurile practice de apărare cibernetică[3].

[1] http://www.ccdcoe.org/

[2] În prezent, NIAG (NATO International Armaments Group) derulează un studiu privind acţiunile de colaborare ale NATO cu industria pentru facilitarea apărării cibernetice pe timpul situaţiilor de criză

[3] Responsabilităţi 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 şi NCI - NATO Communications and Information Agency

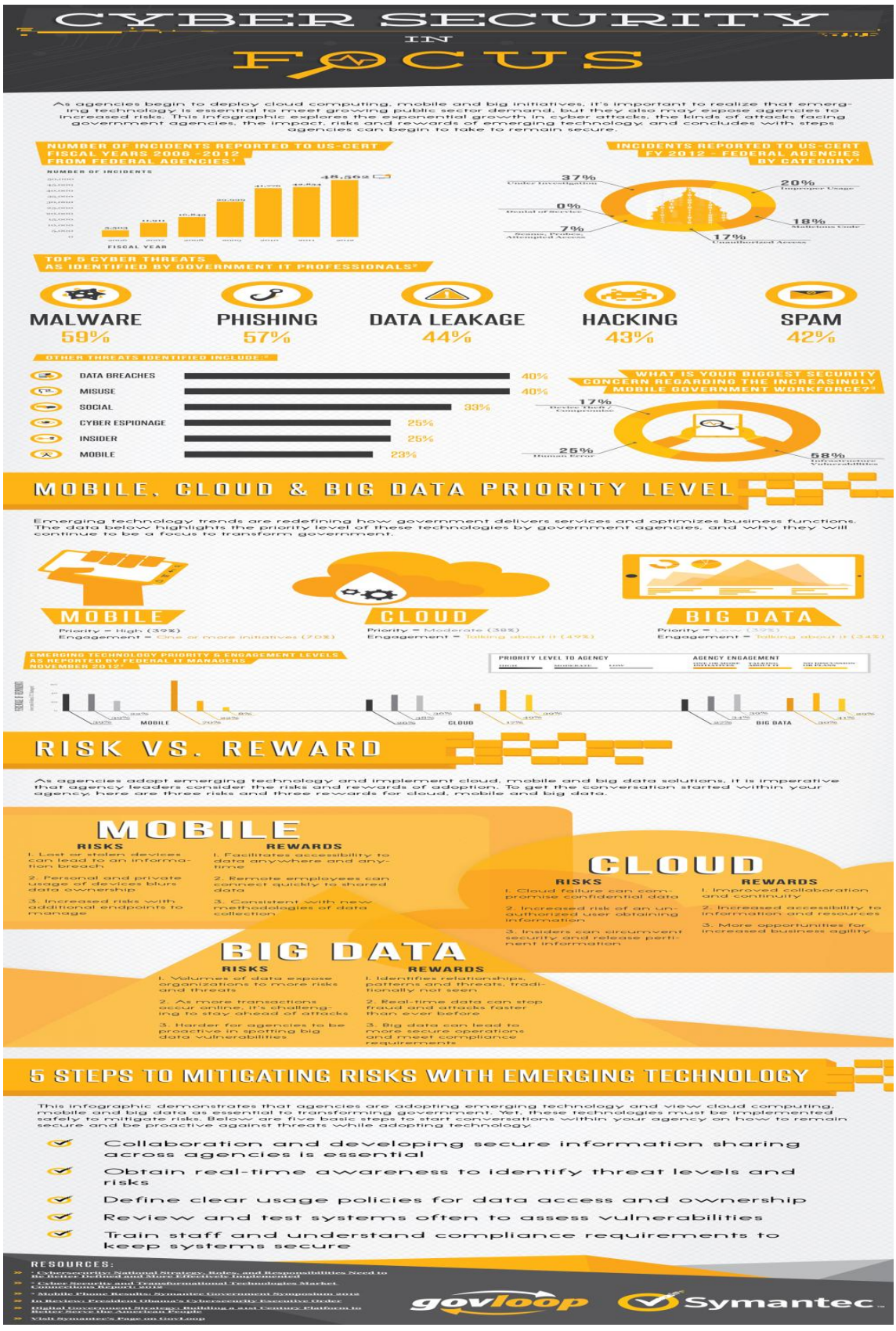


Figura 11.2 Infografie NATO privind domeniul securităţii cibernetice[1]

[1] http://www.nato.int/docu/review/2013/Cyber/Cyber-Security-in-Focus/EN/index.htm

Abordarea apărării cibernetice în NATO se bazează şi pe o strânsă cooperare cu ţările partenere, după caz, precum şi cu organizaţiile internaţionale - printre care UE, Consiliul Europei, ONU şi OSCE, cu sectorul privat şi mediul academic.

Pentru publicul larg, websiteul NATO facilitează accesul la informaţii, expuneri şi dezbateri de idei în domeniul apărării cibernetice în secţiunea dedicată acestui subiect[1], fiind o resursă utilă pentru cei doritori să îşi dezvolte perspectiva în acest domeniu – a se vedea ca exemplu infografia din figura 2.

În 2011, România şi NATO au semnat un Memorandum de înţelegere pentru cooperare în domeniul securităţii cibernetice[2], care asigură cadrul pentru schimbul de informaţii, cooperare şi sprijin între autoritatea naţională în domeniu (SRI) şi structurile responsabile ale Alianţei Nord-Atlantice.

Mai mult, România este parte[3] 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 capabilităților 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) naţionale şi la nivelul UE[5],
- organizarea de simulări pentru incidente de securitate în mediul cibernetic şi
- asigurarea sprijinului pentru pregătirea împotriva atacurilor cibernetice în cadrul Uniunii, cu precădere în ceea ce priveşte protecţia infrastructurii critice[6].

Fundamentarea măsurilor de securitate cibernetică la nivelul UE este realizată de Strategia de Securitate Cibernetică a Uniunii[7] şi de Directiva privind Securitatea Reţelelor şi a Informaţiei în UE, propusă de Comisia Europeană în februarie 2013 şi votată în Parlamentul European la 13 martie 2014[8].

[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
[5] http://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 priorităţi clare pentru politica internaţională a UE în materie de spaţiu virtual (http://eeas.europa.eu/policies/eu-cyber-security/index_ro.htm):

- Libertate şi deschidere: strategia va prezenta viziunea şi principiile privind aplicarea valorilor şi drepturilor fundamentale ale UE în spaţiul virtual.
- Legile, normele şi valorile fundamentale ale UE se aplică în spaţiul cibernetic şi în lumea materială: responsabilitatea pentru un spaţiu cibernetic mai securizat le revine tuturor participanţilor la societatea informaţională globală, de la cetăţeni la administraţii naţionale.
- Dezvoltarea consolidării capacităţilor în materie de securitate cibernetică: UE va colabora cu parteneri şi organizaţii internaţionale, precum şi cu reprezentanţi ai sectorului privat şi ai societăţii civile pentru a sprijini consolidarea capacităţilor globale în ţările terţe. Aceasta va include îmbunătăţirea accesului la informaţii şi la un internet deschis, precum şi prevenirea ameninţărilor cibernetice.
- Încurajarea cooperării internaţionale în materie de spaţiu cibernetic: păstrarea unui spaţiu cibernetic deschis, liber şi securizat reprezintă o provocare la nivel mondial, pe care UE ar trebui să o abordeze împreună cu partenerii şi organizaţiile internaţionale relevante, sectorul privat şi societatea civilă.

[8] http://europa.eu/rapid/press-release_STATEMENT-14-68_en.htm

Pe lângă CERT-EU, activităţile privind securitatea cibernetică în UE sunt în responsabilitatea Agenţiei Europene pentru Securitatea Reţelelor şi a Informaţiei (European Network and Information Security Agency/ ENISA)[1].

În România, sistemul naţional de securitate cibernetică (SNSC) reprezintă cadrul general de cooperare care reuneşte autorităţi şi instituţii publice, cu responsabilităţi şi capabilităţi în domeniu, sub coordonarea Consiliul operativ de securitate cibernetică (COSC)[2], în vederea coordonării acţiunilor la nivel naţional pentru asigurarea securităţii spaţiului cibernetic, inclusiv prin cooperarea cu mediul academic şi cel de afaceri, asociaţiile profesionale şi organizaţiile neguvernamentale. *(Strategia de securitate cibernetică a României, 2013)*

In cadrul SRI – în calitate de autoritate naţională pentru cyberintelligence – funcţionează Centrul Naţional CyberINT[3], cu misiunea de a asigura colectarea, analiza, reacţia, managementul consecinţelor şi diseminarea informaţiilor privind ameninţările şi atacurile cibernetice. În acest sens, responsabilităţile Centrului includ:

- identificarea ameninţărilor cibernetice generate prin intermediul reţelelor naţionale sau internaţionale de date;
- punerea la dispoziţia beneficiarilor legali a unor informaţii şi analize utile pentru prevenirea şi gestionarea situaţiilor de criză;
- contribuţia la securizarea infrastructurilor de comunicaţii şi procesare a datelor;
- asigurarea suportului tehnic pentru realizarea unor operaţiuni de contracarare a atacurilor cibernetice la adresa infrastructurilor IT&C naţionale.[4]

Dezvoltarea infrastructurii de tehnologia informaţiei şi comunicaţiilor a antrenat şi apariţia unui larg spectru de ameninţări la adresa utilizatorilor acestora, fapt ce a reclamat nevoia de protecţie sau reacţie la astfel de evenimente. Această necesitate la nivel public, totodată o nişă de piaţă pentru companiile private, a dus la consolidarea şi evoluţia permanentă a metodelor şi mijloacelor de asigurare a securităţii în domeniul cibernetic.

Atât în cadrul organizaţiilor şi instituţiilor publice, cât şi la nivelul companiilor private, pe lângă mijloacele de protecţie pasivă existente, se impune necesitatea unor structuri specializate care să monitorizeze şi să răspundă unui număr de ameninţări tot mai complexe, care – odată cu evoluţia tehnologiei – ies din tiparele clasice de agresiune (şi 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 specialişti în securitate cibernetică şi având atât rolul de a interveni urgent în situaţii complexe, cât şi prevenirea apariţiei unor incidente similare pe viitor.

---

[1] http://www.enisa.europa.eu/

[2] Din COSC fac parte, în calitate de membri permanenţi, reprezentanţi ai Ministerului Apărării Naţionale, Ministerului Afacerilor Interne, Ministerului Afacerilor Externe, Ministerului pentru Societatea Informaţională, Serviciului Român de Informaţii, Serviciului de Telecomunicaţii Speciale, Serviciului de Informaţii Externe, Serviciului de Protecţie şi Pază, Oficiului Registrului Naţional pentru Informaţii Secrete de Stat, precum şi secretarul Consiliului Suprem de Apărare a Ţării. Conducerea COSC este asigurată de un preşedinte (consilierul prezidenţial pe probleme de securitate naţională) şi un vicepreşedinte (consilierul prim-ministrului pe probleme de securitate naţională). Coordonatorul tehnic al COSC este Serviciul Român de Informaţii, în condiţiile legii. *(Strategia de securitate cibernetică a României, 2013)*

[3] înfiinţarea unităţii cu atribuţii în securitatea cibernetică fiind aprobată în şedinţa Consiliului Suprem de Apărare a Ţării 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)

[4] 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

În România, principalul obiectiv al CERT-RO[1] (structură guvernamentală independentă pentru cercetare, dezvoltare şi expertiză în domeniul securităţii cibernetice[2]) stabilit prin lege este ”înfiinţarea sistemului naţional de alertă timpurie şi informare în timp real privind incidentele cibernetice în scopul avertizării şi emiterii de rapoarte cu privire la distribuţia şi natura incidentelor, precum şi colaborarea cu autorităţile naţionale responsabile în asigurarea securităţii cibernetice în vederea prevenirii şi înlăturării efectelor incidentelor”[3].

Pentru asigurarea eficienţei la nivel naţional şi a relevanţei în plan instituţional internaţional, toate instituţiile publice (utilizatori, sisteme şi reţele din spaţiul cibernetic românesc) sunt obligate să se înroleze în acest sistem; totodată, CERT-RO este membră a comunităţii TF-CSIRT[4], comunicând şi cooperând cu alte CSIRT (figura 11.3).

Figura 11.3 Locaţii CERT în Europa (http://www.enisa.europa.eu/activities/cert/background/inv)

Comitetul de coordonare al CERT-RO este format din reprezentanţi ai:[5]

a) Ministerului Comunicaţiilor şi Societăţii Informaţionale;
b) Ministerului Apărării Naţionale;
c) Ministerului Administraţiei şi Internelor;
d) Serviciului Român de Informaţii;
e) Serviciului de Informaţii Externe;
f) Serviciului de Telecomunicaţii Speciale;
g) Serviciului de Protecţie şi Pază;
h) Oficiului Registrului Naţional al Informaţiilor Secrete de Stat;

[1]înființarea CERT-RO are la bază H.G. 494 / 11 May 2011
[2]RFC 2350 description for CERT-RO (Romanian National Computer Emergency Response Team) (2012), în http://www.cert-ro.eu/files/doc/RFC2350.pdf
[3]http://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) Autorităţii Naţionale pentru Administrare şi Reglementare în Comunicaţii.

În vederea îndeplinirii atribuţiilor ce revin CERT-RO, directorul general al acesteia emite decizii si instrucþiuni.

Echipele CERT oferă o serie de servicii clasificate ca:

a. reactive:

- alerte şi avertizări, concretizate în notificări imediate care fac referire la incidente de securitate aflate în desfăşurare, precum noi viruşi 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 organizaţii, precum bănci, companii energetice, agenţii guvernamentale, ori noi acţiuni ingenioase de inginerie socială menite să obţină date privind cărţile de credit sau date cu caracter personal;
- tratarea incidentelor de securitate (prin intervenţie la locul incidentului sau acordarea de suport la distanţă);
- managementul vulnerabilităţilor (atât hardware, cât şi software);
- culegerea probelor (identificarea fişierelor de pe un calculator atacat, care au fost instalate de un criminal cibernetic în mod direct sau prin intermediul unui cod maliţios precum troieni, viruşi 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 acţiunii criminale);

b. proactive:

- anunţurile;
- urmărirea evoluţiei tehnologice;
- evaluările de securitate;
- configurarea şi menţinerea soluţiilor de securitate;
- dezvoltarea uneltelor de securitate;
- servicii de detectare a intruziunilor;
- diseminarea informaţiilor din domeniul securităţii. (Provision IT Group, 2013)

Metodologia de lucru a CERT face apel şi la utilitatea folosirii de echipe CERT private, care să completeze resursele publice şi să deservească consumatori de mare calibru în domeniul IT&C şi sectoare vizate în mod agresiv de incidente de securitate cibernetică, precum cel al telecomunicaţiilor sau din mediul bancar.

Pentru a acoperi cererea existentă, furnizorii privaţi de servicii de securitate informatică îşi ajustează oferta proprie în servicii reactive şi/sau proactive de tip CERT, în condiţii de confidenţialitate, pe care le oferă contra cost (prin abonament sau servicii punctuale).

Websiteul CERT-RO, pe lângă ghiduri de protecţie, listează şi o serie de link-uri către websiteuri ce furnizează programe şi aplicaţii protecţie în mediul cibernetic:[1]

- aplicaţii pentru devirusare troian FLAME/GAUSS:
  - Bitdefender_Gauss_Removal_Tool
  - Bitdefender_Flame_Removal_Tool
  - Kaspersky_Virus_Removal_Tool_2011_SITU_Edition
- aplicaţii gratuite împotriva software rău intenţionat (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 distanţă:
  PuTTy
- aplicaţii de criptare:
  Pretty Good Privacy - GnuPG
  TrueCript
- aplicaţii de tip Firewall:
  COMODO Free Firewall
  ZoneAlarm Free Firewall
- aplicaţii de detectare a intruziunilor:
  OSSIM
  OSSEC
  SNORT
- scaner 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 şi de comunicaţii ale unui stat, precum şi datele gestionate de acestea, sunt tot mai dependente de spaţiul cibernetic. Totodată, mediul cibernetic găzduieşte elementele de manifestare ale lumii reale, începând cu multiple comunităţi de interes şi reţele umane ce se manifestă în mediul virtual. Dincolo de beneficiile evidente pe care acest mediu le are în facilitarea tuturor aspectelor existenţei umane – de la cele economice, financiare, sociale, culturale şi până la cele politice şi militare – acesta facilitează şi o serie de riscuri specifice, în special în absenţa unor măsuri de securitate adecvate.

Atât entităţile statale, cât şi cele non-statale (la o scară care le pune aproape pe picior de egalitate cu agenţiile guvernamentale în acest cadru), în baza propriilor interese, pot recurge la agresiuni cibernetice împotriva competitorilor sau opozanţilor.

După cum o relevă SRI, astfel de atacuri cibernetice pot fi îndreptate împotriva sistemelor de tehnologia informaţiei şi de comunicaţii, care fie reprezintă infrastructuri critice în sine (de exemplu telecomunicaţiile şi reţeaua Internet), fie sunt esenţiale pentru buna funcţionare a celorlalte infrastructuri critice ale statului (de exemplu infrastructura de transport aerian, feroviar şi rutier, sistemele de aprovizionare cu energie, gaze, petrol şi 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 organizaţie. Din această perspectivă, şi abordarea problematicii Intelligence în domeniul cibernetic comportă o serie de nuanţe, în funcţie de sistemul de referinţă. La rândul ei, fiecare disciplină de culegere a informațiilor din spectrul Intelligence se raportează la aspecte specifice în ce priveşte obiectivele operaţionale şi modalitatea de manifestare în fiecare dintre etapele ciclului Intelligence – planificare şi direcţionare, colectare, procesare şi producţie, diseminare – raportate la definirea cerinţelor de informaţii, tipul de date colectate, metodologia de colectare, resursele implicate/ senzorii utilizați, modul de procesare a datelor şi informaţiilor primare, diseminarea produselor de intelligence, caracterul acestora şi asigurarea conexiunii inverse (feed-back).

Cartea albă a Alianţei pentru Intelligence şi Securitate Naţională (The Intelligence and National Security Alliance/INSA)[1] din SUA, un parteneriat public-privat în domeniu, evaluează necesitatea depăşirii planului tactic ("sistemul" sau "reţeaua") în acest domeniu şi orientarea către cerinţele de informaţii 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 diferenţierea abordărilor privind analiza modului de manifestare a disciplinelor de colectare a datelor, comun acceptate, ale spectrului Intelligence faţă de îmbogăţirea acestui spectru prin definirea unei activităţi 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).

[1]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

Figura 11.4 Ciclul Intelligence

În domeniul cibernetic, **planificarea şi direcţionarea** – ca etapă definită de exprimarea scopului/ intenţiilor – poate urmări descoperirea serverelor de comandă şi control a unui software rău intenţionat (malware) în vederea blocării acestuia; **colectarea datelor** în mediul cibernetic se desfăşoară în zone ca: puncte de atracţie (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 informaţiilor colectate în formate adaptate utilizării acestora; **producţia** asigură transformarea datelor într-un produs de tip ”intelligence” care să răspundă nevoilor de informaţii; **diseminarea** asigură transferul de intelligence către beneficiar, în timp ce **conexiunea inversă** confirmă sau infirmă acurateţea produsului de intelligence raportat la planificare şi direcţionare (Lee, 2014a).

Cyber Threat Intelligence (CTI)

Beaupré și Hellberg descriu conceptul de Cyber Threat Intelligence (CTI) ca abilitate de a colecta, împărți și analiza date în vederea elaborării răspunsului la o amenințare în domeniul cibernetic, soilictând 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 cibernetice.

Centrul pentru Schimbul de Informații și Analiză/ SUA (Information Sharing and Analysis Center/ ISAC) folosește conceptul de **Intelligence pentru amenințările cibernetice** (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 cibernetici 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:

a. 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),
b. abordare științifică a urmelor - *Cyber forensics* - (dedicată analizei cauzelor atacurilor cibernetice și urmăririi căilor de atac de la sursă și pe parcursul infiltrării în sistemele și rețelele proprii),
c. 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 desfăşurată în mediul privat în vederea asigurării securităţii informaţiei şi a reţelelor, se bazează pe: investigaţii în domeniul digital (investigaţia fiind o metodă de lucru a contrainformaţiilor – în acest caz având ca obiectiv depistarea fraudelor bazate pe folosirea computerelor, detectarea spionajului industrial, încălcarea dreptului de proprietate intelectuală, etc.); depistarea prezenţei intruşilor şi analiza de expunere a clienţilor, în vederea prevenirii scurgerilor de informaţii şi atenuării vulnerabilităţilor; folosirea de tehnici şi metodologii OSINT pentru crearea de rapoarte de intelligence în sprijinul proceselor decizionale[2].

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].

[1] http://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 CYBERINT[1]

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 capabilităților 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, cerinţele specifice pentru performanţa analistului în CYBERINT pornesc de la stăpânirea cunoştinţelor specifice (infrastructură, proceduri, protocoale, securitate) şi 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 cibernetice: 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 conţinutului, cuprinsul acestuia oferind detalii esenţiale cu privire la informaţia evaluată, precum şi opiniile analistului – judecăţi de valoare bazate pe istoricul subiectului, informaţiile conexe şi gândirea critică a acestuia, cu valenţe anticipative relativ la evoluţia viitoare a ameninţării (Lee, 2014b).

INSA consideră că CYBERINT nu este o disciplină de culegere a informaţiilor în sine ci, în mod similar cu MEDINT, este o disciplină analitică ce se bazează pe informaţii 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 informaţii, CYBERINT la **nivel strategic** furnizează evaluări de risc menite să orienteze factorii de decizie în ce priveşte planificarea şi investiţiile în securitatea cibernetică. Informaţiile relevante care sunt analizate la acest nivel privesc atât date de reţea, activităţi cibernetice în derulare, cât și evenimente geopolitice cu potenţial de influenţă asupra securităţii cibernetice.

La **nivel operaţional**, ameninţările în domeniul cibernetic reflectă interesele de nivel strategic din spatele vectorilor de atac şi urmăresc blocarea capacităţilor de comandă şi control asupra elementelor tactice, cu efecte în lumea reală. Totodată, ameninţările cibernetice la acest nivel pot fi coordonate cu acţiuni în lumea reală care, conjugate, să sprijine producerea unor efecte dorite.

CYBERINT la nivel operaţional se poate concentra asupra:[2]

- analizelor de trend, menite să indice direcţiile de evoluţie ale adversarului din punct de vedere tehnic;
- identificării de indicatori cu privire la modalitatea selectată de adversar pentru atacarea entităţii proprii;
- identificării de indicatori cu privire la construirea de către adversar a unor capabilităţi în vederea exploatării unor căi de atac;
- descoperirii tehnicilor, tacticilor şi procedurilor adversarilor;
- înţelegerii ciclurilor/ proceselor operaţionale ale adversarului;
- identificării vulnerabilităţilor adversarului (tehnice, sociale, financiare, etc.);

[1] http://www.insaonline.org/i/d/a/b/CyberIntel_embed.aspx
[2] http://www.insaonline.org/i/d/a/b/CyberIntel_embed.aspx

- informaţiilor menite să influenţeze acţiunile adversarului odată declanşat atacul cibernetic.

Nivelul tactic al domeniului cibernetic este reprezentat de cadrul concret al acţiunilor în reţea, cuprinzând atacurile cibernetice şi măsurile de protecţie, apărare şi contracarare a acestora. Identificarea atacurilor se bazează pe alertele sistemelor de securitate, detectarea de ”semnături” specifice ale acestora, analiza acţiunilor unor actori cunoscuţi sau a urmelor comportamentului în reţea. La acest nivel, în anumite contexte geopolitice, CYBERINT poate viza actori statali care acţionează direct sau prin intermediari, determinând identitatea lor, probabilitatea unor atacuri şi orizontul de timp al producerii acestora.

Concluzii

Mediul cibernetic constituie un domeniu acţional în culegerea de date şi informaţii pentru mai multe discipline de colectare din spectrul Intelligence (OSINT, MASINT, SIGINT) sau un facilitator/ interfaţă prin oportunităţile de comunicare şi relaţionare 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 cibernetice și asigurarea securității cibernetice 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 definiţi şi acceptaţi, folosirea produselor de Intelligence în mediul cibernetic, la toate nivelurile de decizie şi acţiune, este o necesitate evidentă. Legat de aceasta, reținem că domeniul cibernetic adresează nevoia unor cunoştinţe tehnice avansate, în special la nivelul analiştilor în domeniu, incluzând înţelegerea proceselor şi protocoalelor informatice, limitele şi oportunităţile oferite de reţele, folosirea terminologiei specifice, etc., dar fără a face rabat de la cunoaşterea aprofundată a adversarului (state, competitori în afaceri, organizaţii criminale), mediile operaţionale ale acestuia şi a fundamentului uman al acţiunilor maliţioase în mediul cibernetic (intenţia, motivaţia, planificarea, reţelele de coordonare, modalităţile de execuţie, 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 indicaţiile pe care websiteul SRI le pune la dispoziţia publicului în vederea educării pentru asigurarea propriei protecţii în mediul online, dar şi ca facilitator pentru depistarea atacurilor cibernetice sau a altor riscuri la adresa securităţii, cu privire la: protecţia informaţiilor clasificate, navigarea sigură pe Internet, depistarea şi semnalarea riscurilor teroriste, protejarea de acţiunea 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 şi capacitate de reacţie, pornind de la nivel individual şi avansând către sisteme publice naţionale şi chiar internaţionale.

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 şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional 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*, înhttp://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber-intelligence/
11. *LEE, Robert M*. (2014b) *Developing Your Cyber Intelligence Analyst Skills*, înhttp://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 şi utilitatea CERT-urilor private*, document realizat în cadrul campaniei de conştientizare a riscurilor de securitate cibernetică derulată în Romania 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