REVISTA ROMÂNĂ
DE STUDII DE INTELLIGENCE

Nr. 3
Octombrie
2010

Bucureşti
- 2010 -

CUPRINS

Provocări la adresa analizei strategice. Studiu de caz: Implicațiile războiului ruso-georgian asupra echilibrului de putere în Eurasia

Drd. Ionel NIȚU
Serviciul Român de Informații
e-mail: **ionelnitu@sri.ro**

Motto
„Războiul nu este altceva decât continuarea politicii cu alte mijloace."
(Carl von Clausewitz)

Abstract

The goal of this article is to look into the strategic implications of the 2008 Russian-Georgian war (military conflict) over the Euro-Atlantic security area from the intelligence point of view, especially from a strategic analysis approach.

Therefore, we will skim through the operational details of the conflict (details regarding the war stages, as well the history of the Russian-Georgian relationships have been mentioned in the annex 1, 2 and 3). Such details are important as long as they help laying the foundations of certain scenarios of the international security environment evolution.

Nowadays, within the framework in which the political and analytical environments focus on the emergence of new forms of asymmetry, the Russian-Georgian conflict brought into attention the typical pattern of threats to the states' existence resulted from the conventional war.

Keywords: strategic analysis, Russian-Georgian war.

Studiul de față combină *abordarea descriptivă* – prin analizarea *post factum* a crizei georgiene cu cea *predictiv-anticipativă* – prin realizarea unei prognoze asupra implicațiilor geostrategice generate de acest conflict, utilizând *metoda scenariilor*.

Scopul prezentei lucrări este de a examina implicațiile strategice ale războiului (conflictului militar) ruso-georgian din 2008 asupra securității spațiului euroatlantic dintr-o perspectivă specifică domeniului *intelligence*, îndeosebi al *analizei strategice*.

Din acest considerent, detaliile operaționale ale conflictului sunt abordate într-o manieră pasageră (detalii privind fazele războiului, precum şi

istoricul relațiilor ruso-georgiene sunt redate în Anexele 1, 2 şi 3), în măsura în care ajută la fundamentarea unor scenarii de evoluție a mediului internațional de securitate.

În contextul în care, în prezent, mediile politice şi de analiză se concentrează asupra emergenței noilor forme de asimetrie, conflictul ruso-georgian din 2008 a readus în atenție modelul clasic al amenințării la adresa existenței statale generat de războiul convențional.

Definiții şi concepte

► Întrucât există foarte multe accepțiuni ale termenului *intelligence*, am optat pentru o definire succintă, dar şi integratoare, a acelor atribute care sunt aplicabile serviciilor de informații şi activității acestora.

Astfel, conceptul de *intelligence*[1] înglobează patru elemente distincte care vizează activitatea de realizare a securității naționale:

(1) procesul prin care informațiile importante pentru securitatea națională sunt solicitate, colectate, analizate şi diseminate factorilor de decizie din stat;

(2) produsul rezultat în urma acestui proces, utilizat pentru susținerea intereselor şi obiectivelor naționale;

(3) forma de organizare pentru desfăşurarea acestui proces, din punct de vedere structural şi al operațiunilor derulate;

(4) protejarea acestui proces şi a informațiilor obținute prin activități de contrainformații.

Principala provocare a analizei de *intelligence* este generată de faptul că incertitudinea care înconjoară amenințările la adresa securității impune ca analiştii şi factorii de decizie să facă raționamente care sunt în mod inerent susceptibile/vulnerabile la eroare. Analiştii trebuie să emită o avertizare cu mult timp înainte de derularea evenimentului, astfel încât factorii de decizie să aibă timp să ia măsurile preventive şi de contracarare ce se impun, însă trebuie să fie temeinic motivată pentru a-i determina pe aceştia să acționeze.

> Aşteptând o confirmare a presupunerii strategice, analistul poate pierde oportunitatea informării beneficiarilor în timp util, în timp ce realizarea unei predicții fără existența unor dovezi certe poate pune sub semnul întrebării credibilitatea analizei.

► *Analiza strategică* (*strategic intelligence*) constituie, în esență, o abordare multisectorială şi multisursă a fenomenelor cu impact major în sfera securității naționale (în plan politic, militar, economic, social) cu o consistentă

[1] Aşa cum a fost abordat la masa rotundă *Societate, Democrație, Intelligence*, organizată de Serviciul Român de Informații în data de 8 octombrie 2008 (www.sri.ro).

dimensiune proiectiv-anticipativă. Rezultatul acesteia se reflectă în evaluări, prognoze sau estimări cu privire la posibile evenimente din viitor, gradul de probabilitate a apariției lor, precum şi potențialul impact al acestora asupra intereselor de securitate națională[2].

Într-o accepțiune simplă, analiza strategică este acea analiză care este necesară pentru formularea unei strategii, a unui plan sau a unei politici a statului, a unei direcții de acțiune într-un domeniu al securității naționale.

Termenul ***intelligence strategic*** a fost lansat de **Sherman Kent** în lucrarea *"Strategic Intelligence for American Foreign Policy"* (1949), fiind definit drept *„cunoaşterea pe care decidenții politici şi militari trebuie să o posede pentru a asigura bunăstarea națională"*[3].

În literatura de specialitate majoritatea definițiilor accentuează rolul *intelligence*-ului *strategic* în fundamentarea strategiilor de securitate (la nivel național ori sectorial), respectiv identificarea modalităților de contracarare a amenințărilor, riscurilor şi vulnerabilităților la adresa securității naționale.

Prezint succint alte definiții:

Adda Bozeman – *intelligence-ul strategic trebuie să faciliteze urmărirea constantă a unor obiective pe termen lung, respectiv să ofere susținere decidenților politici în cazul unor evenimente de politică externă*[4].

Bruce Berkowitz şi **Allan Goodman** – *intelligence-ul strategic este destinat să ofere oficialilor imaginea de ansamblu a mediului de securitate şi proiecții pe termen lung în scopul planificării măsurilor destinate contracarării amenințărilor la adresa securității naționale*[5].

Richard Russell – *analiza strategică reprezintă sinteza informațiilor obținute din surse secrete (umane, interceptarea comunicațiilor, date preluate prin satelit etc.) şi/sau deschise (presă scrisă, radio, TV, Internet etc.) cu relevanță pentru decizionalii în stat cu atribuții în stabilirea şi implementarea obiectivelor naționale majore*[6].

---

[2] Russell, Richard, *Sharpening Strategic Intelligence: Why the CIA Gets it Wrong, and What Needs to be Done to Get it Right*, Cambridge University Press, 2007, p. 6.

[3] Apud Russell, Richard, *Sharpening Strategic Intelligence: Why the CIA Gets it Wrong, and What Needs to be Done to Get it Right*, Cambridge University Press, 2007, p. 6.

[4] Bozeman, Adda, *Strategic Intelligence and Statecraft, Pergamon-Brassey's*, Washington DC, 1992.

[5] Berkowitz, Bruce; Goodman Allan, *Best Truth – Intelligence in the Information Age*, Yale University Press, 2000, p. 63.

[6] Russell, Richard, *Sharpening Strategic Intelligence: Why the CIA Gets it Wrong and What Needs to be Done to Get it Right*, Cambridge University Press, 2007, p. 7.

În esență, analiza strategică reprezintă o analiză pluridisciplinară care abordează fenomenele din multiple perspective – politică, militară, economică, socială, a organizării instituționale şi comportamentului birocratic, a infrastructurii, a culturii şi specificității unor societăți sau grupuri umane –, în scopul fundamentării unor decizii majore (cu arie largă de aplicabilitate, care să vizeze domenii extinse etc.) cu caracter predictiv/anticipativ.

► *Avertizarea strategică* se referă la o amenințare în general (apariția unui conflict militar, schimbarea unui regim politic etc.) şi oferă posibilitatea de a preveni apariția unei crize prin identificarea subiecților acțiunii (cine?, ce?), a modalităților de acțiune ale acestora (cum?), a coordonatelor spațio-temporale (când?, unde?), precum şi a mobilului (de ce?).

Similar preocupărilor analizei strategice, realizarea unei avertizări privind iminența unui atac presupune cunoştințe cumulate despre intențiile grupărilor, organizațiilor ori statelor ostile (greu de identificat şi modificat în absența unor informații exacte, provenite din surse secrete – fie umane, fie tehnice), precum şi despre capabilitățile de care acestea dispun pentru a inița demersul ostil (odată identificate, se poate acționa pentru a le distruge/neutraliza).

De asemenea, avertizarea are implicații atât în plan operațional şi tactic, cât şi în plan strategic, în măsura în care determină mutații ale contextului de securitate (de exemplu, atacul de la Pearl Harbor, criza rachetelor din Cuba, Yom Kippur etc.). Nu în ultimul rând, avertizarea presupune reevaluarea procesului de luare a deciziei şi de alocare a resurselor pentru a contracara în timp util şi adecvat intențiile părții adverse.

În literatura de specialitate nu există o definiție general acceptată a conceptului de avertizare strategică, majoritatea acestora semnalând necesitatea identificării unor indicii sau semnale privind potențarea unei amenințări sau a unui factor de risc[7].

► *Metoda scenariilor* este utilizată, în general, pentru explorarea posibilelor condiții de manifestare a unei situații plecând de la un set de propuneri/ipoteze de lucru, fiecare scenariu reprezentând un viitor plauzibil distinct. În activitatea de informații scenariile reprezintă „tipare-model" ale obiectivului/evenimentului vizat, scopul alcătuirii unui scenariu fiind evidențierea

[7] Cynthia, Grabo, *Anticipating Surprise: Analysis for Strategic Warning*, Joint Military Intelligence College, Washington, 2002, p. 4.

unor factori majori care influenţează viitorul, în vederea anticipării şi formulării unui răspuns adecvat[8].

Scenariile oferă consumatorilor de *intelligence* o imagine a probabilităţii desfăşurării evenimentului, în situaţia în care aceştia se centrează pe un anumit curs al acţiunii dintr-o situaţie complexă ce nu poate fi cuantificată.

După constituirea scenariilor, munca analistului de informaţii este direcţionată spre identificarea şi selectarea indicatorilor relevanţi pentru realitatea analizată. Prin asigurarea unei sfere realiste de posibilităţi/probabilităţi, stabilirea scenariilor alternative ajută decidenţii (beneficiarii) să identifice trăsături comune posibile, să evalueze implicaţiile, indiferent pe ce curs al evenimentelor se situează şi, mai ales, să selecteze variante alternative de acţiune (în funcţie de evoluţiile înregistrate în mod real)[9].

În concluzie, teoria scenariilor – ca şi alte metode de analiză de tip strategic – nu are rolul de a oferi o predicţie exactă asupra viitorului, ci doar de „a sprijini factorii de decizie să gândească asupra viitorului”[10], punând la dispoziţie un set de scenarii, cu grade diferite de probabilitate, care să evidenţieze atât planurile/intenţiile adversarului, cât şi modalităţi adecvate de contracarare a acestora.

Aparatul metodologic

Pentru a analiza situaţia iniţială, am utilizat ***modelul de eliminare a incertitudinii aleatorii*** lansat de Kenneth Waltz[11], centrat pe interacţiunea a trei niveluri de analiză, respectiv:

– influenţele evoluţiilor din mediul internaţional de securitate asupra deciziei celor două tabere de a utiliza forţa militară, ca soluţie de reglementare a acestui „conflict îngheţat”;

– natura relaţiilor ruso-georgiene, precum şi a raporturilor dintre republicile separatiste Osetia de Sud şi Abhazia şi dintre acestea şi cele două state limitrofe;

– importanţa influenţei factorilor de decizie din cele două state, precum şi rolul preconcepţiilor din mentalul colectiv rus şi georgian în declanşarea conflictului.

---

[8] Mandel, T. F., “Future Scenarios and Their Use in Corporate Strategy” în *The Strategic Management Handbook*, New York, Ed. H.J.Albert, 1983, pp. 10-21.

[9] Clark, Robert M., *Intelligence Analysis: A Target – Centric Approach*, Washington DC, CQ Press, 2007, p. 184.

[10] Nye, Joseph S. Jr., „Peering into the Future” în *Foreign Affairs* (July/August 1994), 1994, p. 88.

[11] Waltz, Kenneth, *Man, the State and War*, New York, Columbia University Press, 1954.

Identificarea şi analizarea corectă a variabilelor care determinau evoluțiile relațiilor dintre Moscova şi Tbilisi ar fi putut facilita realizarea unor predicții corecte privind emergența conflictului ruso-georgian.

Având în vedere faptul că războiul nu poate fi disociat de obiectivele politice ale combatanților, dar şi că procesul de luare a deciziilor poate fi afectat de evenimente aleatorii, am apelat la *metoda scenariilor* pentru a ilustra faptul că războiul ruso-georgian:

– reprezintă un eşec al sistemului internațional de securitate;

– nu a fost rezultatul unei acțiuni accidentale, ci mai degrabă o extensie a interacțiunilor politice care au precedat conflictul propriu-zis;

– reprezintă un caz clasic de eşec al domeniului *intelligence* în a prevedea escaladarea tensiunilor şi evoluția către un conflict armat;

– nu şi-a epuizat potențialul de recrudescență, având implicații majore asupra securității Regiunii Extinse a Mării Negre şi a spațiului euroatlantic.

Vectori de analiză în formularea unei avertizări strategice privind declanşarea conflictului din Caucaz

Fără a avea un caracter nondeterminat (aleatoriu) sau nonlinear (relațiile cauză-efect fiind proporționale), războiul ruso-georgian poate fi asimilabil unei surprize strategice în măsura în care semnalele/avertismentele care au precedat atacul nu au fost corect interpretate (îndeosebi de factorii europeni de decizie).

Emiterea unei avertizări timpurii a serviciilor de informații privind declanşarea unui conflict la granița dintre Georgia şi regiunile separatiste Osetia de Sud şi Abhazia ar fi putut fi facilitată de analiza următorilor indicatori de nivel:

a) geostrategic

– agresivitatea acțională şi retorică a Moscovei în raport cu Occidentul şi, în particular, față de state din „vecinătatea apropiată" cu aspirații prooccidentale (Georgia şi Ucraina);

– decizia de declarare (şi, ulterior, recunoaşterea de către unele state din spațiul euroatlantic) a independenței Kosovo (februarie 2008), urmată de avertismentul lui Vladimir Putin privind perspectiva unei acțiuni *qui pro quo* în Caucaz;

– decizia de amânare a acordării MAP Georgiei la Summitul NATO de la București (2-4 aprilie 2008);

b) operațional

– multiplicarea unor *pattern*-uri acționale (acuzații, provocări, incidente, ciocniri armate ş.a.) şi intensificarea retoricii belicoase în lunile preliminare declanşării conflictului;

– substanţialitatea programelor militare de înarmare derulate de autorităţile georgiene;

– doborârea, de către aviaţia rusă, a unor drone georgiene în „zona de securitate";

– suplimentarea „forţelor pacificatoare ruse" staţionate în Abhazia până la limita maximă admisă de acordurile de încetare a focului (aproximativ 2 500 de militari);

– refacerea, de către trupele militare ruse, a infrastructurii rutiere şi feroviare din Abhazia;

– pregătirile militare ale ambelor tabere, care au culminat cu mascarea masării forţelor armate în apropierea graniţei Osetiei de Sud (prin intermediul exerciţiilor militare derulate cu puţin timp înainte de izbucnirea conflictului: *Kavkaz 2008* în cazul Rusiei, respectiv *Immediate Response* în cazul Georgiei – ambele simulând o acţiune militară îndreptată împotriva celeilalte tabere).

Importanţa unor factori de natură exogenă şi endogenă în declanşarea războiului

► ***Colapsul procesului de pace din Osetia de Sud şi Abhazia a relevat o serie de limite ale sistemelor/instrumentelor de aplicare a principiului neutilizării forţei în relaţiile internaţionale***, în special din perspectiva funcţionării ONU ca organism însărcinat cu asigurarea securităţii colective, precum şi a prezenţei ineficiente a observatorilor OSCE.

Totodată, conflictul a readus în prim-plan unele neconcordanţe din jurul noţiunilor „suveranitate", „integritate teritorială" sau „inviolabilitatea frontierelor", pe de o parte, respectiv „intervenţie umanitară", „autodeterminare" sau „autoapărare individuală şi colectivă", pe de altă parte.

Cu toate că toate aceste noţiuni au fost concepute pentru a contribui la asigurarea păcii mondiale, în practică natura lor conflictuală ridică probleme sistemului internaţional de asigurare a securităţii colective. Odată cu prăbuşirea URSS şi extinderea procesului de democratizare au devenit tot mai evidente fenomenele de autodeterminare a unor minorităţi care se confruntau cu practici abuzive din partea statelor de rezidenţă. Pe acest fond, lansarea unor mecanisme de intervenţie umanitară şi protecţie a populaţiilor ce se considerau discriminate a intrat în contradicţie cu principiile de suveranitate şi integritate teritorială.

Deşi, *de jure,* integritatea teritorială a Georgiei este de necontestat, în contrapondere există multiple surse de legitimare a dreptului Abhaziei şi Osetiei de Sud la autodeterminare, atât în dreptul internaţional (inclusiv Carta

ONU), cât şi în retorică (drepturile omului) sau practică (modelul Kosovo), care, *de facto*, alimentează noua realitate geopolitică rezultată în urma conflictului ruso-georgian.

De altfel, Carta ONU precizează în mod clar faptul că statele membre urmăresc „dezvoltarea relațiilor de prietenie între națiuni, în baza respectului principiului egalității în drepturi şi a autodeterminării popoarelor" (preambul) şi „asigură, cu respectarea cuvenită a culturii popoarelor, progresul lor politic, economic, social şi în domeniul educației, tratamentul lor echitabil şi protecția lor împotriva abuzurilor", precum şi „dezvoltarea capacității lor de a se autoguverna, de a ține seama de năzuințele politice ale acestor popoare" (art. 73, lit. a şi b).

Recunoaşterea unilaterală de către Rusia a independenței Abhaziei şi Osetiei de Sud reprezintă, conform Cartei ONU, un act ilegal, în măsura în care a subminat integritatea teritorială a Georgiei şi, pe cale de consecință, poate fi asimilabilă recunoaşterii (de către alte state, mai puțin Rusia) a independenței Kosovo.

Totodată, Rusia susține că a acționat ca urmare a agresiunii Georgiei şi a actelor de „genocid" săvârşite de aceasta asupra populației sud-osetine, dar şi a resortisanților săi. De altfel, conceptul *„responsability to protect"*, adoptat de ONU în 2005, este aplicabil în situațiile circumscrise „genocidului, crimelor de război, purificărilor etnice şi crimelor împotriva umanității". Or, Rusia susține că a acționat în baza acestui principiu pentru a proteja populația din Osetia de Sud, din motive umanitare.

► Dispariția URSS a constituit principalul factor favorizant al declanşării tendințelor separatiste din Caucaz, fenomen cu care chiar autoritățile sovietice s-au confruntat în anii '80. Intervenția trupelor ruse ca mediator între părțile implicate a contribuit la apariția *conflictelor înghețate*[12]. Cazul Georgiei este cu atât mai complicat cu cât această țară caucaziană s-a confruntat cu acțiunile centrifugale a trei regiuni – Abhazia, Osetia de Sud şi Adjaria.

După proclamarea independenței de către Abhazia şi Osetia de Sud şi conflictele care au urmat au fost semnate acorduri de încetare a conflictului[13], prin intermediul cărora erau instituite misiuni ONU sau CSI de menținere a păcii. În realitate, aceste acorduri au fundamentat, paradoxal, o situație ce a fost

[12] Heinrich, H.G., "Frozen Crisis in the Caucasus: Can the Circle Be Unsqaured?", *31st Viene Seminar*, Diplomatic Academy, 2001, p. 109.

[13] Acordul de la Moscova privind încetarea focului dintre Georgia şi Abhazia (1994), respectiv Acordul de la Soci privind reglementarea conflictului georgiano-osetin dintre Georgia şi Federația Rusă (1992).

caracterizată în mediile politice şi de analiză internaţionale prin sintagma „no peace, no war”[14].

Deşi organizaţiile de securitate implicate în reglementarea conflictului dintre Tbilisi şi cele două republici separatiste au recunoscut fără echivoc integritatea teritorială a Georgiei, Federaţia Rusă a monopolizat toate negocierile care au urmat privind reglementarea conflictului şi şi-a exercitat influenţa în Consiliul de Securitate al ONU asupra deciziilor adoptate. În realitate, autorităţile ruse au încurajat secesionismul republicilor separatiste, inclusiv prin acordarea pe scară largă a cetăţeniei ruse, ca instrument de menţinere a influenţei asupra fostelor republici sovietice şi de contracarare a extinderii influenţei Occidentului în „vecinătatea apropiată”.

► ***Venirea la putere în Georgia a lui Mihail Saakashvili şi asumarea de către acesta a unei politici de apropiere faţă de structurile europene şi euroatlantice au determinat deteriorarea substanţială a relaţiilor cu Kremlinul.*** Mai mult, după înlăturarea liderului separatist din Adjaria, Aslan Abashidze, în mai 2004, autorităţile georgiene au iniţiat diferite strategii de reîncorporare a celorlalte două republici.

Pe acest fond, încercările georgiene de a susţine o administraţie paralelă în Osetia de Sud şi perspectiva, după Summitul NATO de la Bucureşti, de acordare a MAP-ului Georgiei şi Ucrainei au contribuit la determinarea Moscovei de a fructifica orice oportunitate pentru a impune o reglementare a conflictului favorabilă propriilor interese.

Motivul invocat de ambele părţi pentru declanşarea războiului este la prima vedere banal, dar reflectă existenţa în mentalul elitelor politice din cele două state a ideii că singura soluţie de reglementare a separatismului abhaz şi sud-osetin este calea armelor:

- Georgia a susţinut că decizia de a utiliza forţa militară i-a fost impusă, fiind provocată de tirurile sistematice ale osetinilor şi ruşilor asupra forţelor georgiene;

- Rusia s-a apărat afirmând că reacţia sa a avut drept obiectiv apărarea drepturilor cetăţenilor ruşi din cele două provincii separatiste.

Resorturile deciziei Georgiei de a declanşa o acţiune militară sunt neclare, fiind greu de apreciat în ce măsură obiectivele politico-statale au primat asupra altor factori precum orgoliul naţional, creşterea imaginii pe plan regional şi european sau pasiunile individuale.

[14] Newman, Edward; Richmond, Oliver, *Challenges to Peacebuilding: Managing Spoilers During Conflict Resolution*, New York, United Nations University Press, 2006, p. 282.

Astfel, raportând la obiectivele declarate inițial de Tbilisi – protejarea cetățenilor georgieni din Osetia de Sud – la efectivele militare georgiene dislocate la Tskhinvali, putem observa o ***discordanță între obiectivul politic major urmărit de Georgia*** (revenirea regiunilor separatiste în componența statului georgian) ***şi capabilitățile militare reduse angrenate la granița osetină***, pe fondul dislocării unor importante trupe în Irak şi la granița cu Abhazia. De aceea, ***decizia autorităților georgiene de a utiliza forța militară nu poate fi explicată din punct de vedere al strategiei militare.***

Din această perspectivă, decizia Georgiei de a utiliza forța armată ar putea avea două cauze:

– falsul sentiment de încredere că Vestul va susține necondiționat statul georgian în distanțarea de Rusia, generat de integrarea acestei țări în Programul Parteneriat pentru Pace al NATO şi Programul american de pregătire şi echipare a Georgiei;

– devierea atenției de la puternica presiune sub care s-a aflat preşedintele Mihail Saakashvili, ca urmare a incapacității de a realiza reformele sociopolitice şi economice asumate prin *„Revoluția trandafirilor”*.

Nu este de neglijat nici momentul ales pentru începerea ostilităților, respectiv în ajunul deschiderii Olimpiadei de vară de la Beijing, mizându-se, în mod evident (indiferent de cine a fost autorul moral al declanşării ostilităților militare), pe impactul redus la nivelul opiniei publice al războiului.

De asemenea, obiectivul militar al Rusiei a avut multiple valențe politice, în măsura în care ocuparea Georgiei oferea Moscovei posibilitatea de a scăpa de preşedintele Mihail Saakashvili, precum şi de a transmite un mesaj SUA şi NATO privind apartenența statului georgian la sfera sa de influență. ***Din această perspectivă, acțiunea militară rusă poate fi considerată un mesaj al Moscovei la adresa SUA privind capacitatea Rusiei de a iniția acțiuni împotriva oricăror interese americane din spațiul euroasiatic, fără ca Washington-ul să poată iniția acțiuni de retorsiune.***

Faptul că Moscova nu a reuşit să îl elimine (politic ori fizic) pe Saakashvili nu înseamnă că aceasta nu şi-a atins şi scopul politic. Mult mai important este faptul că acest conflict a oferit Rusiei o „fereastră de oportunitate”[15] în demersul de revizuire a arhitecturii europene de securitate, rezultată la sfârşitul Războiului Rece.

[15] Termen utilizat de George Friedman (The Russo-Gorgian War and the Balance of Power, articol disponibil la www.stratfor.com) pentru a evidenția faptul că Rusia va utiliza acest conflict pentru a impune un nou „echilibru” în relațiile cu Occidentul, marcat de trasarea unor noi sfere de influență.

Acțiunea militară a Rusiei a contribuit, pe de o parte, la restabilirea credibilității armatei ruse ca forță redutabilă de luptă, cel puțin în mentalul societății ruse şi, pe de altă parte, la relevarea ineficienței garanțiilor de securitate oferite de SUA unui stat partener/aliat (în speță Georgia) în condițiile în care capacitățile militare americane erau dispersate în două teatre majore de operațiuni (Afganistan şi Irak).

Scenarii ante bellum

Abhazia şi Osetia de Sud	*Best case scenario*	independența față de Georgia
	Middle case scenario	menținerea *statu quo*-ului
	Worst case scenario	reintegrarea în Georgia şi acceptarea unei autonomii lărgite în cadrul statului georgian
Georgia	*Best case scenario*	reluarea controlului asupra celor două republici separatiste
	Middle case scenario	pierderea definitivă a celor două republici separatiste, însă sporirea sprijinului politic şi economic din partea Occidentului şi accederea în NATO
	Worst case scenario	pierderea celor două provincii şi reintrarea în sfera de influență a Rusiei
Federația Rusă	*Best case scenario*	schimbarea regimului de la Tbilisi, atenuarea (chiar schimbarea) orientării prooccidentale a Georgiei şi consolidarea controlului asupra Abhaziei şi Osetiei de Sud
	Middle case scenario	susținerea independenței celor două provincii georgiene şi integrarea lor în structurile politice şi de securitate controlate de Moscova
	Worst case scenario	integrarea Georgiei în structurile europene şi euroatlantice şi transformarea acesteia într-un model de urmat de alte state ex-sovietice (Ucraina, Republica Moldova, Azerbaidjan)

Analiza conflictului

► **Principala interpretare** dată evenimentelor din august 2008 a fost acea că atacul Rusiei asupra Georgiei reprezintă o primă etapă a unei politici externe a Moscovei mult mai militantă față de anii precedenți, care ar avea drept scop reluarea controlului asupra unor părți din fostul „imperiu sovietic”[16].

[16] King, Charles, “The Five-Day War” în *Foreign Affairs*, vol. 87, no. 6/2008, 2008, pp. 2-11.

Sub impactul evenimentelor din Caucaz, mulți analiști au considerat că viitorul pas al Moscovei va fi preluarea sub control a Ucrainei[17]. Însă, acest raționament exclude posibilitatea ca războiul ruso-georgian să fi avut drept principal resort disensiunile ireconciliabile dintre cele două state, care nu pot fi replicate în altă parte. *„Teoria refacerii imperiului"* a fost ușor acceptată și pentru că generează o predicție foarte clară cu privire la răspunsul politic al Occidentului, centrat pe ideea confruntării cu Moscova.

Această abordare este susținută de:

a) activismul acțional al Moscovei din lunile premergătoare conflictului, cu vădită tentă antigeorgiană

Declanşarea conflictului a oferit posibilitatea reanalizării *post factum* a unor acțiuni ale Moscovei din prima jumătate a anului 2008, care – dacă ar fi fost corect decriptate – ar fi putut constitui sursa unor semnale de avertizare asupra intențiilor reale ale Federației Ruse. Demersurile Moscovei au vizat:

a.1.) *stabilirea unor mecanisme de relaționare oficială cu republicile separatiste*, acestea fiind inițial interpretate drept simple contra-reacții la declararea independenței provinciei Kosovo.

Relevante din acest punct de vedere sunt:

- retragerea în mod oficial (6 martie 2008) a sancțiunilor economice impuse Abhaziei de către Comunitatea Statelor Independente (facilitând accesul produselor și investițiilor ruse în regiune) în 1996;
- emiterea de către Vladimir Putin a unei directive (din 16 aprilie 2008) privind autorizarea relațiilor guvernamentale directe cu Abhazia și Osetia de Sud, respectiv a serviciilor consulare, urmare a numărului ridicat de deținători de pașapoarte ruseşti în cele două regiuni;
- derularea unor negocieri directe între autoritățile ruse și abhaze pentru semnarea unui acord privind transferul cetățenilor ruşi în închisorile din Abhazia.

Deşi cele două provincii separatiste aveau deja conexiuni semnificative cu Federația Rusă în multiple domenii, aceste acțiuni au fost mai degrabă simbolice, sugerând deopotrivă „consolidarea graduală a independenței acestora"[18]. Mai mult, o rezoluție a Dumei de Stat, din 21 martie 2008, a recomandat Kremlinului recunoaşterea independenței Abhaziei, Osetiei de Sud şi Transnistriei.

[17] Aron, Leon, "Russia's Next Target Could be Ukraine" în *Wall Streat Journal*, sept. 2008.
[18] Allenova, Olga, *Russia Armed with Rebel Republics. For the NATO summit next month, Kommersant*, 11 martie 2008, disponibil la http://www.kommersant.com.

a.2.) *consolidarea prezenței militare ruse în Abhazia şi în apropierea coridorului Roki*

- Prima acțiune relevantă a Moscovei, în acest sens, a avut loc la 6 martie 2008, când Federația Rusă s-a retras în mod unilateral din Tratatul CSI referitor la interdicția de a livra sprijin militar regiunilor separatiste din Georgia.
- Ulterior, Moscova a utilizat incidentul din 20 aprilie 2008, generat de survolarea de către o dronă georgiană a spațiului abhaz[19], drept pretext pentru creşterea numărului „pacificatorilor ruşi" din Abhazia de la 458 la 3 000, limită impusă, de altfel, prin decizia Reuniunii şefilor de state ai CSI din 22 august 1994.
- Însă, în afara forțelor convenționale, Moscova a transferat în regiune şi capacități militare ce excedau utilizării lor de către trupe specializate în menținerea păcii, respectiv sisteme avansate de artilerie sau sisteme antiaeriene.
- Mai mult, la 31 mai 2008, Rusia a deplasat în Abhazia, fără consimțământul Georgiei, 400 de militari ruşi pentru refacerea infrastructurii feroviare a acestei regiuni.
- Pe fondul derulării exercițiului militar Kavkaz 2008, trupele ruse au rămas staționate în apropierea graniței cu Osetia de Sud, alimentând temerile privind o eventuală invazie. Unul dintre motivele invocate ulterior de reprezentanți ai armatei ruse pentru menținerea trupelor în Caucazul de Nord şi după 2 august, data încheierii exercițiului militar, a fost tocmai concentrarea trupelor georgiene în apropierea graniței cu Osetia de Sud.

În opinia majorității mediilor occidentale de analiză, dar şi din Federația Rusă, politica Moscovei față de Georgia a fost favorizată inclusiv de refuzul unor state europene, în special Germania şi Franța, de a amâna acordarea Membership Action Plan Georgiei la Summitul de la Bucureşti, situație asimilabilă de Moscova cu „un cec în alb"[20]. Din acest punct de vedere, acțiunile provocatoare ale forțelor militare separatiste din Osetia de

[19] Pe fondul doborârii acesteia de către un avion rus MIG-29, atât autoritățile de la Tbilisi, cât şi cele de la Moscova au reluat acuzele reciproce privind violarea acordului de încetare a focului, ca urmare a survolării zonei de securitate.

[20] Malek, Martin, „The Unknown Prelude to the Five Day War" în *Caucasian Review of International Affairs*, vol. 3/2009, pp. 227-232, disponibil la http://www.cria-online.org.

Sud la granița cu Georgia, întreprinse după 2 august, ar putea fi considerate un mijloc de a determina un răspuns din partea autorităților georgiene, care să determine intervenția rusă[21].

b) pregătirea anticipată a ofensivei forțelor militare ruse în Osetia de Sud şi, ulterior, în Abhazia şi Georgia

Chiar şi pentru observatori nefamiliarizați cu tehnicile militare, reacția rapidă şi masivă a trupelor ruse[22] într-un spațiu geografic muntos a apărut drept o acțiune pregătită cu atenție. O serie de foşti colaboratori ai lui Vladimir Putin, printre care Modest Kolerov, fost şef al departamentului pentru relații intraregionale şi culturale cu țările străine din cadrul Preşedinției Ruse, precum şi Andrei Illarionov, fost consilier economic al prim-ministrului rus, au susținut teoria atacului premeditat al Rusiei asupra Georgiei[23].

Mai mult, pătrunderea trupelor ruse, la 10-11 august, în interiorul teritoriului georgian pe două direcții principale, staționarea acestora la 50-60 km de Tbilisi, inclusiv după semnarea acordului de încetare a focului, din 15 august 2008, precum şi zvonurile legate de posibila răsturnare a regimului Saakashvili au alimentat această interpretare.

Prelungirea staționării forțelor militare ruse în Georgia, până la 9 octombrie 2008, a jucat un rol important în ceea ce priveşte evaluarea intențiilor Federației Ruse. Simpla ocupare a teritoriului georgian a generat, cu fiecare zi, deteriorarea tot mai clară a relațiilor ruso-occidentale, relevând faptul că autoritățile de la Moscova erau dispuse să accepte costuri din ce în ce mai mari pentru a-şi apăra interesele în Caucaz. Pe acest fond, unii analişti au avansat chiar ipoteza că Rusia nu se va retrage din Georgia, absorbind *de facto* o parte din teritoriul georgian.

c) reconceptualizarea politicii de securitate a Federației Ruse

Fără a fi un factor declanşator, războiul ruso-georgian a reprezentat pentru Federația Rusă un catalizator al operării, în regim de urgență, a unor schimbări în plan conceptual (nivel strategic), structural (nivel tactic şi operațional) şi relațional (avansarea propunerii de edificare a unei noi arhitecturi de securitate regională).

---

[21] La 5 august 2008, o comisie tripartită de monitorizare care cuprindea observatori OSCE şi reprezentanți ai forțelor de pacificare ruse au înaintat un raport, semnat inclusiv de comandantul trupelor ruse, generalul Marat Kulakhmetov, în care se menționa derularea unor atacuri asupra unor sate georgiene.

[22] Estimate la 25 000 militari şi 1 200 tancuri.

[23] Whitmore, Brian, "Did Russia Plan Its War in Georgia?", *Radio Free Europe*, 15 august 2008, disponibil la http://www.rferl.org, 2008.

Reconceptualizarea principalelor documente strategice[24], demersurile de operaționalizare a Forței Colective de Reacție Rapidă a OTSC şi accelerarea procesului de restructurare/modernizare a forțelor armate naționale reflectă congruența gândirii în interiorul elitei politico-militare ruse în ceea ce priveşte percepția asupra imposibilității depăşirii, pe termen mediu şi lung, a rivalității dintre Rusia şi Occident.

► **O interpretare alternativă** a motivațiilor Rusiei în Georgia poate fi evidențiată de logica jocurilor de semnalizare propusă de Cho şi Kreps[25]. Mulți analişti occidentali au susținut că unul dintre principalele motive acționale ale Moscovei în conflictul cu Tbilisi a fost decizia NATO de a continua extinderea spre Est, prin posibila încorporare a Georgiei şi Ucrainei. Potrivit acestora, deşi a tolerat integrarea în NATO a unor foste state comuniste din centrul şi estul Europei, Rusia a asimilat accesul Ucrainei în spațiul de securitate euroatlantic drept una dintre cele mai mari amenințări la adresa propriei securități[26] (aspect confirmat şi de recenta *Doctrină militară*, ratificată de preşedintele Medvedev).

Analizând această ipoteză din perspectiva *teoriei jocurilor de semnalizare*, războiul ruso-georgian ar putea reprezenta modalitatea aleasă de Moscova pentru a atrage atenția Occidentului asupra intolerabilității accesului celor două state ex-sovietice în Alianța Nord-Atlantică. Deşi autoritățile ruse au transmis în repetate rânduri semnale privind opozabilitatea proiectelor de extindere ale NATO spre Est față de interesele sale strategice[27], în logica teoriei lui Cho şi Kreps, invadarea Georgiei ar reprezenta o acțiune premeditată şi un risc asumat de către Moscova în termeni de costuri politice şi economice.

Acest lucru nu înseamnă că acțiunea militară disproporționată a Rusiei împotriva Georgiei a avut un scop limitat, respectiv doar de a semnala iritabilitatea în raport cu proiectele de securitate ale Occidentului.

În afara obiectivului (minimal) inițial, de consolidare a prezenței militare ruse în Abhazia şi Osetia de Sud, cu siguranță, Moscova a avut mai multe scenarii de acțiune, funcție de derularea conflcitului, inclusiv înlăturarea lui Saakashvili şi instaurarea unui regim servil (în logica teoriei sferelor de influență).

---

[24] Strategia de securitate națională a Federației Ruse până în anul 2020, Concepția privind Combaterea Terorismului şi Doctrina militară a Federației Ruse.

[25] Cho, In-Koo; Kreps, David M., „Signaling Games and Stable Equilibria" în *The Quarterly Journal of Economics*, Vol. 102, No. 2/1987, pp. 179-221, disponibil la http://www.econ.yale.edu.

[26] Friedman, George, op.cit, p. 3.

[27] Elocvent, în acest sens, fiind discursul lui Vladimir Putin de la Munchen din februarie 2007.

Totodată, următorii paşi ai Moscovei par a sugera că războiul din Caucaz a reprezentat, într-adevăr, un semnal adresat în primul rând statelor europene. Criza gazelor din ianuarie 2009 şi lansarea *Planului Medvedev*, de reconfigurare a arhitecturii europene de securitate, au determinat modificarea substanțială a atitudinilor majorității statelor europene față de Moscova.

Scenarii privind situația geopolitică din regiune

Conflictul ruso-georgian a evidențiat, pe de o parte, aspirațiile Moscovei de a-şi recăpăta statutul de mare putere şi, pe de altă parte, potențialul ridicat de influență pe care îl are în plan regional, într-un moment în care unitatea Europei în materie de politică externă era tot mai fragilă, iar atenția SUA era concentrată asupra teatrelor de conflict din Irak, Afganistan sau asupra pericolului potențat de Iran.

Atât conflictul în sine, cât mai ales evoluțiile subsecvente – recunoaşterea de către Moscova a independenței celor două republici separatiste, lansarea „planului Medvedev" de reconfigurare a arhitecturii europene de securitate, opoziția față de edificarea unui scut antirachetă în Europa, relația tensionată cu regimul Iuşcenko – constituie premise de reconceptualizare a unui nou tablou de securitate în Eurasia, în care Regiunea Extinsă a Mării Negre (REMN) capătă un rol tot mai important.

Configurația geopolitică actuală a zonei caucaziene, precum şi evoluțiile politico-economice, sociale şi militare din spațiile riverane ori aflate în proximitatea acestui spațiu conferă regiunii o importanță strategică majoră, din perspectiva:

– intersectării intereselor principalilor actori ai scenei internaționale, ce converg, însă, spre acelaşi obiectiv final, în speță obținerea/prezervarea statutului de „putere decizională" în zonă;

– afirmării opțiunii Georgiei de accelerare a demersurilor de aderare la structurile nord-atlantice şi comunitare;

– potențialului de insecuritate conferit de celelalte conflicte înghețate (din zonele Transnistria - Republica Moldova, Nagorno-Karabah - Azerbaidjan şi Armenia), respectiv de (re)activarea unor demersuri separatiste (Crimeea, Caucazul de Nord);

– divergenței intereselor în domeniul energetic, în special în ceea ce priveşte operaționalizarea unor rute de transport al hidrocarburilor dinspre Bazinul caspic către Europa.

În ceea ce priveşte contextul zonal de securitate, acesta este complet schimbat faţă de cel din vara anului 2008, reprezentative fiind:

– capacitatea redusă a Georgiei de a lansa o operaţiune militară majoră, în condiţiile în care în prezent dispune de capabilităţi limitate în raport cu vara anului 2008;

– concentrarea de semnificative trupe militare ruse în cele două provincii separatiste, fapt ce reprezintă principalul factor descurajant pentru autorităţile de la Tbilisi;

– amplificarea în plan intern a manifestărilor contestatare la adresa preşedintelui Mikhail Saakashvili şi suportul redus al populaţiei georgiene pentru o nouă acţiune în forţă;

– priorităţile autorităţilor ruse de a limita efectele crizei economice şi de a combate insurgenţa islamică din Caucazul de Nord.

Cum se vor răsfrânge aceste evoluţii asupra securităţii regionale, de la cea militară la cea energetică? Cum va fi modelat comportamentul statelor din regiune sau a actorilor globali, precum şi cel al organizaţiilor de securitate existente? Care vor fi următoarele „mişcări" ale Moscovei? Abordarea de către Moscova a relaţiilor cu Occidentul va urma în continuare raţionamentul confruntării? Pentru a răspunde la aceste întrebări este important să decelăm asupra unor posibile scenarii de evoluţie a securităţii spaţiului euroatlantic, în general, dar şi a bazinului pontic, în special.

► ***Un prim scenariu*** (*raţionamentul confruntării*) are la bază ipoteza menţinerii şi chiar amplificării politicii asertive a Rusiei în REMN, fiind de aşteptat ca Moscova să blocheze o prezenţă activă a UE şi NATO în acest areal.

Astfel, este previzibil ca Moscova să-şi consolideze prezenţa militară ori instrumentele de control politic, economic şi cultural în Ucraina, Armenia, Transnistria, precum şi în Abhazia şi Osetia de Sud, proiectând un „cordon sanitar", care ar avea rolul de prim inel strategic de apărare împotriva Occidentului. O atare perspectivă este susţinută de adoptarea recentă a noii Doctrine militare a Federaţiei Ruse care evidenţiază NATO drept principal inamic al Moscovei.

Din această perspectivă, instalarea scutului antirachetă în România şi Bulgaria va fi considerată de Moscova drept o ameninţare la adresa securităţii Federaţiei Ruse, fiind de aşteptat acţiuni de retorsiune, după modelul aplicat anterior în ipoteza edificării GMD american în Polonia şi Cehia.

Acest scenariu nu presupune neapărat o abordare a relaţiilor cu UE în termeni de ostilitate, fiind posibil ca Moscova să promoveze în continuare „politica relaţiilor bilaterale" cu state europene dezvoltate (Germania,

Franța, Italia, Spania) care să îi permită transferul de resurse energetice către Europa şi să accepte tacit, în contrapondere, anumite forme de relaționare a periferiei europene a fostului spațiu sovietic cu forurile comunitare în măsura în care acestea se mențin la un nivel incipient.

În condițiile activizării Moscovei ca jucător independent şi ostil Occidentului, extinderea NATO şi UE către Est ar fi o evoluție necesară ancorării REMN la evoluțiile din spațiul european şi euroatlantic. Integrarea Turciei în UE ar putea deveni o prioritate, având în vedere necesitatea de a contracara potențialul de convergență al intereselor ruso-turce la Marea Neagră. Similar, integrarea Republicii Moldova în UE şi a Georgiei în NATO ar putea fi accelerată, tocmai din considerentul agregării unui răspuns adecvat la acțiunile ostile ale Moscovei.

În contrapondere, este posibil ca Moscova să se concentreze pe influențarea evoluțiilor de politică internă şi externă ale Ucrainei, percepută de elita rusă drept pivot pentru asigurarea intereselor sale strategice în regiune. Temperarea atitudinilor prooccidentale ale Kievului ar genera avantaje multiple pentru Moscova:

- din punct de vedere militar, Moscova şi-ar putea asigura prelungirea prezenței navale ruse la Sevastopol;
- din punct de vedere energetic, asigurarea pentru Gazprom a unei participații confortabile la sistemul de transport al gazelor naturale din Ucraina ar consolida poziția Rusiei de furnizor major al Europei.

Pe acest fond, Rusia este posibil să persuadeze Ankara pentru a adera la strategia Moscovei de dezvoltare a unor *rute alternative* – „South Stream", „Blue Stream II" –, nefiind exclusă ipoteza potrivit căreia autoritățile turce să militeze pentru integrarea celor două proiecte concurente („Nabucco" *versus* „South Stream"), ca parte a strategiei de transformare a Turciei în „hub energetic".

Relațiile cu Tbilisi vor continua să fie tensionate pe întreaga durată a ultimului mandat al lui Mihail Saakashvili (expiră în 2013). Nu este exclus ca Moscova să alimenteze nemulțumirile interne din Georgia în perspectiva unei schimbări anticipate din funcție a actualului preşedinte georgian, respectiv să încerce să fructifice în propriul interes o nouă acțiune imprudentă a liderului georgian.

Având în vedere, însă, opțiunile majoritare existente atât la nivelul elitei politice, cât şi al populației cu privire la orientarea prooccidentală a țării, este puțin probabil ca Moscova să poată impune alegerea unui preşedinte cu viziuni clare proruse. De asemenea, persistența înghețului în relațiile bilaterale nu va

aduce beneficii Moscovei, accelerând procesul de integrare a Georgiei în structurile euroatlantice.

În pofida retoricii incendiare, este puțin probabil să aibă loc o reluare a unui conflict între Rusia şi Georgia în viitorul apropiat. Regiunile separatiste de graniță rămân puternic militarizate şi există un risc mare ca un act izolat de violență sau provocare să poată escalada rapid, în special de-a lungul frontierei sud-osetine, în zone precum Akhalgori şi Kveşi.

Pe termen scurt, situația de securitate din Osetia de Sud şi Abhazia va continua să fie imprevizibilă şi instabilă. Impunerea unei rezolvări acceptate la nivel internațional va fi dificilă ținând cont că cele mai multe state nu recunosc independența celor două provincii separatiste, plecând de la premisa integrității teritoriale şi suveranității Georgiei, în timp ce Rusia pretinde ca baza negocierilor să fie noua realitate.

► ***Al doilea scenariu*** (*paradigma cooperării*) ia în considerare REMN ca un areal suspendat între Occident şi Federația Rusă, ambele părți acceptând tacit, pe termen scurt şi mediu, *statu quo*-ul zonal din motive diferite. Pe acest fond, prioritățile autorităților ruse vor fi consolidarea statalității Abhaziei şi Osetiei de Sud, atragerea Ucrainei într-un parteneriat strategic, de natură a limita legăturile politico-militare ale acesteia cu Occidentul, depăşirea efectelor crizei economice, precum şi combaterea insurgenței islamice din Caucazul de Nord.

Totodată, având în vedere faptul că eforturile SUA se vor concentra asupra evoluțiilor din Orientul Mijlociu Extins, este de aşteptat ca Administrația Obama să vizeze atragerea Moscovei la dialog în cadrul platformelor de securitate existente. Un posibil subiect de dispută ar putea fi decizia Washington-ului de edificare a unui sistem de apărare antirachetă în sud-estul Europei, în măsura în care Moscova va considera că proiectul SUA vizează doar extinderea scutului antirachetă american prin elemente dislocate pe continentul european.

În contrapondere, lansarea „proiectului Medvedev" are scopul de a reliefa deschiderea Rusiei pentru depăşirea blocajului existent pe axa Est-Vest în ceea ce priveşte domeniul securității şi survine pe fondul preocupărilor occidentale de revitalizare a unor organizații consacrate (NATO, OSCE şi chiar UE). Momentul este cu atât mai prielnic pentru partea rusă cu cât la nivelul unor state europene există percepția necesității angrenării Federației Ruse într-un demers instituționalizat de consolidare a securității europene.

Realizarea acestui scenariu este alimentată de absența unei strategii coerente comune UE-NATO-SUA față de arealul lărgit al Mării Negre.

Pe fondul reticențelor existente la nivel comunitar față de aderarea Turciei la UE, este posibilă amplificarea coordonării acțiunilor turco-ruse la Marea Neagră, centrată pe cooperarea în domeniul energetic, „colaborarea tacită" în asigurarea stabilității în Caucazul de Sud şi respingerea oricăror ingerințe externe sau încercări de modificare a *statu quo*-ului în Marea Neagră. Relaționarea bilaterală ar putea trece în 2010 la un nivel superior, în cazul materializării proiectului comun de înființare a unui Consiliu pentru relații strategice de nivel înalt între Turcia şi Rusia.

Un potențial factor inhibator în substanțierea parteneriatului turco-rus este achiziționarea de către Moscova a unei/mai multor nave militare de tip Mistral (de la Franța), care modifică echilibrul relativ din Bazinul pontic în materie de *hard security*.

În ceea ce priveşte Abhazia şi Osetia de Sud, ca urmare a sprijinului de care beneficiază din partea Moscovei, acestea îşi vor consolida securitatea militară în raport cu Georgia, statutul lor internațional continuând să rămână neschimbat pe termen scurt şi mediu. Izolarea politico-diplomatică a Abhaziei şi Osetiei de Sud, dublată de dependența economică față de Federația Rusă ar putea determina replicarea modelului „Republicii Turce a Ciprului de Nord".

Amplificarea incertitudinii cu privire la statutul celor două regiuni va avea repercusiuni în plan economic pe termen lung şi va accentua dependența de investițiile provenite din Rusia în condițiile în care gradul de risc ridicat va descuraja investițiile din alte țări.

Beneficiind de o infrastructură turistică dezvoltată încă de pe vremea URSS şi apreciată la nivelul turiştilor din spațiul CSI, Abhazia are resurse de a-şi asigura din punct de vedere economic autonomia de Moscova, însă va depinde de afluxul de investiții ruse pentru modernizarea bazelor turistice.

De asemenea, gradul de integrare a Osetiei de Sud la infrastructura Federație Ruse se va amplifica pe termen lung, având în vedere dependența energetică (Gazprom va construi rețeaua de alimentare cu gaze din Osetia de Sud, urmând să asigure inclusiv livrarea de gaz către populație) şi, mai ales, inexistența unei legături cu mediul internațional, cu excepția celei prin Rusia.

Concluzii

Evoluția relațiilor dintre regiunile separatiste, sprijinite de Moscova şi Georgia, prezintă un grad ridicat de incertitudine, o eventuală reactivare a focarului putând genera efecte mai ales în plan regional, dar şi internațional.

► Atacul Rusiei asupra Georgiei a confirmat **fragilitatea şi impasul actualului sistem internațional (îndeosebi a cadrului normativ) de a acționa eficient în situații de criză** şi a readus în prim-plan acțiunea armată ca mod de rezolvare a diferendelor între subiecți de drept internațional.

► Federația Rusă a demonstrat că rămâne un **actor internațional impredictibil**, războiul ruso-georgian putând fi caracterizat drept o etapă în procesul inițiat de Moscova pentru reconfigurarea relațiilor cu Occidentul într-o direcție favorabilă propriilor interese.

► Moscova şi-a creat un cadru de negociere avantajos în Caucaz, Bazinul caspic, precum şi Regiunea Extinsă a Mării Negre, determinând modificări de poziție ale tuturor statelor din aceste zone în plan strategic, dar şi tactic sau operațional. Mai mult, Moscova a utilizat acest eveniment şi pentru a transmite Washington-ului un semnal cu privire la zona de influență asumată unilateral de Federația Rusă.

► În condițiile în care UE nu a devenit încă un *jucător* important în conceperea sau impunerea politicilor de securitate, SUA rămân singura putere care poate exercita presiuni asupra Moscovei.

► În absența unui angajament de securitate clar din partea Occidentului, Georgia poate fi în pericol de a fi „reabsorbită" în sfera de influență a Rusiei.

Anexa nr. 1

ANEXA 1
(http://en.wikipedia.org/wiki/2008_South_Ossetia_War)

Anexa nr. 2

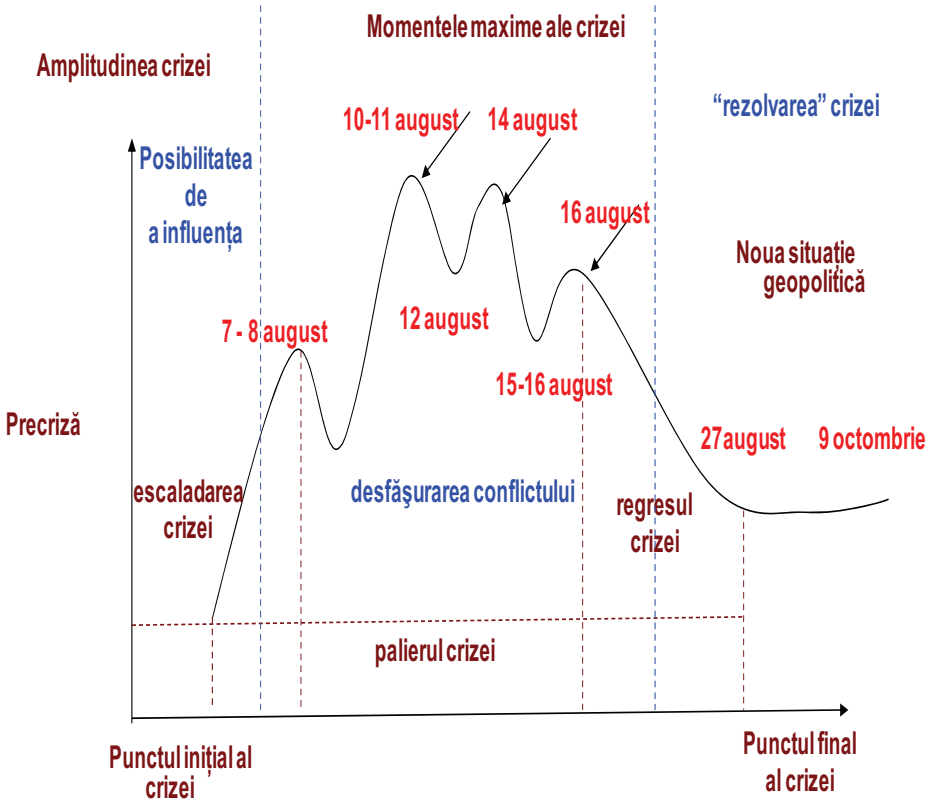
Etapizarea „crizei georgiene" – prezentare cronologică

Situație de risc potențială	→ **decembrie 1990** – Georgia şi Osetia de Sud au declanşat un nou conflict armat care durează până în 1992. → **iunie 1992** – liderii ruşi, georgieni şi osetini se întâlnesc la Soci pentru a semna un armistițiu şi a conveni asupra înființării unei forțe tripartite de menținere a păcii. → **noiembrie 1993** – Osetia de Sud redactează propria Constituție. → **noiembrie 1996** – Osetia de Sud îşi alege primul preşedinte. → **decembrie 2000** – Rusia şi Georgia semnează un acord interguvernamental pentru restabilirea economiei în zona de conflict. → **decembrie 2001** – Osetia de Sud îl desemnează pe Eduard Kokoitî drept preşedinte al Republicii, în 2002 acesta cere Moscovei să îi recunoască independența şi să accepte integrarea sa în teritoriul rus. → **ianuarie 2005** – Rusia aprobă planul Georgiei de acordare a unui statut de autonomie extinsă Osetiei de Sud în schimbul renunțării la ambițiile de dobândire a independenței. → **noiembrie 2006** – populația Osetiei de Sud susține în cadrul unui referendum decizia de separare a teritoriului de Georgia. Premierul georgian declară că acest demers face parte din planul Rusiei de provocare a unui conflict armat. → **aprilie 2007** – Parlamentul georgian aprobă o lege privind înființarea unei administrații temporare în Osetia de Sud, intensificând tensiunile în relațiile cu Rusia. → **iunie 2007** – separatiştii osetini susțin că Georgia a atacat Thinvali prin tiruri de mortieră şi focuri trase de lunetişti, acuzații respinse de Tbilisi. → **octombrie 2007** – negocierile dintre Georgia şi Osetia de Sud, mediate de OSCE, eşuează.
Situație de risc emergentă	→ **6 martie 2008** – Rusia se retrage în mod unilateral din Tratatul CSI referitor la interdicția de a livra sprijin militar regiunilor separatiste din Georgia. → **21 martie 2008** – printr-o rezoluție, Duma de Stat recomandă Kremlinului recunoaşterea independenței Abhaziei, Osetiei de Sud şi Transnistriei. → **martie 2008** – Osetia de Sud cere comunității internaționale să recunoască independența sa, după secesiunea Kosovo de Serbia.

	→ **martie 2008** – Eforturile Georgiei de aderare la NATO, deşi lipsite de succes, determină Duma de Stat de la Moscova să ceară Kremlinului să recunoască independența Osetiei de Sud şi a Abhaziei. → **aprilie 2008** – Osetia de Sud respinge o propunere georgiană de împărțire a puterii şi insistă asupra obținerii independenței. → **aprilie 2008** – transferul a aproximativ 1 500 soldați georgieni în defileul Kodori, un subiect de dispută între Georgia şi Abhazia. → **16 aprilie 2008** – prim-ministrul rus Vladimir Putin emite o directivă prin care autorizează relațiile guvernamentale directe cu Abhazia şi Osetia de Sud. → **20 aprilie 2008** – o dronă georgiană care survola *Zona de securitate* din Abhazia este doborâtă de un avion rus MIG-21. → **sfârşitul lui aprilie 2008** – 12 000 de soldați georgieni sunt cantonați la Senaki (în apropierea Abhaziei), iar 6 000 de soldați ruşi sunt transferați în provincia separatistă. → **mai 2008** – derularea exercițiilor militare *Kavkaz 2008* (trupe ruseşti) şi *Immediate Response* (trupe georgiene şi americane). → **31 mai-1 august 2008** – trupele ruse refac infrastructura feroviară a Abhaziei. → **1-7 august 2008** – schimburi de focuri şi ciocniri militare zilnice în zona de securitate din Osetia de Sud.
Conflictul ruso-georgian (7-27 august 2008)	→ **7-8 august 2008** – atacul terestru georgian asupra pozițiilor osetine din capitala Thinvali. → **8-10 august 2008** – riposta generală militară rusă (*Bătălia pentru Thinvali*). → **12-13 august 2008** – ofensiva trupelelor abhaze în defileul Kodori. → **14 august 2008** – ocuparea de către trupele ruse a portului georgian Poti. → **16 august 2008** – raiduri ale trupelor ruse în oraşul georgian Kaspi (50 km de Tbilisi).
Situație de risc latentă	→ **15-16 august 2008** – semnarea acordului de pace, mediat de preşedintele francez Nicolas Sarkozy. → **25-26 august 2008** – recunoaşterea de către Moscova a independenței Abhaziei şi Osetiei de Sud. → **9 octombrie 2008** – retragerea trupelor ruse. → până în prezent, independența celor două republici separatiste a mai fost recunoscută de Nicaragua, Venezuela şi Nauru (în cazul Abhaziei). ***Noua realitate geopolitică***

Anexa nr. 3

Evoluția grafică a conflictului ruso-georgian



Bibliografie

Cărți

1. Bozeman, Adda, *Strategic Intelligence and Statecraft*, Washington DC, Pergamon-Brassey's, 1992.
2. Berkowitz, Bruce; Goodman Allan, *Best Truth – Intelligence in the Information Age*, Yale University Press, 2000.
3. Mandel, T. F., "Future Scenarios and Their Use in Corporate Strategy" în *The Strategic Management Handbook*, New York, Ed. H. J. Albert, 1983.
4. Clark, M. Robert, *Intelligence Analysis: A Target – Centric Approach*, Washington DC, CQ Press, 2007.
5. Grabo, Cynthia, *Anticipating Surprise: Analysis for Strategic Warning*, Joint Military Intelligence College, Washington, 2002.
6. Newman, Edward; Richmond, Oliver, *Challenges to Peacebuilding: Managing Spoilers During Conflict Resolution*, New York, United Nations University Press, 2006.
7. Russell, Richard, *Sharpening Strategic Intelligence: Why the CIA Gets it Wrong, and What Needs to be Done to Get it Right*, Cambridge University Press, 2007.
8. Waltz, Kenneth, *Man, the State and War*, New York, Columbia University Press, 1954.

Articole în reviste şi publicații (inclusiv on-line)

1. Allenova, Olga, "Russia Armed with Rebel Republics. For the NATO summit next month" în *Kommersant*, 11 martie 2008.
2. Aron, Leon, "Russia's Next Target Could be Ukraine" în *Wall Streat Journal*, septembrie 2008.
3. Friedman, George, "The Russo-Gorgian War and the Balance of Power", articol disponibil la www.stratfor.com.
4. Cho, In-Koo; Kreps, M. David, „Signaling Games and Stable Equilibria" în *The Quarterly Journal of Economics*, vol. 102, no. 2/1987, disponibil la http://www.econ.yale.edu.
5. King, Charles, "The Five-Day War" în *Foreign Affairs*, vol. 87, no. 6/2008.
6. Malek, Martin, "The Unknown Prelude to the Five Day War" în *Caucasian Review of International Affairs*, vol. 3/2009, disponibil la http://www.cria-online.org.
7. Nye, S. Joseph Jr., "Peering into the Future" în *Foreign Affairs* July/August 1994.
8. Whitmore, Brian, "Did Russia Plan Its War in Georgia?", *Radio Free Europe*, 15 august 2008, disponibil la http://www.rferl.org.

Alte surse Internet
www.sri.ro
www.stratfor.com
www.kommersant.com
www.rferl.org

Lucrări prezentate la seminarii şi conferinţe
1. Heinrich, H. G., "Frozen Crisis in the Caucasus: Can the Circle Be Unsqaured?", *31st Viene Seminar*, Diplomatic Academy, 2001.

Ionel NIŢU este absolvent al Academiei Naţionale de Informaţii *„Mihai Viteazul"* şi are un master în relaţii internaţionale şi integrare europeană la Şcoala Naţională de Studii Politice şi Administrative, respectiv un master în studii de securitate la Facultatea de Sociologie (Universitatea Bucureşti). Este expert în analiza de intelligence, fiind implicat în pregătirea şi susţinerea de cursuri de pregătire pentru analiştii din serviciile de informaţii, precum şi autor al unor studii privind managementul procesului de analiză şi prognoza de intelligence.

Lectura activă – principiu în analiza informațiilor. De la „lectura" faptelor, la „lectura" semnificațiilor

Conf. univ. dr. Irena DUMITRU
Acedemia Națională de Informații *„Mihai Viteazul"*
e-mail: **irenachiru@yahoo.com**

Motto

„Adevărata problemă a erei informaționale nu este de natură tehnologică; mai degrabă, problema ne priveşte pe noi – ce să gândim, la ce să ne gândim (...) utilizând noile metode analitice, noile instrumente conceptuale cu care să analizăm şi să înțelegem produsele minții umane."

(Keith Devlin, 1997 *apud* Moore, 2007)

Abstract

Defined as a "process of transforming intelligence to be collected in any way[1] in a product which may be used by the decision makers and the military decision-makers" (Shulsky and Schmitt, 2008, 79), intelligence analysis involves two key sub-processes[2]: reading and drafting.

The premise from which we start is that ***we cannot conceive intelligence analysis without reading intelligence which the analytical product is based on*** *and, subsequently, in the absence of "translating" the conclusions into intelligence ready to be used.*

This article will refer to the former of the two sub-processes, trying to define those parameters of active reading which should allow drafting an intelligence product: differentiating perspectives, identifying social, political and economic factors, separating facts from opinions and identifying and interpreting the biases existing in the text. ***We do not read to criticize, to agree or disagree, but to obtain the intelligence from the text.*** *The premise – a text is not a verdict with respect to the given subject, but it is the object of interpreting and evaluating. In*

[1] "To be collected in any way" means by different sources either – OSINT, or covert – HUMINT, SIGINT. This is the typology more often offered by literature. There are also classifications which include more INTs – for example, IMINT, ELINT, COMINT, FISINT.
[2] Not reducing to these two processes.

other words, getting accustomed to the active reading principles may help us in becoming knowledgeable readers, the more so within the present-day technological environment, when the Internet allows anyone, anytime and anywhere to be able to pose as an information source.

Keywords: intelligence analysis, active reading.

Abilitatea de a citi se formează gradual, începând cu studiile primare, când învățăm să parcurgem cuvânt cu cuvânt fraze şi frază cu frază texte, când cunoaşterea unui subiect se rezumă la o singură sursă şi când lectura ne este dublată de credința că un text descrie cu acuratețe realitatea în cauză. Aceasta este „lectura nonactivă", care oferă doar fapte şi un tip de cunoaştere bazată pe memorarea conținuturilor unui text. Spre exemplu, un cititor nonactiv va lectura o lucrare de istorie pentru a cunoaşte evenimentele/faptele trecutului şi interpretarea dată acestor evenimente.

Prin comparație, pentru un cititor activ, textul[3] va oferi doar o variantă de interpretare a faptelor sau perspectiva unui autor despre subiectul respectiv: cititorul activ va înțelege „ce spune" textul, dar şi „cum reprezintă" textul problema în cauză. Practica lecturii active ne ajută să înțelegem că fiecare text este creația unică a unui anumit autor şi să evaluăm modalitatea în care o perspectivă asupra evenimentelor sau o selecție a evenimentelor poate determina un anumit mod de reprezentare a realității descrise (incomplet/complet, obiectiv/partizan). Cu alte cuvinte, alegerile pe care orice autor le face în procesul de elaborare şi redactare a unui text, la nivelul conținutului, limbajului şi structurii specifice, trebuie evaluate deoarece au efecte asupra semnificației atribuite textului în cauză.

În termenii analizei informațiilor, se impune ca lectura să fie una activă: obiectivul lecturii nu se poate rezuma la înțelegerea „a ceea ce se spune". Pe acest palier, lectura trebuie să permită identificarea şi înțelegerea perspectivelor, a *bias*-urilor şi a subînțelesurilor, în sensul în care **trebuie să vedem cum lumea este portretizată de un text şi nu să vedem lumea aşa cum este portretizată de un text**.

Din literatura de specialitate a ultimilor şase decenii – fundamentată pe experimente şi exemple oferite de realitate – am învățat că **informația este rareori neutră**. Datele, utilizate în mod selectiv pentru a compune informații, reprezintă doar puncte de vedere ale unei surse/autor. Problema

[3] Utilizăm termenul de „text" în sens generic, ca suport al unei informații (i.e. discurs (scris), articol de presă etc.).

evaluării a devenit tot mai dificilă odată cu necesitatea integrării informațiilor conținute de internet, mediu de comunicare a cărui popularitate l-a transformat rapid în ținta perfectă a mizelor şi *parti-pris*-urilor comerciale, politice, sociale.

Rezultă că pe palierul surselor deschise de informare (OSINT), arii supuse utilizării „interpretative" a datelor, este necesară aplicarea unor instrumente de evaluare şi validare a informațiilor, instrumente care să permită identificarea diverselor grade de interpretare a decupajului de realitate în informație, determinarea măsurii în care realitatea relevantă este descrisă adecvat, detectarea modificărilor apărute pe parcursul observării, interpretării şi transmiterii (de la o sursă la alta), identificarea erorilor de conceptualizare sau a persoanelor care au generat deformarea. Lectura activă în sine nu asigură atingerea acestor obiective, însă susține demersul de obținere a unui grad cât mai mare de obiectivitate în elaborarea produselor de informare.

Lectura ideilor şi lectura cuvintelor. Rolul inferențelor

În registru ideal[4], procesele de comunicare sunt caracterizate de izomorfism între ceea ce intenționează emițătorul să comunice şi ce comunică de fapt, precum şi între semnificația pe care emițătorul intenționează să o transmită şi cea pe care o ataşează receptorul. În realitate, înțelegerea a ceea ce citim sau auzim se realizează în pondere importantă în mod indirect, prin inferențe. Un text dat nu conține *per se* semnificația. Cititorul este cel care construieşte semnificația pe baza cunoştințelor sale preexistente, pe baza convențiilor sociale, pe baza unor date pe care le deține despre autor („X nu ar afirma aşa ceva!"), despre context („Nimeni nu ar declara aşa ceva cu ocazia unui asemenea eveniment!") sau despre audiență („X nu ar recunoaşte o asemenea faptă în public!"). Cu alte cuvinte, **în calitate de cititori facem inferențe având ca resort convenții, cunoştințe, experințe şi valori împărtăşite social**. Citim mai degrabă idei decât cuvinte şi facem inferențe în detrimentul identificării semnificației intenționate de autor.

Pentru a ilustra, vom lua exemplul frazei următoare: *„Preşedintele a recunoscut că arma cu care a fost împuşcată soția sa îi aparținea"*. Dincolo de ceea ce fraza conține în mod explicit (recunoaşterea proprietății armei),

[4] A se citi „utopic".

deducem că preşedintele era căsătorit şi că soţia sa a decedat. Mai mult, deducem că: există un preşedinte, preşedintele deţine o armă, preşedintele este căsătorit, soţia sa a decedat, arma i-a provocat moartea, preşedintele a recunoscut că arma îi aparţinea.

Într-un alt plan, rezultă că o persoană publică este implicată într-un caz de crimă, arma (sau cel puţin glonţul) a fost probabil recuperată şi identificată ca armă a crimei (altfel, asumarea proprietăţii armei de către preşedinte nu ar avea sens). În egală măsură, trebuie să recunoaştem că nu ştim dacă afirmaţia preşedintelui este adevărată, dacă preşedintele este vinovat sau a fost implicat în moartea soţiei sau dacă aceasta din urmă a murit în urma unei împuşcături (putea fi lovită cu arma respectivă), dacă a fost crimă, accident sau sinucidere. Parte din inferenţele integrate inerent în procesul de gândire sunt justificabile, parte nu.

În economia prezentului articol, abordarea problemei inferenţelor are o dublă justificare. În primul rând, pentru a ilustra teza conform căreia „informaţiile nu sunt neutre", ele putând fi fundamentate de inferenţele autorului/sursei. În al doilea rând, pentru a explica rolul inferenţelor care dublează inerent lectura, evaluarea şi analiza acestor informaţii.

Inferenţa are ca resort nevoia de a da înţeles, de a găsi semnificaţii, de a atribui scopuri şi cauze. Este un proces mental prin care este extrasă o concluzie generală din mai multe fapte particulare. Indivizii inferează motivaţii, scopuri şi intenţii. Interpretează acţiuni particulare ca fiind exemple ale unor *pattern*-uri de comportament, ale unor intenţii sau sentimente. Conchidem că plouă dacă cineva şi-a deschis umbrela. Sau conchidem că informaţiile sunt veridice dacă este citată o voce avizată a domeniului în cauză.

Inferenţele nu sunt întâmplătoare. Pot fi presupuneri, însă sunt *presupuneri educate*, adică bazate pe fapte (faptele ca probe ne conduc spre o anumită concluzie). Rezultă că, plecând de la aceeaşi referinţă, toţi indivizii vor ajunge la aceeaşi concluzie. Ceea ce nu se întâmplă în exemplele mai sus citate: umbrela poate fi o protecţie împotriva soarelui, iar citarea poate fi dezechilibrată cedând spaţiu doar unei părţi implicate într-o problemă controversată.

Soluţii pentru o lectură activă

Abilitatea de a citi activ presupune în primul rând **distanţare faţă de text**. Doar aceasta permite combinarea celor două paliere ale unui text: (1) ce informaţii îmi oferă textul? şi (2) cum este construit textul?, cum sunt

utilizate şi interpretate argumentele (fapte, exemple)?, cum ajunge autorul la concluziile prezentate? şi care pot fi variantele alternative de a analiza subiectul textului?

Ambele paliere sunt importante pentru înțelegerea unei probleme şi pentru elaborarea unui produs informativ bun, deoarece informațiile pot fi relevante prin raport cu tema produsului informativ, însă pot fi viciate (de exemplu prin distorsiune sau decontextualizare). Prin urmare, evaluarea combinată pe cele două paliere permite extragerea informațiilor relevante, dar deopotrivă veridice.

Punctual, un cititor activ va supune textul unei analize pe următoarele planuri: (1) **sursa/sursele informației** – permite evaluarea autorului informațiilor, dar şi a celor din spatele informației (surse primare, secundare etc.), (2) **conținutul informației**, (3) **modalitatea de exprimare** sau **tendința** care este, de cele mai multe ori latentă, ascunsă, dar cu un impact foarte puternic în planul percepției conținutului informației, (4) **argumentele conținute în text** sau **probele aduse**, care conferă sau nu temei informațiilor prezentate şi (5) **efectele** – impactul informației (formă şi fond) la nivelul receptorului (a se vedea tablelul *Paliere de analiză pentru o lectură activă*).

PALIERE DE ANALIZĂ PENTRU O LECTURĂ ACTIVĂ	
Evaluarea sursei (cine?)	Tipul publicației Background-ul autorului pe tema respectivă (alte articole) Cui se adresează autorul? Autorul are o abordare din interiorul sau din exteriorul problemei? Cum influențează acesta informațiile care sunt incluse/excluse în/din text?
Evaluarea informațiilor (ce?)	Care sunt premisele de la care pleacă autorul? Sunt acestea explicit sau implicit formulate? Depind premisele de contextul prezentat? Care este motivația autorului în a scrie un asemenea text? Care este scopul său? Există ale abordări teoretice sau aplicate care ar fi putut fi incluse în text? Cine/ce a fost exclus? Textul conține grafice, statistici, ilustrații? Sunt acestea prezentate şi dezbătute? Contribuie la argumentarea perspectivei autorului?
Identificarea tendințelor (cum?)	Care este atitudinea autorului? Stilul? *Bias*-urile? Termenii, stilul sau exemplele pun în evidență *bias*-uri? În ce măsură *bias*-urile diminuează credibilitatea autorului? Textul face apel la registrul emoțional? Invocă alte surse? Autorul își asumă textul sau tratează subiectul cu umor, satiră, ironie sau sarcasm? Care dintre aserțiuni sunt fapte şi care sunt opinii? Sunt prezentate opinii ca fapte? În ce măsură autorul simplifică ideile complexe? În ce măsură face apel la generalizări nejustificate? Inferențele sunt corecte? Autorul citează ideile altor surse în mod corect? Sau le distosionează şi le prezintă în afara contexului potrivit? Autorul face apel la tehnici de persuasiune (apelul la prejudecăți sau inducerea fricii)? Oferă textul o imagine echilibrată asupra problemei?
Analiza argumentelor (de ce?)	Care dintre aserțiunile autorului sunt exemplificate? Care nu? Sunt exemplele atribuite surselor în mod corect? Sunt exemplele actuale? Care dintre aserțiunile autorului sunt exemplificate şi argumentate? Care nu? La ce concluzii ajunge autorul? Sunt acestea justificate sau nu?
Analiza efectelor	Sunteți de acord cu perspectiva autorului? Care vă sunt propriile *bias*-uri în legătură cu subiectul în cauză? În ce măsură textul vă schimbă propriile valori, credințe, idei?

Un exemplu: lectura ştirilor

În contextul actual, mass-media reprezintă mijlocul de comunicare socială dominant, care propune receptării un flux continuu de date, fapte şi idei şi, în paralel cu informaţiile transmise, semnificaţii prin prisma cărora configurează o imagine despre lume. **Mass-media definesc realitatea** prin intermediul ştirii, al comentariului şi al ficţiunii, iar procesele fireşti de selecţie şi ierarhizare determină ceea ce este inclus şi ceea ce este exclus, impun anumite evenimente şi omit alte evenimente. Dincolo de faptul că deschid „ferestre spre lume", oferind perspective selective, mass-media interpretează, propun cadre explicative explicite sau implicite, bazate pe asocieri de idei, imagini cu semnificaţii latente, raţionamente cauzale „fireşti". În egală măsură, mass-media clasifică şi etichetează, realizând distincţii între ceea ce este normal şi deviant, acceptabil sau inacceptabil, nomic sau anomic.

Prin urmare, **reprezentările audiovizuale surprind realitatea dintr-una din perspectivele posibile**, iar informaţia oferită este o informaţie mediată. Actul de producere a ştirilor presupune, inevitabil, nu reproducerea, ci construirea realităţii (Tuchman, 1978, 12) în două sensuri: în primul rând, deoarece unele evenimente sunt creaţia mass-mediei (prin aceasta înţelegem că unele evenimente sunt create – de exemplu, interviul sau orice alt eveniment în sfera relaţiilor publice –, dar şi că unele evenimente primesc statutul de ştire şi un grad de importanţă doar pentru că sunt reprezentate mediatic), iar în al doilea rând, prin apel la teorema lui Thomas[5], presupunând că în măsura în care indivizii apreciază relatările mass-mediei ca fiind veridice, ei vor acţiona în consecinţă. „Poveştile" relatate sau create de media, indiferent de cât de false sunt, ajung să funcţioneze ca realitate (Lichtenberg, 1991, 221).

Ştirea reflectă contextul cultural în care este redactată. Jurnaliştii generează tipizări-sisteme operaţionale de clasificare a realităţii care traduc preferinţa acestora pentru întâmplări dramatice, cu impact puternic asupra audienţei şi faptele uşor de prezentat şi interpretat. Dacă jurnaliştii nu ar avea la dispoziţie „hărţi culturale ale lumii sociale" (Hall, 1992), ei nu ar putea descifra evenimentele neprevăzute care formează pentru audienţele lor conţinutul primar al valorii de ştire. La cel mai înalt nivel de generalizare, hărţile descriu societatea ca fiind fragmentată în sfere distincte, compusă din indivizi ale căror acţiuni sunt percepute ca fiind rezultatul faptelor, intenţiilor, motivaţiilor şi opţiunilor personale, ierarhizată centralizat din

[5] Conform teoremei lui Thomas, „o situaţie este reală prin consecinţele definirii ei ca reală" (Zamfir şi Vlăsceanu, 1998, 303).

punct de vedere social şi geografic şi, nu în ultimul rând, consensuală sau în acord cu un sistem central de valori.

Prin urmare, **ştirea** nu **este** o radiografiere perfectă a realităţii descrise, ci **un discurs cultural** şi **dependent de instanţe multiple**, care trebuie „citit" (interpretat) în mod activ. În acest sens, principiile lecturii active recomandă:

- Interpretarea evenimentelor din perspective multiple (interpretare multisursă: mai multe surse diferite şi nu exclusiv surse mass-media);
- Identificarea punctelor de vedere „închise" în ştire;
- Reconstruirea (rescrierea) ştirii din perspectiva celorlalte surse (cum ar reda sursa X acelaşi eveniment?);
- Evaluarea ştirii pe baza criteriilor clarităţii, acurateţii, relevanţei, profunzimii, amplorii şi semnificaţiei;
- Identificarea contradicţiilor din modul în care este redat evenimentul (frecvent întâlnite chiar în cadrul aceleiaşi ştiri);
- Identificarea „agendei ascunse" şi a intereselor care stau în spatele relatării;
- Identificarea faptelor acoperite, precum şi a celor omise din ştire;
- Identificarea punctelor de vedere prezentate sistematic în mod favorabil şi a celor prezentate sistematic în mod negativ.

Concluzii

În calitate de cititori, indivizii nu inferează cu rigoare matematică. Aceştia se bazează pe deducţie, dar şi pe cunoştinţe şi experienţe prealabile, credinţe şi presupuneri proprii. Cu alte cuvinte, inferenţele reflectă punctul de vedere al unui individ într-o situaţie dată. Inferenţele dublează în mod firesc comunicarea, fie ea verbală sau în scris. Frecvent, comunicatorii lasă să se înţeleagă unele lucruri şi vizează obţinerea unui efect în planul receptorilor mult peste ceea ce transmit explicit. Dar, în calitate de cititori activi, trebuie să cunoaştem tentaţia şi implicaţiile avansării de interpretări şi concluzii în absenţa unor date sau argumente şi, în contrapartidă, să citim cu mintea deschisă în faţa a cât mai mai multor variante alternative de interpretare.

O comparaţie ilustrativă pentru a conchide este oferită de Daniel Kurland (1994) – lectura unui text este similară privirii şi evaluării unui tablou:

> *„Când privim un tablou, conştientizăm că examinăm opera unui autor. Conştientizăm intenţia autorului din spatele operei, încercarea lui de a exprima ceva. Deoarece opera nu îşi exprimă sensul în mod direct şi explicit, efortul de a găsi sensul ne revine nouă. Privind la Mona Lisa, ştim că nu o privim pe Mona Lisa în sine, ci privim un tablou. Putem discuta pe tema semnificaţiei*

tabloului, dar şi pe tema modului de realizare a tabloului (...). Cu cât vom cunoaşte mai multe particularităţi ale tabloului, cu atât interpretarea dată de noi va fi mai solidă".

Însă, chiar acceptând această comparaţie, textele rămân aserţiuni „negru pe alb", care pot fi reformulate. Sunt „simboluri pe o pagină" (idem), pe care, ca şi cititori, le recunoaştem, dar le înţelegem (le atribuim semnificaţii) într-un context istoric şi social, integrând propriile aşteptări şi proiecţii. Indiferent de miza lecturii, dar cu atât mai mult când rezultatul este integrat procesului de analiză a informaţiilor, suntem responsabili de semnificaţia pe care o atribuim, precum şi de corelaţiile pe care le realizăm dincolo de „ceea ce se afirmă".

Bibliografie

1. Devlin, K., *Goodbye Descartes: The End of Logic and the Search for a New Cosmology of the Mind*, New York, John Wiley and Sons, 1997.

2. Hall, S., „The Question of Cultural Identity", în S. Hall, D. Held şi T. McGrew (coord.), *Modernity and Its Futures*, Cambridge, Polity Press, 1992.

3. Harnadek, A., *Critical Reading Improvement*, New York, McGraw-Hill, 1978.

4. Kurland, D., *I Know What It Says...What Does It Mean? Critical Skills for Critical Reading*, New York, Wadsworth, 1994.

5. Lichtenberg, J., „Objectivity as Strategic Ritual", în Curran, J. şi Gurevitch M. (coord.), *Mass-media and Society*, London, Arnold, 1991.

6. Moore, D. T., *Critical Thinking and Intelligence Analysis*, 2007, disponibil la http://www.ndic.edu/press/2641.htm, ultima accesare 22 martie 2010.

7. Paul, R. şi Elder, L., *How to Read a Paragraph The Art of Close Reading,* Dillon Beach, CA: Foundation for Critical Thinking, 2006.

8. Shulsky, A. N. Schmitt, G. J., *Războiul tăcut. Introducere în universul informaţiilor*, Iaşi, Editura Polirom, 2008.

9. Tuchman, G., *Making News: A Study in Construction of Reality*, New York, Free Press, 1978.

10. Zamfir, C., Vlăsceanu, L., *Dicţionar de Sociologie*, Bucureşti, Editura Babel, 1993.

Irena DUMITRU este conferenţiar universitar în cadrul Academiei Naţionale de Informaţii *„Mihai Viteazul"* şi doctor în sociologie (Universitatea Bucureşti, Facultatea de Sociologie şi Asistenţă Socială). A publicat, în calitate de unic autor, coautor şi coordonator, şase volume şi peste cincizeci de studii, articole de specialitate şi comunicări ştiinţifice. Domeniile sale de competenţă sunt: analiza de intelligence şi comunicarea publică şi instituţională.

Despre eşecurile în intelligence şi necesitatea unui proces „*After Action Review*"(*AAR*) în domeniul analitic

Drd. Cristian NIŢĂ
Academia Naţională de Informaţii *„Mihai Viteazul"*
e-mail: **cnita@dcti.ro**

Motto
„Noi nu suntem oameni de ştiinţă, noi suntem analişti. (...) Ştiinţa este ceea ce faci în laborator. (...) Ştiinţa e prea formală. Noi nu putem să efectuăm experimente aici. (...) nu ne interesează prea mult teoriile, ci faptele."[1]

Abstract
An intelligence failure is the inability of one or more parts of the intelligence process (collection, evaluation, analysis, production, dissemination) to produce timely, accurate intelligence on an issue or event of importance to national interest (Mark Lowenthal, 1985). But intelligence is not perfect and it is not a science, mistakes within an organization as a whole could occur and, naturally, failures are an inherent part of intelligence due to the reality of human and economic limitations. Economic limitations entail the allocation of scarce financial resources towards security threats.[2] So, what do we understand by an intelligence failure?
Keywords: intelligence failure, fault of knowledge, intelligence analysis, strategic surprise, deception.

Argument

Timp îndelungat, procesul de culegere a informaţiilor a constat în încercarea de a culege cât mai multe date, în speranţa de a afla ceva. Acest fapt explică parţial volumul foarte mare de date culese de comunitatea de

[1] Notă – traducerile din cadrul articolului aparţin autorului. Rob Johnston, Analytic Culture in the US Intelligence Community. An Etnographic Study, Washington, DC Press, 2005, chapter two – Findings, p. 20.
[2] Gustavo Díaz, „Methodological approaches to the concept of intelligence failure", *UNISCI Discussion Papers*, January 2005, p. 10, în http://www.revistas.ucm.es/cps/169962206/articulos/uni50505/30003a.pdf

informații. Dar direcționarea unei cantități uriaşe de date către analişti nu rezolvă problema, ci, dimpotrivă, poate genera eşecuri de intelligence. Activitatea care a fost mult timp exclusă din această ecuație a fost cea de analiză a informațiilor.

Analiştii de informații, prin metodele aplicate în vederea obținerii unei analize eficiente, urmăresc de fapt evitarea celor trei motive ale nereuşitei: eşecul în schimbul de informații, eşecul în analiza obiectivă a materialului obținut, eşecul beneficiarului cu privire la luarea în considerare a informației furnizate.[3]

Studiile au arătat că nu există o metodă sau metode de analiză standard în cadrul oricărei comunități de informații. Orice comunitate de informații dezvoltată este compusă dintr-o gamă variată de ramuri, fiecare cu propria metodă de analiză a informațiilor. Mai mult decât atât, analiştii de informații concep, în mod obişnuit, metode ad hoc de rezolvare a anumitor probleme intervenite în demersul analitic. Această abordare individualistă a condus la apariția a numeroase procedee, mai mult de 160 identificate ca fiind la dispoziția celor care se ocupă de analiza informațiilor în SUA.[4]

Rațiuni de ordin pozitiv proliferează aceste tehnici, dezvoltate în scopul rezolvării cu succes a problemelor specifice întâmpinate, unele fiind utilizate frecvent numai într-o singură ramură, cum ar fi analiza ştiințifică şi tehnică sau cea economică (aceasta din urmă beneficiază, probabil, de colecția cea mai bogată de metodologii de rezolvare a problemelor). Ca un exemplu despre înmulțirea metodelor, după colapsul Uniunii Sovietice economiştii, care îşi petrecuseră întreaga viață profesională analizând o economie la comandă, au fost puşi, brusc, în situația confruntării cu privatizarea şi cu prețuri ale pieței libere. Nicăieri nu există însă un model al analizei acestui tip de economie de tranziție, analiştii trebuind să improvizeze din metode disparate calcularea, de exemplu, a capacității sectorului privat al Rusiei.[5]

În aceeaşi măsură, succesul analizei depinde de acuratețea definirii conceptului, aşa cum unul dintre beneficiarii sistemului aprecia pe marginea eşecurilor în activitatea de informații: *„(...) câteodată, ceea ce ei [ofițerii*

[3] Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach*, Ed. CQ Press – A Division of Congressional Quarterly Inc., Washington DC, SUA, 2007, p. 6.
[4] Rob Johnston, op.cit., p. 70.
[5] Center for the Study of Intelligence, CIA, Watching the Bear: Essays on CIA's Analysis of the Soviet Union, conferință, Universitatea Princeton, martie 2001, www.cia.gov/cis/books/watchingthebear/article08.html, p. 8.

analişti – n.a.] cred că este important, de fapt nu este, iar ceea ce cred că nu este important, de fapt este."[6]

Din acest motiv, analiştii profesionişti privesc procesul de analiză puţin diferit faţă de cei abia iniţiaţi. La demararea rezolvării unei sarcini, novicii tind să acţioneze imediat în direcţia rezolvării cerinţei formulate de beneficiar, în timp ce profesioniştii petrec timp mai îndelungat gândindu-se la solicitare, utilizând experienţa din cazurile anterioare în crearea unor modele mentale cu ajutorul cărora rezolvă problema. De asemenea, se pricep mai bine să descopere oportunităţi acolo unde lipseşte informaţia necesară soluţionării sarcinii[7], deoarece acordă mai mult timp fazei de definire a conceptului. În cazurile complexe, cum sunt cele descrise în acest capitol, definiţia problemei ar trebui să reprezinte cam jumătate din munca analistului.

Definirea conceptului reprezintă primul pas în procesul cunoscut sub denumirea de argumentaţie organizată. De remarcat că argumentaţia organizată începe întotdeauna prin divizarea problemei, în aşa fel încât fiecare parte să poată fi examinată sistematic.

Un mod de evitare a eşecului de intelligence – evaluarea demersului analitic prin programe de cercetare ştiinţifică

Din păcate, evenimentele de la 11 septembrie 2001, au demonstrat cel puţin în cazul comunităţii de informaţii a SUA, că acest tip de analiză nu funcţiona conform cerinţelor beneficiarilor. În sprijinul acestor afirmaţii vine şi interesantul studiu al cercetătorului Rob Johnston. În august 2001, acesta a acceptat ca director al Centrului de Intelligence, un parteneriat în cercetare postdoctorală cu Centrul pentru Studii de Intelligence (CSI) al CIA. Scopul parteneriatului, care era menit să înceapă în septembrie 2001 şi să dureze doi ani, a fost acela de a identifica şi a descrie condiţiile şi variabilele care afectează negativ analiza de intelligence. Pe durata acelei perioade trebuiau investigate cultura analitică, metodologia, eroarea şi eşecul în cadrul comunităţii de informaţii, folosind metodologia de antropologie aplicată, care ar include interviuri, observaţii directe şi cu participare, precum şi grupuri de interes.

Johnston nu a găsit nicio metodă analitică standard care să stea la baza analizei de intelligence. În loc de aceasta, practica cea mai comună era

[6] Stew Magnuson, „Satellite Data Distribution Lagged, Improved in Afghanistan", în *Space News*, 2 septembrie, 2002, p. 6.
[7] Rob Johnston, op. cit., p. 64.

aceea de a face un *brainstorming* limitat pe baza analizei anterioare, producând astfel o înclinație către confruntarea părerilor anterioare. Validarea datelor nu putea fi de încredere – de exemplu, „curățarea" rapoartelor ofițerilor de informații nu permitea testarea validității lor, întărind tendința de a căuta date care confirmă ipoteze convingătoare. Procesul punea accentul pe conceptul de antirisc, cu un considerabil conservatorism managerial, şi pe evitarea erorilor, decât pe evitarea surprizelor. Procesul analitic era pus în mişcare de intelligence, în special de produsul analitic al CIA-ului, informarea zilnică a preşedintelui, care în mod caricatural era şi este denumită „CNN plus secrete". Comunitatea de intelligence era interesată mai mult de raportul în sine decât de a face analize în adâncime.

Niciuna dintre agențiile analitice nu cunoştea prea multe despre tehnicile analitice ale celorlalte. Per total, se punea accentul mult mai mult pe abilitățile de scriere şi comunicare decât pe metode analitice.

Remediile identificate de Johnston pentru îmbunătățirea calității produselor analitice şi evitarea eşecului/erorilor de intelligence sunt legate de:

- nevoia unui studiu serios al metodelor analitice în contextul existenței a trei tipuri de intelligence: investigativ sau operațional, strategic şi tactic;
- necesitatea analiştilor de a avea mai multe oportunități pentru a efectua munca de teren în străinătate, ceea ce le-ar conferi o idee despre modul în care acționează aceste agenții;
- crearea de legături formale şi informale cu elita nonprofit – comunitatea academică – şi cu mediul economic privat – comunitatea industrială;
- creşterea în folosirea analizelor alternative a surselor deschise;
- necesitatea de a găsi şi utiliza un număr cât mai variat de resurse exterioare şi interioare în sectorul analitic, care reprezintă factorul indispensabil pentru a îmbunătăți performanțele acestei infrastructuri;
- necesitatea ca sectoarele analitice din cadrul agențiilor de informații să formeze „comunități de practică", cu pregătire, grupuri de practică analitică şi diferite tipuri de surse on-line, incluzând forumuri pentru metode şi rezolvări de probleme. Aceste comunități ar fi conectate către arhiva centrală pentru lecții învățate bazate pe *After Action Review* şi ar include mai multe revizuiri formale ale produselor de intelligence strategic. Din

aceste revizuiri ar trebui să derive lecții pentru indivizi şi pentru echipe şi ar trebui să reiasă cauzele erorilor şi eşecurilor. Istoriile scrise şi orale ar servi drept alte surse pentru lecții. Aceste comunități ar putea, de asemenea, să înceapă să reformeze organizațiile, prin restructurarea designurilor organizaționale, prin dezvoltarea mai multor programe formale de socializare, prin testarea configurației de grup pentru eficiență şi pentru practicile manageriale şi de leadership.

Necesitatea unui mecanism care să exploateze ceea ce numim memoria instituțională este o prioritate pentru ceea ce unii analişti denumesc „intelligence XXI". Rezultatele programului de cercetare ştiințifică demarat de CIA în 2001 demonstrează lipsa acestui mecanism central de informații ca principal depozitar a ceea ce numim *„lessons learned"*. Un număr de firme din mediul privat şi organizații guvernamentale, incluzând Departamentele Apărării şi Energiei şi NASA, deja dețin asemenea centre pentru *„lessons learned"*, precum şi centre de informații pentru angajații săi.

Aceste centre acționează ca şi depozite de informații pentru operațiuni şi intervenții realizate cu sau fără succes. Scopul acestora este să micşoreze cantitatea de surplus de informații şi nivelurile de eroare şi eşec prin urmărirea, analizarea şi prezentarea unui raport ulterior acțiunii, precum şi informațiile analitice rezultate. Cealaltă funcție primară a acestor repozitorii este să stabilească legături pentru comunitățile de practică în şi între organizații.

Comunitățile de practică interconectate permit profesioniştilor să interacționeze, să schimbe informații metodologice, să posteze şi să răspundă studiilor individuale de caz şi să formuleze ad hoc echipe de experți în rezolvarea cerințelor cu probleme specifice. Cu instrumente simple de cercetare, cu un program elementar pentru baze de date şi o simplă interfață de vizualizare a rețelei, orice analist din comunitatea de intelligence ar fi capabil să identifice orice alt expert al cărui domeniu de specialitate necesită un răspuns la o problemă specifică sau rezolvarea unei probleme specifice. Alt avantaj al acestui model este dezvoltarea unui sfătuitor (*„mentoring"*) formal şi informal în cadrul rețelei. Orice începător ar putea să găsească un expert în cadrul comunității de intelligence, să stabilească o relație care ar fi benefică pentru amândoi. Cu stimulente potrivite, experții ar fi încurajați să contribuie la rețea şi să-şi pună la dispoziție timpul şi cercetările pentru realizarea pregătirii.

Evaluarea prin programe de cercetare ştiinţifică a factorilor care pot conduce la eşecuri de intelligence se realizează şi la nivelul comunităţii de informaţii din România. Un asemenea demers a fost iniţiat în anul 2010, la nivelul SRI, în calitate de autoritate naţională în materie antiteroristă. Potrivit cadrului legal în vigoare, acestuia îi revin responsabilităţi în domeniile prevenirii, protecţiei şi ripostei antiteroriste, fiind implicat prin componentele sale specializate în concretizarea tuturor măsurilor-cheie identificate în Strategia UE de combatere a terorismului. Proiectul de cercetare demarat la nivelul mediului academic din SRI, mai exact în cadrul Academiei Naţionale de Informaţii *„Mihai Viteazul”*, investighează modul în care „erorile de cunoaştere”, ce decurg din particularităţile confesionale sau culturale ale unui anumit grup/organizaţie/comunitate, pot genera eşecuri de intelligence, care la rândul lor pot crea vulnerabilităţi majore în actul de decizie politică. Demersul ştiinţific menţionat demonstrează că una dintre erorile care afectează cel mai frecvent demersurile analitice este aşa-numita „imagine în oglindă”, generată de incapacitatea analistului de a percepe culturi şi ideologii străine fără a le suprapune propriile standarde de valoare şi tipare mentale. În atare situaţii, este puţin probabil ca analistul să anticipeze corect comportamente şi reacţii în contexte predeterminate, dată fiind capacitatea sa redusă de empatie cu indivizi/entităţi de care îl separă bariere culturale şi/sau de mentalitate.

În acest context, considerăm că este necesară o cercetare sociologică în special la nivelul sectorului analitic din SRI, care să investigheze nivelul de cunoştinţe, de informare a specialiştilor pe o asemenea problematică, precum şi modul în care nivelul de cunoaştere (concepte, terminologie specifică, noţiuni lingvistice/confesionale/identitare) determină calitatea produselor informaţionale furnizate, precum şi posibilitatea aprecierii incorecte a unei situaţii operative, plecând de la erori de cunoaştere.

Eşecul de intelligence şi necesitatea unui *After Action Review (AAR, Examinare după acţiune)* în sectorul analitic

Dacă avem ca punct de pornire definiţia dată de fostul director CIA, William Colby, intelligence-ului, văzut ca un proces menit să faciliteze asumarea *„deciziei pentru a determina un viitor mai bun şi pentru a evita pericolele”*[8], menit să rezolve probleme şi situaţii noi, să ofere soluţii

[8] Colby, William, „Deception and Surprise: Problems of analysis analysts”, *Intelligence and National Security*, 1981, p. 84.

acționale[9], eşecul de intelligence, conform lui Mark Lowenthal, *„este inabilitatea unei părți sau mai multor părți din procesul de intelligence (colectarea, evaluarea, analiza, producția, diseminarea) de a produce la timp, un produs de intelligence exact despre o problemă sau un eveniment important de interes național”.*[10]

Pentru Abram N. Shulsky, un eşec de intelligence este în mod esențial *„o interpretare greşită a unei situații pe baza căreia factorii guvernamentali iau decizii nepotrivite sau contraproductive propriilor interese (care coincid de fapt cu interesele naționale)”.*[11]

Un eşec de intelligence este în mod fundamental o greşeală de interpretare a unei situații pe baza căreia liderii politici sau forțele de securitate iau măsuri care sunt contraproductive propriilor interese. Dacă factorii guvernamentali sau forțele de securitate sunt surprinşi/se de ceea ce se întâmplă, este de mai mică importanță decât faptul ca ei să continue să ia decizii greşite pentru a rezolva o situație pe baza unei prime erori de analiză. O cauză comună a eşecului de intelligence este simplul fapt că informația nu este la îndemână sau este lipsită de acuratețe.[12] Cu excepția cazurilor în care nu pot fi obținute niciun fel de informații relevante, eşecurile din activitatea de informații sunt legate de o dereglare a procesului analitic, ce determină ignorarea sau interpretarea greşită a datelor. Prin urmare, ele sunt similare erorilor specifice oricărui demers intelectual sau de înaltă calificare.

O altă cauză a erorilor survenite în procesul de analiză a informațiilor este însă aplicarea unui raționament greşit, lucru care se întâmplă într-o mare diversitate de situații, nefiind legat de cadrul instituțional în care se desfăşoară analiza. Fenomenul este numit „proiectarea unei imagini simetrice”, care presupune că situațiile nefamiliare sunt interpretate pe baza celor familiare. În activitatea serviciilor de

[9] Niță, Cristian, „O încercare de definire a termenului de intelligence”, în *Revista Română de Studii de Intelligence*, nr. 1-2, decembrie 2009, Bucureşti, p. 61.

[10] Lowenthal, Mark, „The Burdensome Concept of Failure”, în Maurer, Alfred C., Tunstall, Marion D. and Keagle, James M. (eds.), Intelligence: Policy and Process. Boulder, Westview Press, 1985, p. 51.

[11] Abram N. Shulsky, Gary J. Schmitt, *Războiul tăcut. Introducere în universul informațiilor secrete*, capitolul 3, „Ce înseamnă toate acestea? Analiza şi producerea informațiilor”, Iaşi, Editura Polirom, 2008, p. 110.

[12] Vezi studiul semnat de Brig. Gen George P. H. Kruys (rtd.), „Intelligence failures: causes and contemporary case studies”, în *Strategic Review for Southern Africa*, vol. 28, no. 1, Institute for Strategic Studies, University of Pretoria , pp. 71-72.

informații, aceasta înseamnă că acțiunile altui stat sunt evaluate sau anticipate prin analogie cu acțiunile pe care consideră analistul că le-ar lua el (sau țara sa) dacă s-ar afla într-o situație similară.[13]

Eşecul este un eveniment uşor de reamintit; afectează ego-ul şi conduce la investigarea erorilor şi adaptarea sau schimbarea comportamentului bazat pe aceste investigații.

Presupozițiile şi prejudecățile rămân surse majore ale eşecurilor analitice, ele afectând atât analiştii cât şi produsele analitice pe care aceştia le produc. Aceasta deoarece este foarte dificil să conştientizăm propriile prejudecăți şi presupoziții pe parcursul analizei informațiilor.

Eşecul de intelligence poate fi analizat şi evitat prin raportare la alte domenii de vârf, în speță chirurgia şi astronautica. De altfel, aşa cum argumenta şi Ronald Garst, domeniul intelligence-ului nu este singurul domeniu în care constrângerile temporale pot forța luarea deciziilor înainte de strângerea integrală a informațiilor. Timpul este mereu o variabilă-cheie, indiferent dacă individul se află într-o sală de operații ori într-o arenă. Să fiu sincer domeniul intelligence-ului este o profesie pe viață şi pe moarte, dar tot aşa sunt medicina şi deportarea maselor. În ambele situații, eşecul înseamnă pierderi.

Fiecare din aceste două subdomenii specializate poate servi drept backround pentru studiile analizatorilor de intelligence. Chirurgii şi astronauții au standarde de performanță foarte ridicate şi rata erorilor destul de scăzută. Ambele situații subliniază ideea adoptării unor metode de căutare variate care să conlucreze cu controverse complicate şi sugerează că există lecții ce aparțin altor domenii şi care trebuie învățate. Probabil cea mai cunoscută legătură dintre activitatea de intelligence şi cele două domenii de vârf este aceea că, deoarece sunt vieți în joc, chirurgii şi astronauții experimentează presiuni externe şi interne uriaşe, ei trebuind să evite eşecul. Acelaşi lucru se aplică şi pentru analiştii de intelligence. În adaos, chirurgia şi astronautica sunt selective şi, mai ales, sunt discipline selective şi secrete. Deşi munca lor nu este secretă, ambele grupuri tind să fie protejate de lumea exterioară: chirurgii din motive de selecție profesională, instruire şi realitate financiară, responsabilității cu privire la malpraxis; astronauții pentru că sunt un grup foarte mic, iar procesul de

[13] Abram N. Shulsky, Gary J. Schmitt, op.cit., p. 115.

selecţie şi instruire este foarte costisitor. Analiştii de intelligence împărtăşesc multe dintre aceste circumstanţe organizaţionale şi profesionale.

O posibilă soluţie pentru abordarea acestei situaţii este instituţionalizarea, la nivelul comunităţii de informaţii, a unor mecanisme similare cu cele din domeniile menţionate, care să asigure simularea unor situaţii, exerciţii scurte, informale în cadrul cărora analiştii să se concentreze pe modul în care aceştia ar putea greşi, pe ceea ce Gary Klein numeşte „modelul premortem”[14]. În acest exerciţiu de grup, indivizii îşi închipuie eşecuri legate de aria lor de responsabilitate – în cazul analizei informaţiei, un eşec de avertizare – şi dezbat asupra modului în care acestea ar apărea, precum şi rezolvările posibile. Accentuarea părţilor negative ajută la alungarea mulţumirii de sine ce apare din fireasca prea-mare-încredere în judecăţi. Un astfel de exerciţiu ar fi un echivalent funcţional al exerciţiului „probabilitate mică/impact mare” din analiza alternativă tradiţională, având totuşi diferenţa că natura sa informală îi permite o mai deasă folosire.

Participanţii la dezbateri au discutat de asemenea schimbarea culturii din cadrul organizaţiilor de informaţii înspre una care să fie axată mai mult pe îndoiala de sine. Evaluările performanţei analitice sunt deseori făcute de persoane din exterior, iar greşelile descoperite sunt exploatate de către media şi criticii externi, rezultând astfel o poziţionare defensivă a profesioniştilor din cadrul birourilor de informaţii. A existat numai o atenţie internă modestă asupra studiului eşecurilor – şi una şi mai mică asupra succeselor – în încercarea de a identifica nişte elemente necesare îmbunătăţirii personale.[15]

Un alt exemplu este oferit de către Centrul Armatei de Lecţii Învăţate (CALL) din cadrul armatei americane, care studiază încontinuu problemele operaţionale pentru a găsi elemente de îmbunătăţire a performanţelor. Un efort dedicat de a investiga continuu şansele de a eşua şi de a reuşi prin intermediul periodicelor recapitulări „de după analiză” – realizate în baza recapitulărilor armatei numite „de după luptă” – ar putea

[14] Vezi, în acest sens, Gary Klein, *Intuition at Work: Why Developing Your Gut Instinct Will Make You Better at What You Do*, Doubleday, New York, 2002, pp. 90 şi 203.

[15] Vezi, în acest sens, o versiune scurtă a unui raport intitulat *Găsirea Logicii Ameninţărilor Transnaţionale*, lucrările Ocazionale ale Centrului Kent, vol. 3, nr. 1, disponibil pe pagina de internet a CIA-ului, www.cia.gov. Rezumate pentru fiecare din cele patru sesiuni de dezbateri ale proiectului pot fi găsite în raportul corporaţiei RAND (CF-200) Îmbunătăţirea Avertizării pentru Ameninţările Transnaţionale: Rapoartele Dezbaterilor.

ajuta la crearea unui mediu mai introspectiv[16]. Oferind analiştilor timpul necesar pentru astfel de exerciţii, ar demonstra într-un mod evident angajamentul organizaţional faţă de învăţare.

De altfel, eşecul este un lucru din care se poate învăţa şi rezultă într-un moment favorabil învăţării. Sunt puţine motive pentru a realiza un *After Action Review* atunci când evenimentele se desfăşoară după preziceri. Prezumţia este că mecanismele de analiză au fost valabile, pentru că rezultatele analizelor au fost corecte. Pericolul evident este că această ipoteză exclude posibilitatea ca una să fie corectă din pură întâmplare. Mai mult, concentrându-se numai pe eşecul de intelligence, se riscă prelevarea de probe părtinitoare, prin alegeerea doar a cazurilor în care există erori. Riscul de a ignora succesul este determinat de faptul că potenţialele lecţii pot rămâne nedescoperite. O alternativă la a conta pe eşec în provocarea presupunerilor cuiva o reprezintă crearea unui standard de practică pentru revizuirea fiecărui caz, indiferent de rezultate, în principal prin utilizarea unui *After Action Review* oficial.

After Action Review (AAR, Examinare după acţiune) este utilizat de către armata SUA pentru a surprinde lecţiile învăţate după un exerciţiu de antrenament sau o operaţie reală. Spre deosebire de convenţionalul postmortem şi tradiţionala critică a performanţei, *AAR*-ul este utilizat pentru a evalua succesele, dar şi eşecurile. Deşi în general eşecul primeşte mai multă critică şi atenţie decât succesul, o abordare care examinează doar eşecurile rezultă într-o eroare. Dacă se pune accentul doar pe greşeli, metode de altfel eficace pot fi considerate sursa erorilor. Faptul că aceste metode au avut succes în 99 din 100 de cazuri poate trece neobservat, având ca rezultat faptul că eşecurile primesc o atenţie exagerată şi influenţează rezultatul statistic al postmortemului. *AAR*-ul a fost creat special pentru a evita această problemă.

Procesul *AAR* a fost introdus la mijlocul anilor ’70, dar este bazat pe metoda „istoriei orale a interviurilor de după luptă” folosită de SLA Marshall în al Doilea Război Mondial, în războiul din Coreea şi în războiul din Vietnam. Cât de repede posibil după o bătălie, indiferent de rezultat, Marshall aduna soldaţii care fuseseră implicaţi şi, utilizând o tehnică de

[16] Pentru o discuţie despre procesul de după acţiune al armatei, vezi Nancy M. Dixon, *Common Knowledge: How Companies Thrive By Sharing What They Know*, Harvard Business School Press, Boston, 2000, pp. 37-38.

interviu semistructurală, îi antrena pe aceştia într-o discuţie de grup despre rolul individual şi colectiv şi despre acţiunile din timpul luptei.

Actuala metodă *AAR* include, de asemenea, date obiective precum tactici, logistică, rata de ucidere, timpul pentru sarcină, precizia sarcinii şi rezultatele operaţionale. Informat de date obiective, grupul de discuţii se desfăşoară sub conducerea unui facilitator instruit în procesul de strângere de informaţii. *AAR*-ul, alături de documentele suplimentare, cum ar fi studii istorice şi materiale doctrinare relevante, este depozitat apoi într-o arhivă de cunoştinţe la Centrul pentru Lecţii Învăţate al Armatei SUA (US Army's Center for Army Lessons Learned – CALL)[17].

Eşecul de intelligence ca generator al inovării în sectorul analitic al comunităţii de informaţii americane

Comunitatea de intelligence este relativ mică, foarte selectivă şi foarte bine acoperită de ochii publicului. Pentru toţi practicanţii, munca de intelligence este costisitoare din punct de vedere intelectual şi o meserie cu un ridicat grad de risc care poate ghida politica publică, poate proteja naţiunea sau o poate expune într-un grad de risc mai ridicat. Deoarece consecinţele unui eşec sunt atât de grave, profesioniştii de intelligence sunt expuşi unei continue presiuni, atât în interior, cât şi în exterior, tocmai pentru a evita astfel de consecinţe. Provocarea pentru analişti este, în aceste condiţii, aceea de a transforma tensiunile existente în avantaje profesionale prin păstrarea unor standarde analitice riguroase, mărind în acelaşi timp gradul de utilitate al evaluărilor lor pentru beneficiarii politici.

În ultimele trei decenii, eşecul de intelligence a fost un subiect de interes pentru mediul academic şi, mai ales, pentru analiştii de intelligence, iar acum pentru aproape toate studiile contemporane americane în acest domeniu.[18] Studiile au avut ca punct de plecare cazul atacului japonez de la

[17] Vezi site-ul Centrului pentru Lecţii Învăţate al Armatei SUA, care are link-uri către numeroase alte arhive. Deşi fiecare organizaţie a personalizat conceptul pentru a satisface propriile nevoi, în prezent toate serviciile militare ale SUA, Administraţia Naţională de Aeronautică şi Spaţiu, Departamentul de Energie, Agenţia de Protecţie a Mediului, Organizaţia Tratatului Atlanticului de Nord, Naţiunile Unite şi Ministerele Apărării din Australia şi Canada au arhive de „lecţii învăţate".

[18] Gustavo Díaz, „Methodological approaches to the concept of intelligence failure", *UNISCI Discussion Papers*, January 2005, p. 1

Pearl Harbour, caz examinat de Roberta Wohlsletter[19]. În anii '80, multe lucrări au avut în centrul atenției subiectul surprizei strategice. În acest sens, Richard Betts şi Michael Handel au dezvoltat teoria eşecului de intelligence prin studierea războiului de Yom Kippur, din 1973.[20]

Dacă se consultă vasta literatură de specialitate scrisă pe tema eşecurilor de intelligence, se poate ajunge la concluzia că ele au fost atribuite unor cauze fie subiective, adică psihologice, fie obiective, care țin de organizare.

Tipologia eşecurilor serviciilor de informații în literatura actuală[21]

	Nivel suficient de informații în sistem		Insuficient
	Interpretare greşită	Informația nu a ajuns la destinația corectă	——
Cauza eşecului	Psihologică	Procedurală	Organizațională
Remediu	Pluralism şi conştientizare psihologică	Schimbare organizațională	Centralizare

Eşecul cel mai grav şi care se poate solda cu cele mai mari prejudicii în activitatea de informații se înregistrează atunci când are loc un atac neanticipat şi forțele militare ale țării sau desfăşurate în teatrul de operații sunt luate prin surprindere. De altfel, configurația postbelică a comunității de informații americane s-a datorat tocmai unui astfel de eşec, cel de la Pearl Harbour din 7 decembrie 1941[22].

[19] Ibidem. Menționează în acest sens studiul lui Wohlsletter, Roberta, *Pearl Harbour Warning and Decision*, Stanford, Stanford University Press, 1962.

[20] Ibidem. Menționează în acest sens studiul lui Kahn, David, "The Intelligence Failure at Pearl Harbour", *Foreign Affairs*, Vol. 70, No. 5 (Winter 1991/1992), precum şi pe cel al lui Handel, Michael, "The Yom Kippur War and the Inevitability of Surprise", *International Studies Quarterly* (September 1977).

[21] Steve Tsang, *Serviciile de informații şi drepturile omului în era terorismului global*, Bucureşti, Editura Univers Enciclopedic, 2008, p. 270.

[22] Vezi Steve Tsang, op.cit., capitolul 11, Isaac Ben, *Israel, O nouă abordare în domeniul evaluării informațiilor*, pp. 265-287. Roberta Wohlstetter, în volumul *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962), atribuie eşecul faptului că serviciile americane de informații au fost induse în eroare de „zgomote" (adică, rapoarte neimportante) care acopereau adevăratele „semnale". Este clar că, şi în acest caz, a existat o problemă de selecție şi interpretare, ci nu o lipsă de informații.

Surprize majore de-a lungul timpului, adică eşecuri în a previziona din timp[23], includ, pe lângă exemplul amintit: atacarea URSS de către Germania, 22 iunie 1941[24]; debarcarea Aliaților în Normandia, 6 iunie 1944; atacul Aliaților asupra podului de la Arnhem – *„podul prea îndepărtat"*, septembrie 1944; atacul german din Ardeni, decembrie 1944; intrarea Chinei în războiul coreean, decembrie 1950; războiul de graniță sino-indian din 1962; criza rachetelor din Cuba (1962); ofensiva nord-vietnameză şi a Vietcongului (ofensiva Tet) asupra Vietnamului de Sud la sfârşitul lunii ianuarie 1968; invazia sovietică a Cehoslovaciei (1968); atacul egipteano-sirian asupra Israelului din 1973 (războiul de Yom Kippur); revoluția din Iran (1979)[25]; atacurile asupra Ambasadei americane din Beirut (aprilie 1983), asupra sediului infanteriştilor marini americani (octombrie 1983) şi asupra unei anexe a Ambasadei americane din Beirutul de Est (septembrie 1984)[26]; invazia irakiană din Kuweit (august 1990); testele nucleare indo-pakistaneze din 1998[27]; atacurile de la 11 septembrie 2001[28].

---

[23] Subiectul eşecului strategic este tratat de Richard K. Betts, *Surprise Attack: Lessons for Defense Planning*, The Brookings Institution Washington DC, 1982 şi Abraham Ben-Zvi, „Hindsight and Foresight: A Conceptual Framework for the Analysis of Surprise Attacks", *World Politics*, vol. 28, no. 3, april 1976.

[24] Vezi, în acest sens, Barton, Whaley, *Code Word Barbarrosa*, The MIT Press, Cambridge MA, 1973, p. 171. Barton Whaley, care a examinat cazul invaziei naziste asupra Uniunii Sovietice, argumentează că „factorul critic în atacul surpriză a constat într-o campanie coordonată de deception, de inducere în eroare, căreia i-au căzut victime analiştii".

[25] Subiectul revoluției din Iran, ca eşec de intelligence, este tratat de Kristine Tockman, coordonator-proiect şi Doug MacEachin, Janne E. Nolan, co-preşedinți, „Iran: Intelligence Failure or Policy Stalemate?", *Working Group Report*, nr. 1, Georgetown University, november 23, 2004, www.georgetown.edu.

[26] Subiectul atentatelor din Liban asupra obiectivelor americane este prezentat de Glenn P. Hastedt, „Intelligence Failure and Terrorism: The Attack on the Marines in Beirut", *Conflict Quarterly VIII*, nr. 2, spring 1988, David Kennedy and Leslie Brunetta, „Lebanon and the Intelligence Community: A Case Study", *Studies in Intelligence 37*, no. 5, 1994 şi Robert Baer, *See No Evil: The True Story of a Ground Soldier in the CIA's War on Terrorism*, Crown Publishers, New York, 2002.

[27] Surpriza strategică produsă de realizarea testelor nucleare indo-pakistaneze din 1998 este tratată de Brian Duffy, Robert Greenberger, „Fallout Is Heavy as CIA Fails to Predict India Test", *The Wall Street Journal*, 12 May 1998.

[28] Vezi, în acest sens, Goodman, Melvin, „9/11. The failure of strategic Intelligence", *Intelligence and National Security*, Vol. 8, No. 4 (Winter 2003), pp. 59-71.

De exemplu, surpriza provocată de atacul egipteano-sirian din 1973 (războiul de Yom Kipur[29]) este considerată greşeala cea mai costisitoare şi mai importantă comisă de comunitatea de informaţii a Israelului de la înfiinţarea ei şi până astăzi. Ea a constat în evaluarea greşită a intenţiilor egiptene şi siriene, din preajma declanşării războiului de Yom Kippur, când cele două armate au atacat pe neaşteptate Israelul în încercarea de a recâştiga teritoriile pierdute în urma războiului din anul 1967. La momentul respectiv, Israelul beneficia de toate avantajele: acoperire informativă superioară, resurse umane excelente care beneficiau de un bun acces la informaţii, existenţa unui dialog discret la nivel înalt cu mai mulţi lideri arabi şi musulmani şi a unei direcţii de evaluare a informaţiilor care transmisese un avertisment cu mai multe luni înainte de război, prevenind, astfel, izbucnirea sa în acel moment. Însă, în pofida tuturor celor menţionate mai sus, Israelul a înţeles totul greşit. Abundenţa informaţiilor a condus la *„încrederea"* în informaţii: intelligence-ul israelian avea încredere, mai degrabă, în capacitatea analitică superioară decât în semnalele ameninţătoare de pe teren. În faţa probelor privind un potenţial atac, serviciile de informaţii israeliene şi-au menţinut concepţia sau ideea că Egiptul nu va ataca până când nu va fi capabil să organizeze atacuri aeriene ample pentru a distruge forţele aeriene israeliene, iar Siria nu va ataca fără Egipt. Prima şi cea mai importantă parte a acestei concepţii reflectă, la nivel militar, aceeaşi imagine în oglindă existentă la nivel politic – convingerea că Egiptul nu va declanşa un război pe care nu are şanse reale să îl câştige. Faptul ca liderii serviciilor de informaţii israeliene aveau o concepţie *a priori* în legătură cu precondiţiile necesare pentru izbucnirea ostilităţilor este privit ca o dovadă clară că evaluarea lor a fost incorectă. Se spune că un bun analist de informaţii nu trebuie să fie încorsetat într-un singur tipar conceptual. Alţii susţin că o estimare informativă nu este posibilă fără a apela la un anumit fel de cadru conceptual.

[29] Surpriza provocată de atacul egipteano-sirian din 1973 – războiul de Yom Kipur – este tratată de Handel, Michael, „The Yom Kippur War and the Inevitability of Surprise", *International Studies Quarterly* (September 1977).

Elucidarea eşecurilor de intelligence: 8 analize de caz[30]

	Culegere				Analiză				
Cazuri	Informaţie-cheie lipsă	Informaţie nedistribuită	Cerinţe insuficiente	Negare şi *deception*	Imaginaţie insuficientă	Zgomot de fond	Ipoteze greşite	Informaţie greşit interpretată	Impactul negării necorectat
Pearl Harbour		•	•	••	•	•	•		•
Criza rachetelor Cuba	•			••	•		•		•
Yom Kippur		•		••	•		•	•	•
Revoluţia iraniană	•			•	•		•		•
Arme biologice sovietice	•		•	••	•				•
India NW	•			•	•		•		•
9/11	•	•	•	•	•	•	•		•
Irak WMD	•			••	•		•	•	•

[30] James B. Bruce, „The missing link: the analyst-collector relationship", în Roger Z. Goerge, James B. Bruce (ed.), *Analyzing intelligence. Origins, obstacles and innovations*, Georgetown University Press, Washington, DC, 2008, p. 204. Denial and deception: • Doar negarea este prezentă: minciuna semnificativă nu este evidentă; • • Atât negarea cât şi minciuna sunt prezente.

Dacă dezastrele care pot rezulta în urma confruntării cu surprizele strategice pe plan militar sunt evidente, prejudiciile provocate de neanticiparea unor evenimente politice sau economice sunt mai greu de evaluat. În mare măsură acestea depind de modul în care guvernul este pregătit să ia măsuri, dacă ar fi fost avertizat şi de existenţa unor strategii ce puteau să evite producerea evenimentului sau să diminueze impactul său negativ. În acest sens menţionăm criza petrolului din 1973, prăbuşirea rapidă a lagărului socialist şi a URSS în intervalul 1989-1991, criza economică din 2008-2010.

Din eşecurile unor asemenea acţiuni au rezultat cele mai multe şi reale critici şi tot de aici pot fi învăţate şi cele mai multe lecţii.[31] De exemplu, eşecul în generarea unor avertismente legate de invazia Kuweitului de către Irak în 1990 a generat recomandări privind schimbarea modului de analiză din partea unui reputat specialist în analiza de intelligence ca Doug MacEachin[32]. Judecata de bază referitoare la Irak a fost că nu va iniţia o acţiune militară pe termen scurt, prezumţie bazată pe aserţiunea că ţara va avea nevoie de câţiva ani pentru a-şi reveni economic şi militar după războiul cu Iran. O asemenea viziune era una atât de evidentă în acel moment încât o viziune critică asupra ei era de neconceput. Structurile informative decizionale au acuzat viziunile analiştilor asupra incertitudinii ca fiind o tombolă a previzunilor menită să impună viziunea unora asupra altora. De asemenea, Doug MacEachin recomanda pentru o analiză mai riguroasă o atenţie sporită în selectarea factorilor ce sunt cei mai probabili să determine o anumită stare de fapt viitoare, în lipsa unor informaţii clare pe care se poate baza o prezicere concretă.

Alte două studii asupra practicii informative preventive au fost determinate de un eşec în previzonarea acţiunilor guvernului indian ales care a finalizat programul nuclear: raportul Jeremiah (*Intelligence Community's*

[31] Jack Davis, „Improving CIA Analytic Performance: Strategic Warning, The Sherman Kent Center for Intelligence Analysis", *Occasional Papers*, Volume 1, Number 1, Sept. '02, p. 2.

[32] Menţiune în Richards J. Heurr, *Psychology of Intelligence Analysis*, Center for Strategic Study Intelligence, CIA, 1999, pp. XVII-XVIII. Douglas MacEachin a fost director adjunct al CIA. În 1997, după 32 de ani de activitate în cadrul Agenţiei, s-a retras şi a devenit Senior Fellow la John F. Kennedy School of Government, din cadrul Universităţii Harvard. Doug MacEachin îşi rezuma caracterul esenţial a ceea ce el a intitulat previzune (modul de acţiune Linchpin), diferit de „prezicerea viitorului"(judecăţi pe baza unor ipoteze de bază) într-un eseu intitulat „Tradecraft of Analysis", publicat în *US Intelligence at the Crossroads: Agendas for Reform* (1995, Roy Godson).

Performance on the Indian Nuclear Tests, June 1998) şi raportul Biroului Inspectorului General (*Alternative Analysis in the Directorate of Intelligence*, May 1999), reiterând critici asupra lipsei unei analize a alternativelor.

Raportul Jeremiah a recunoscut restrângerile asupra avertismentelor strategice datorate lipsei de resurse analitice urmare a micşorării importanţei departamentului informativ după sfârşitul Războiului Rece. Şi al doilea raport punea accentul pe anumite presiuni exercitate pe analiştii Agenţiei pentru viteză, concizie, ca şi obstacole în calea unei metode de lucru mai eficiente pentru combaterea incertitudinii. Ambele critici au reiterat nevoia folosirii analizei alternativelor, ca şi modalitate pentru o testare mai bună a factorilor de bază, precum şi pentru acoperirea acelor variante mai puţin probabile, dar cu un eventual impact foarte important.

Amiralul Jeremiah a subliniat nevoia instituţionalizării analizei alternativelor în cazul problemelor complexe când o schimbare politică creşte posibilitatea depărtării de pe firul analitic anterior descris. Una dintre capcanele cognitive ce trebuie depăşite o reprezintă „imaginile în oglindă" – estimarea rezultatului calculului risc-beneficiu pe baza unor argumente ce ar avea sens într-un context american sau vest-european.

Pe lângă o mai bună gândire critică a analiştilor, Jeremiah a sugerat şi alte două soluţii pentru o viziune mai riguroasă asupra schimbărilor majore de factori, astfel:

- Introducerea de experţi din exterior într-un mod sistematic, pentru evitarea gândirii de genul „toată lumea gândeşte ca noi".
- Aducerea de experţi în analiză, în momentul în care se face o trecere pe o altă temă majoră.

Cel de-al doilea raport recunoştea activitatea directoratului agenţiei pentru promovarea gândirii critice şi făcea mai multe recomandări pentru un mai bun management al folosirii analizei alternativelor:

- stabilirea unor linii de bază pentru folosirea potrivită a analizei alternativelor şi o mai bună încorporare a viziunilor minoritare şi a incertitudinilor derivate din analiza în rezultate;
- stabilirea unui mecanism pentru identificarea celei mai bune practici în analiza atât înăuntrul, cât şi în afara directoratului;
- crearea unui plan comprehensiv de îmbunătăţire a analizei alternativelor;
- revizuirea şi îmbunătăţirea metodologiei de lucru a directoratului;
- implementarea unui curriculum care oferă o expunere foarte bună a instrumentelor analizei şi tehnicilor de prezentare.

Răspunsul oficial al structurilor informative s-a concretizat printr-o atenție sporită asupra tehnicilor şi metodelor aflate sub spectrul analizei alternativelor. Au fost aduşi experți din exterior, analiştii şi-au intensificat folosirea de tehnici, cum ar fi jucarea de roluri în cadrul calculelor echipei adverse, găsirea de argumente contra unui punct de vedere extrem de puternic al directoratului pentru identificarea incertitudinilor şi creşterea atenției pe amenințările cu impact major, dar probabilitate scăzută.

Istoria recentă ne oferă două exemple relevante: concluziile extrase ulterior atacului terorist din 11 septembrie 2001 şi concluziile formulate cu privire la intervenția trupelor coaliției în Irak începând din martie 2003.

Comunitatea americană de informații şi-a asumat erorile în analiza datelor care anunțau atacul terorist din 11 septembrie 2001. Raportul US Senate este categoric în acest sens: *„indiciile incerte au fost folosite ca dovezi, iar informațiile care contraziceau tabloul de ansamblu anterior au fost ignorate”*. Prin urmare, CIA a căutat acele informații care corespundeau aşteptărilor decidentului politic.[33]

Grupurile de lucru care au analizat intervenția SUA în Irak au explicat: comunitatea de analişti a dezamăgit factorii de decizie pentru că *„au controlat greşit complexitatea epistemică prin omiterea distincțiilor dintre fapt şi judecată”*. Conform Raportului elaborat de Pentagon – intitulat *„Review of Pre-Iraqi War Activities of the Office of the Under Secretary of Defence for Policy”* –, „informațiile secrete” privind regimul Saddam Hussein, care au justificat invazia din martie 2003, au fost „prefabricate” şi „false”. Acestea căutau să demonstreze, contrar rapoartelor inspectorilor ONU, că Irakul stochează, în secret, arme de distrugere în masă şi că regimul laic al lui Saddam ar fi avut legături strânse cu organizația islamistă fundamentalistă al-Qaida. Aceasta, cu toate că CIA a avertizat public, în mai multe rânduri, că nu deține niciun fel de dovezi cu privire la o eventuală legătură între dictatorul irakian şi Ossama bin Laden.

În concluziile raportului se precizează: *„reprezentanții comunității de informații au stat sub semnul unei presupoziții colective sau al dinamicii*

[33] Irena Dumitru, *Psihologia analizei informațiilor*, suport de curs, Editura Academiei Naționale de Informații *„Mihai Viteazul”*, Bucureşti, 2009, pp. 37-38.

specifice gândirii de grup care i-a determinat să interpreteze unele probe ambigue ca şi argumente pentru o ipoteză anterioară, în absența aplicării mecanismelor formale de testare a ipotezelor".

„Produsele analitice au indicat că Irakul şi-a reînnoit producția de arme chimice până la 500 de tone de agent chimic… Aceste evaluări se bazau în mare parte pe o altă presupunere, conform căreia Irakul s-ar fi implicat în activități de transport al armelor chimice, începând din anul 2002. Această ipoteză se baza pe o alta, conform căreia prezența unui anumit tip de camion-cisternă era un indicator pentru derularea unor activități corelate cu armele chimice şi biologice. Comunitatea de informații nu a precizat explicit în evaluările sale că această presupunere se baza pe o altă presupunere analitică. Ceea ce a dat beneficiarului produsului informativ impresia că programul de înarmare chimică a Irakului era în derulare şi în creştere, fără să precizeze că evaluările se bazau pe date foarte puține şi fără credibilitate"[34].

Dacă serviciile de informații din Israel şi din Occident[35] ar fi adoptat metoda combaterii şi negării[36], nu ar fi putut evita concluzia finală că irakienii nu aveau capacitatea operațională de a lansa rachete balistice cu focoase chimice, cu toate că irakienii ar fi putut deține un număr limitat de rachete sau focoase ascunse.

---

[34] Ibidem, pp. 37-38.

[35] În Raportul Carnegie se menționează şi următorul aspect: „în cazul Irakului, cele mai bune trei servicii de informații din lume – al Statelor Unite, al Marii Britanii şi al Israelului – s-au dovedit incapabile de a furniza informațiile corecte necesare întreprinderii unor acțiuni în absența unei amenințări iminente". Vezi J. Cirincione, J. Tuchman Mathews, G. Perkovich şi Alexix Orton, *WMD in Irak: Evidence and Implications*, Washington, DC: Carnegie Endowment Report for International Peace, january 2004, p. 61.

[36] Metoda a fost propusă de Isaac Ben-Israel, un ofițer cu experiență îndelungată în activitatea de informații israeliană, şi a avut ca reper eşecurile înregistrate de armata şi serviciile de informații israeliene în timpul războiului din octombrie 1973. Isaac Ben-Israel propune comunității de informații o alternativă incitantă la modul actual de abordare a analizei informațiilor. În locul inducției şi al căutării unor probe care să vină în sprijinul ipotezei luate în calcul, susține ideea căutării de probe contrară pentru verificarea şi eliminarea ipotezelor. Aceasta ar trebui să contribuie la reducerea sau chiar eliminarea tendinței inevitabile de a găsi dovezi care să demonstreze valabilitatea teoriei sau a ideilor preconcepute preferate. Chiar dacă nu elimină riscul unei erori, această abordare asigură analiştilor o bază de pornire mult mai sigură pentru formularea concluziilor şi evaluarea amenințărilor concrete.

Un aspect major al eşecului activităţii de informaţii în cazul „Irak – arme de distrugere în masă" l-a reprezentat şi creşterea dificultăţii în a convinge beneficiarul să accepte rezultatul muncii informative, acolo unde intervin chestiuni legate de programul platformei politice[37]. Comisia pentru cercetarea existenţei armelor de distrugere în masă în Irak declara că *„analiştii au şi responsabilitatea de a informa beneficiarul despre eventualele dezacorduri din interiorul comunităţii de informaţii, referitor la un anume subiect şi, de asemenea, trebuie să găsească modalităţi prin care să le explice diferitele niveluri de nesiguranţă, inerente muncii de analiză"*.[38] Provocarea constă în faptul de a reuşi să îl convingă pe beneficiar, fără ca acesta să aibă ulterior resentimente faţă de munca de informaţii.

Pentru a facilita procedura, beneficiarul trebuie integrat în procesul activităţii de informaţii – aspect destul de dificil de realizat în cazul decizionalilor cu o agendă încărcată. Dacă se reuşeşte acest lucru, comunicarea rezultatelor devine mai lejeră, iar beneficiarul va acorda o mai mare credibilitate informaţiei şi o va înţelege mai bine.

Pregătirea unui raport informativ pe subiecte tehnice are întotdeauna unele modalităţi, mai explicite, în care să fie prezentate deşi, din nefericire, nu sunt mereu aceleaşi. Concizia exprimării reprezintă o problemă specială în inginerie. Devine aproape axiomatic faptul că dacă un raport poate fi citit şi înţeles, atunci este neconform din punct de vedere tehnic. Numai un analist excepţional poate atinge acurateţea tehnică şi descifrabilitatea într-un singur document, iar metoda constă în eliminarea detaliilor tehnice abundente, cel mai important fiind înţelegerea mesajului.

Concluzii

În faţa acestor limite şi pericole ale informării, serviciile de informaţii au datoria de a găsi soluţiile de afirmare şi consolidare a independenţei analiştilor la nivelul întregii comunităţi de informaţii.

[37] Douglas H. Dearth, R. Thomas Goodden, *Strategic Intelligence: Theory and Application*, ediţia a II-a (Carlisle Barracks, PA: US Army War College, and Washington DC: Defense Intelligence Agency), 1995, p. 197.

[38] Report of the Commision on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 31 martie 2005, www.wmd.gov/wmd_report.pdf, p. 419.

Soluția evitării eşecului în activitatea de analiză a informațiilor o reprezintă cooperarea între cei care activează în munca de informații. Cu toate că nu există metode universale aplicabile tuturor problemelor, se pleacă totuşi de la un proces primar de bază. De asemenea, pot fi utilizate o varietate de tehnici standard.

Un analist trebuie să dețină un repertoriu de astfel de metode, aplicabile în depăşirea dificultăților întâlnite în procesul de culegere şi valorificare a informațiilor. Aici pot fi incluse analiza de model, predicția tendințelor, studiul literaturii de specialitate, analiza statistică şi nu numai. O asemenea abordare va diminua rata eşecului, va asigura reflectarea unor puncte de vedere diverse în produsele informaționale finite şi va reinventa procesul de producere a informațiilor secrete prin integrarea completă a surselor deschise ca bază pentru obținerea unui produs din toate sursele.

De asemenea, printr-un proces de asimilare instituțională, un proces *AAR* şi o arhivă de lecții învățate ar putea constitui un alt instrument util de lucru pentru analiştii de intelligence. Deşi pare greu şi întins pe o perioadă de timp considerabilă, cu pregătire şi experți facilitatori, procesul *AAR* ar putea fi modificat şi adaptat pentru folosul analiştilor la sfârşitul unui ciclu de producție. Ca o chestiune practică, procesul ar fi folosit mai degrabă pentru acțiuni îndelungate, cum ar fi estimările şi evaluările. Produsul de intelligence, împreună cu notițele *AAR*, ar fi încorporate într-o arhivă de cunoştințe ale comunității. Această arhivă de cunoştințe ar ajuta, de asemenea, la dezvoltarea şi rafinarea unui curs avansat de analiză prin asigurarea dezvoltării cursurilor cu o bază de date analitice. Pe scurt, arhiva devine un instrument pentru analizarea nevoilor educaționale continue şi face legătura directă între pregătire şi munca practică a analiştilor. Aceste date pot fi folosite ca un test pentru cercetare asupra eficacității metodologiilor analitice. În acest mod, lecțiile învățate nu sunt pierdute pentru viitoarele generații de analişti.

IDEI PRACTICE PENTRU EVITAREA EŞECULUI DE INTELLIGENCE

Idee	Implementare şi scop
Dezvoltarea unei tehnologii a informației pentru a stoca şi a recupera automat ipoteze, idei.	Ajută memoria şi gândirea creativă a analiştilor, promovând de asemenea colaborarea.
Angajarea metodologilor analitici cu pregătire în creativitate şi facilizare.	Pregătirea şi facilitarea exercițiilor de gândire divergente şi a dialogurilor structurate, urmărind identificarea viziunilor alternative.
Combinarea constantă a persoanelor cu înclinații diferite în echipe (de exemplu, *barbelling*)	Creşterea posibilității de a interpreta în mod alternativ dovezile.
Introducerea proceselor de „logica colaborativă cu voce tare".	Va duce la dialoguri structurate pentru a putea acoperi toate posibilitățile.
Folosirea blogurilor ca un instrument de producție.	O platformă comună şi continuă pentru a completa *„dialogul virtual"* pe tema alternativelor.
Pregătirea constantă a rapoartelor de după acțiune.	Studierea eşecurilor şi succeselor cu ochi critic pentru a extrage lecții constructive.
Oferirea posibilității de a învăța din experiență prin intermediul consumatorilor. Susținerea analiştilor în acțiuni de reflecție şi introspecție.	Scurte simulări/jocuri pentru a ajuta consumatorii să înțeleagă raza incertitudinii. Permiterea unui răgaz pentru *premortem* şi pentru exerciții de după acțiune.
Căutarea de dovezi care pot nega sau combate orice ipoteză concurentă.	Se poate ajunge la o supoziție care nu poate fi negată, cel puțin nu încă, şi astfel poate fi folosită până când sau dacă este negată. Justificarea pentru adoptarea unei astfel de ipoteze nu este faptul că este susținută de dovezi, ci faptul că nu poate fi negată sau combătută de informațiile pe care le putem descoperi şi cunoaşte.

Bibliografie

1. Ben-Zvi, Abraham, „Perception, Misperception and Surprise in the Yom Kippur War: A Look at the New Evidence", în *Journal of Conflict Studies*, Volume XV, Number 2, Fall 1995, Centre for Conflict Studies, University of New Brunswick, Fredericton, New Brunswick, Canada, la http://www.lib.unb.ca/Texts/JCS/Fall95/ben-zvi.pdf.

2. Bell, Bowyer J., „Toward a Theory of Deception", *International Journal of Intelligence and Counterintelligence 16*, No. 2 (Summer 2003).

3. Bracken, Paul, Bremmer Ian, Gordon David (editors), *Managing Strategic Surprise: Lessons from Risk Management and Risk Assessment*, Cambridge University Press, 2008.

4. Celaya, Fernando, „To what extent was Western intelligence at fault in failing to indentify the nature of the terrorist threat before 9/11 and its aftermath?", în *Athena Intelligence Journal*, Vol. 4, No. 1, 2009.

5. Cissé, Amadou, „Peut-on parler d'une faillite du renseignement américain avec les événements du 11 septembre 2001?", *Dossier de recherche, Ecole des Hautes Etudes Internationales*, 2004.

6. Clark, Robert M., *Intelligence Analysis: A Target-Centric Approach*, Washington DC, SUA, Ed. CQ Press – A Division of Congressional Quarterly Inc., 2007.

7. Dahl, Arden B., Major, *Command Dysfunction. Minding the Cognitive War*, USAF, School of Advanced Airpower Studies, Air University Press, Maxwell Air Force Base, Alabama, May 1998.

8. Dahl, Erik J., *Warning of terror: Explaining the failure of intelligence against terrorism*, Master of Arts in Law and Diplomacy Thesis, The Fletcher School, January 2004.

9. Davis, Jack, „Improving CIA Analytic Performance: Strategic Warning", The Sherman Kent Center for Intelligence Analysis, *Occasional Papers: Volume 1*, Number 1, Sept. '02.

10. Diamond, John M., *The CIA and the Culture of Failure: U.S. Intelligence from the End of the Cold War to the Invasion of Iraq*, Stanford University Press, 2008.

11. Diaz, Gustavo, „Methodological approaches to the concept of intelligence failure", în *UNISCI Discussion Papers*, January 2005.

12. Dumitru, Irena, *Psihologia analizei informațiilor*, suport de curs, București, Editura Academiei Naționale de Informații *„Mihai Viteazul"*, 2009.

13. George, Roger Z., Bruce, James B. (ed.), *Analyzing intelligence. Origins, obstacles and innovations*, Washington DC, Georgetown University Press, 2008.

14. Godson, Roy and Wirtz, James J., eds., *Strategic Denial and Deception: The Twenty-First Century Challenge*, New Brunswick, NJ: Transaction Publishers, 2002.

15. Herbig, Katherine L. and Daniel, Donald C., „Strategic Military Deception", în *Intelligence: Policy and Process*, ed. Alfred C. Maurer, Marion D. Tunstall, and James M. Keagle, Boulder, CO: Westview Press, 1985.

16. Heuer, Richards J., Jr., „Limits of Intelligence Analysis", în *Orbis, Winter 2005*, Foreign Policy Research Institute.

17. Hilsman, Roger, *Strategic Intelligence and National Decision*, New Jersey, Princetown University Press, 1953.

18. Jajko, Walter, „Deception: Appeal for Acceptance; Discourse on Doctrine; Preface to Planning", *Comparative Strategy 21*, No. 5, October-December 2002.

19. Johnston, Rob, *Analytic Culture in the US Intelligence Community*, Washington DC: Center for the Study of Intelligence, 2005.

20. Krishnadas, Devadas, *Imagining Surprise: Locating the Causality of Strategic Surprise*, Master of Arts in Law and Diplomacy Thesis, 1 February 2005, The Fletcher School.

21. Klein, Gary, *Intuition at Work: Why Developing Your Gut Instinct Will Make You Better at What You Do*, New York, Doubleday, 2002.

22. Kruys, H Brig Gen G P (rtd), Intelligence failures: Causes and contemporary case studies, University of Pretoria, Institute for Strategic Studies, 2006.

23. Laqueur, Walter, *World of Secrets. The Uses and Limits of Intelligence*, New York: Basic Books, 1985.

24. Levy, Jack S., „Misperception and the Causes of War: Theoretical Linkages and Analytical Problems", în *World Politics*, Vol. 36, No. 1 (Oct. 1983), The Johns Hopkins University Press.

25. Lowenthal, Mark, „The Burdensome Concept of Failure", în Maurer, Alfred C., Tunstall, Marion D. and Keagle, James M. (eds.) (1985): *Intelligence: Policy and Process*. Boulder, Westview Press.

26. Marrin, Stephen, „Preventing Intelligence Failures by Learning from the Past", în *International Journal of Intelligence and CounterIntelligence*, Volume 17, Number 4, 2004.

27. Mitnick, Kevin, *The Art of Deception*, Wiley Publishing, Inc., 2003.

28. Mouton, Troy M., *Organizational culture's contributions to security failures within the United States Intelligence Community*, University of Southwestern Louisiana, May 2002 (teză de masterat în *„Liberal Arts"*).

29. Prothro, John Samuel, *The Misguided Reaction: Reconsidering Intelligence Flow before 11 September 2001*, (teza de master la Texas A & M University), August 2004.

30. Record, Jeffrey, *Japan's decision for war in 1941: Some enduring lessons*, Strategic Studies Institute, US Army War College, February 2009.

31. Rodgers, R. Scott, *Improving Analysis: Dealing with Information Processing Errors*, Warfighter Interface Division, Cognitive Systems Branch, November 2006, Interim Report for October 2003 to November 2006.

32. Tockman, Kristine (coord.), „Iran: Intelligence Failure or Policy Stalemate?", în *Working Group Report*, No. 1, november 23, 2004.

33. Varouhakis, Miron, „Fiasco in Nairobi. Greek Intelligence and the Capture of PKK Leader Abdullah Ocalan in 1999", în *Studies in Intelligence*, Vol. 53, No. 1 (Extracts, March 2009).

34. Waters, Lonn Augustin, *Secrecy, Deception and Intelligence Failure: Explaining Operational Surprise in War*, Massachusetts Institute of Technology, September 2005. (teză master în Ştiinţe politice)

35. Shulsky, Abram N., Schmitt, Gary J., *Războiul tăcut. Introducere în universul informaţiilor secrete*, Iaşi, Editura Polirom, 2008.

36. Spinney, F., „Learning the Lesson We Want to Learn?", în *Proccedings*, SUA, Vol. 125, Nr. 9, sept. 1999.

37. Tsang, Steve, *Serviciile de informaţii şi drepturile omului în era terorismului global*, Bucureşti, Editura Univers Enciclopedic, 2008.

38. Waltz, Edward, Michael, *Bennett,* Counterdeception: Principles and Applications for National Security, Artech House, Inc., 2007 – 117 USD la Amazon.com.

39. Whaley, Barton, *Stratagem: deception and surprise in war*, Artech House, Boston, London, 2007.

40. Whaley, Barton and Busby, Jeffrey, „Detecting Deception: Practice, Practitioners, and Theory", în *Strategic Denial and Deception: The Twenty-First Century Challenge*, ed. Roy Godson and James J. Wirtz, New Brunswick, NJ, Transaction Publishers, 2002.

41. Whaley, Barton, „Toward a General Theory of Deception", *Journal of Strategic Studies 5*, no. 1 (March 1982).

42. Whaley, Barton, *Detecting deception: A bibliography of counterdeception across time, cultures, and disciplines*, Second Edition, Foreign Denial & Deception Committee Washington, DC, March 2006.

Cristian NIŢĂ este absolvent al Facultăţii de Istorie, Universitatea Bucureşti (1997), al Facultăţii de Ştiinţe Politice, Universitatea Bucureşti (2002), iar, în prezent, este doctorand al Academiei Naţionale de Informaţii *„Mihai Viteazul"*, în domeniul ştiinţe militare-informaţii, cu un proiect de cercetare referitor la rolul comunităţii de informaţii israeliene în gestionarea conflictelor din Orientul Mijlociu. A participat la o serie de conferinţe şi sesiuni de comunicări în domeniul securităţii şi a publicat un număr de articole şi studii referitoate la intelligence-ul modern sau problematica de securitate a Balcanilor de Vest, a Regiunii Extinse a Mării Negre sau a Orientului Mijlociu.

Ghidul analistului. Compendiu pentru analiştii de intelligence – o pledoarie pentru reconceptualizarea instrumentarului analitic în problematica de securitate

Adrian ENE
Marius PERIANU
Serviciul Român de Informaţii
e-mail: **ani@sri.ro**

Motto
„Analistul are trei deziderate: să cunoască totul, să fie crezut şi să exercite o influenţă pozitivă asupra sistemului culegerii şi valorificării informaţiilor."
(Sherman Kent)

Abstract
During the past decade, the international security environment has significantly changed under the influence of globalization, information revolution and the ever increasing complexity of risks. As a result, intelligence agencies have to adapt to new security challenges by stressing upon analysis rather than collection of intelligence.
The analysts within the Romanian Intelligence Service have also put much effort into improving the accuracy of their assessments and prognosis by adapting new methods and techniques available in the academic field to the specific needs of intelligence analysis.
Keywords: intelligence analysis, analytical methods and tools.

Argument

Dacă iniţial studiile de *intelligence* au constituit un domeniu aproape „prohibitiv", adresându-se, în special, personalului militar specializat, sfârşitul Războiului Rece a impus, practic, redefinirea conceptului de securitate, din perspectiva noilor ameninţări (esenţialmente „polimorfe", cu geneză multisectorială), diversificării surselor de risc şi dispersiei lor geografice, precum şi a dezvoltării interconexiunilor între fenomene şi manifestări aparent independente.

Mutațiile înregistrate la nivelul mediului actual de securitate a validat, finalmente, o modificare de paradigmă care s-a tradus inclusiv prin demilitarizarea studiilor de securitate.

O tendință majoră în activitatea de *intelligence*, îndeosebi după 11 septembrie 2001, a reprezentat-o şi sporirea vizibilității serviciilor de informații, atât la nivelul beneficiarilor, cât şi la cel al percepției publice, inclusiv ca răspuns la presiunile exercitate de societatea civilă – devenită, între timp, deosebit de sensibilă față de eforturile pentru combaterea terorismului – în scopul creşterii transparenței acestui proces.

În aceste condiții, nu poate fi ignorată creşterea progresivă a accesibilității informațiilor în ceea ce priveşte natura şi obiectivele domeniului *intelligence* la nivelul societății civile, cu atât mai mult cu cât în ultimii ani au apărut numeroase studii şi cercetări, menite să popularizeze/promoveze în rândul publicului realitățile acestui domeniu, ca „alternativă" la imaginea conturată de filmele hollywoodiene cu superspioni invulnerabili.

În consecință, studiile de *intelligence* au devenit tot mai accesibile publicului, ca o componentă a culturii de securitate.

Agențiile de informații din unele state au realizat parteneriate cu mediul academic (universități, centre de cercetare etc.) pentru organizarea de cursuri, cercetări şi diverse alte activități conexe domeniului securității naționale, iar unele centre de studii coodonează programe de *internship*, pentru atragerea studenților din cadrul diverselor instituții de învățământ superior, în scopul familiarizării lor cu domeniul *intelligence*[1].

Nu în ultimul rând, este deja un adevăr unanim acceptat faptul că actuala eră de globalizare a informației şi disoluție a monopolurilor asupra cunoaşterii şi circulației ideilor (din sfera privată, academică ori instituțională), caracterizată printr-o multiplicare fără precedent a datelor şi informațiilor şi un acces tot mai extins şi mai rapid la acestea, impune, la rândul ei, necesitatea reevaluării paradigmei „clasice" de procesare a informației.

Altfel spus, dezvoltarea societății informaționale a constituit, la rândul său, un „motor" în procesul de modernizare a analizei de *intelligence*. Accesul practic nelimitat la datele provenite din surse deschise/publice generează, la rândul său, un paradox evident: dificultatea de a prelucra, în mod eficient, volume informaționale tot mai mari, într-un timp cât mai scurt, utilizând metode analitice „tradiționale".

[1] De altfel, încă din anul 1935, părintele analizei de intelligence, Sherman Kent, lansa ideea potrivit căreia intelligence-ul trebuie regândit drept domeniu academic.

Tendința este acut resimțită inclusiv de structurile de *intelligence*, care se confruntă cu un veritabil „diluviu" informațional, urmare a „exploziei" surselor deschise şi a fluctuațiilor tot mai imprevizibile ale noului mediu de securitate. Creşterea exponențială a ofertei informaționale (suprainformarea) tinde să redirecționeze eforturile rezolutive dinspre căutarea informației către rafinarea instrumentarului mental de interpretare a acesteia.

În raport cu toate aceste provocări, la nivelul Serviciului Român de Informații s-a conturat necesitatea inițierii unui proces de îmbogățire a actualului arsenal conceptual utilizat în elaborarea de analize şi estimări menite să fundamenteze implementarea politicilor de securitate, prin înglobarea noilor metode şi tehnici de analiză şi cercetare ştiințifice consacrate în spațiul academic.

În contextul în care majoritatea structurilor de *intelligence* (atât din zona euroatlantică, cât şi în plan global) încearcă să se adapteze la noul mediu de securitate, ideea unei asemenea transformări s-a impus ca un imperativ al momentului, cu atât mai mult cu cât, în ultimii ani, componenta analitică a devenit un factor esențial în „competiția" angajată cu ceilalți actori din „piața informațională", servicii speciale ori structuri private de analiză[2].

Pe fondul preocupării SRI pentru optimizarea componentei de analiză şi prognoză, un colectiv de analişti din cadrul Serviciului a elaborat, la finele anului 2009, lucrarea intitulată **Ghidul analistului. Compendiu pentru analiştii de *intelligence***, cu scopul de a oferi analiştilor de *intelligence*, indiferent de specializare şi nivel de experiență, un instrument de lucru menit să faciliteze însuşirea principalelor repere ale metodologiei analitice în domeniu.

Raportat la intenția autorilor (din cadrul departamentului central de analiză al SRI), mărturisită încă din prefața Ghidului, lucrarea a reprezentat, de la bun început, un demers intelectual versatil, deschis oricăror „presetări dogmatice". Pe de o parte, pentru că nu targhetează – neapărat şi exclusiv – breasla analiştilor în general ori o anumită categorie de analişti în special (delimitată tipologic ori ca nivel de expertiză), ci se adresează, la limită, tuturor celor care îşi desfăşoară activitatea în domenii ce presupun gestionarea informațiilor cu relevanță pentru securitatea națională. Pe de altă parte, Ghidul nu se plasează nicidecum sub semnul imperativului didactic, aşa cum poate

[2] Este incontestabilă, din această perspectivă, tendința – vizibilă în ultimii ani – de „privatizare" a culegerii de informații, a prelucrării şi distribuirii acesteia (merchandising intelligence), ca reflex al apariției actorilor nonstatali şi al privatizării asigurării securității în domeniul informațiilor.

sugera denumirea. Din această perspectivă, lucrarea nu reprezintă neapărat un ghid sau – mai bine spus – este, în fapt, mai mult decât un ghid. În primul rând, pentru că nu este şi nici nu aspiră să fie un *manual* (în înțelesul de *handbook* sau ghid practic destinat să faciliteze deprinderea unor tehnici analitice aplicate), ci mai curând o *propedeutică* cu caracter general la orice demers de inițiere şi perfecționare în „tehnologia" analitică de *intelligence*.

Nu în ultimul rând, titulatura de manual este inadecvată, în plus, pentru că problematica abordată în cuprinsul lucrării atinge şi subiecte considerate până de curând inedite, referitoare, spre exemplu, la deontologia analitică ori la proiecția carierei analistului de informații.

Întrucât, în prezent, există o întreagă varietate de metodologii derivate din teoriile şi/sau paradigmele cercetărilor de securitate care le-au inspirat, rămâne la latitudinea fiecărui lector să evalueze, potrivit capacității şi preferințelor personale, relevanța fiecărei tehnici pentru problematica avută în atenție, potențialul utilizării acestora fiind limitat, practic, doar de imaginația individuală a analiştilor de *intelligence*.

Aşa cum precizează şi autorii, lucrarea nu aspiră să ofere o perspectivă strict normativă, aşa cum este conturată prin reglementările interne ale Serviciului (aflate ele însele în plin proces de modificare şi adaptare la exigențele impuse de noul mediu de securitate), ci doar să clarifice şi să sistematizeze puncte de vedere şi abordări ştiințifice (academice) cu privire la resorturile intime şi „tehnologia" procesului de *intelligence* în perspectiva sa analitică.

Unul dintre principalele beneficii ale unei astfel de abordări rezidă în aceea că utilizarea Ghidului ar putea contribui în mod semnificativ la consacrarea unui limbaj comun asimilabil la nivelul sistemului intern de *intelligence* şi, implicit, instituirea unei „interoperabilități conceptuale" în raport cu metodologia analitică utilizată de servicii de informații aliate şi/sau partenere ale comunității româneşti de informații.

Totodată, grație complexității tematicii abordate (care „panoramează", în unele cazuri cu detalieri sugestive, cele mai importante aspecte ale activității de *intelligence*), lucrarea poate fi integrată cursurilor de formare/perfecționare în domeniu.

Conştienți de caracterul „perisabil" al bibliografiei utilizate, autorii Ghidului țin să sublinieze că unele dintre aspectele tratate sunt oricând pasibile de ajustări/perfecționări, în funcție de evoluțiile ce s-ar putea înregistra în perspectivă, recomandând lectorului ca, în măsura în care se consideră necesar, să extindă ori să completeze aria tematică propusă în contextul lucrării printr-o cercetare personală.

Prezentare sinoptică

Creşterea în complexitate a problematicii de securitate a produs o deplasare a accentului de la analizele de nivel tactic şi operaţional (centrate pe „informări punctuale") către evaluări şi prognoze cu caracter strategic, în măsură să furnizeze o „lentilă" cuprinzătoare asupra dinamicii evoluţiilor de risc. Concomitent, ascendentul unor actori cu preocupări în domeniul securităţii (mediul privat, comunitatea academică sau mass-media) a catalizat, în mod semnificativ, aşteptările factorilor de decizie (dar şi ale opiniei publice) în raport cu activitatea serviciilor de *intelligence* – situaţie ce a motivat, suplimentar, eforturile agenţiilor de securitate în direcţia reconceptualizării procesului analitic.

Este ceea ce îşi propun să întreprindă autorii Ghidului, într-un demers sugerat de însuşi *motto*-ul primului capitol[3], în conţinutul căruia o pondere importantă este acordată clarificării/definirii, în plan conceptual, a analizei de *intelligence*.

Pe lângă stilul utilizat (o vizibilă încercare de evitare a limbajului administrativ, „lemnos" şi neatractiv, în favoarea celui speculativ, cu veleităţi filosofice), reţine atenţia şi metodologia abordată, aproape *maieutică*, prin care analistul este invitat să conştientizeze aspecte ori nuanţe pe care, într-o exprimare socratică, „nu ştie că le ştie".

Aceste particularităţi metodologice devin evidente încă din debutul lucrării, consacrat identificării locului analizei în activitatea de *intelligence* şi încadrării conceptului de analiză a informaţiilor în contextul mai larg al problematicii referitoare la informaţia de securitate naţională.

În încercarea de a creiona o definiţie a analizei de *intelligence* (efort marcat de dificultăţi inerente, generate de plurivocitatea semantică a termenului generic de analiză, dar şi de înţelegerea parţială a conceptului de analiză a informaţiilor de securitate naţională), autorii reuşesc să surprindă, cu claritate, elementele de specificitate ale acesteia, ca proces şi produs al activităţii de *intelligence*.

Potrivit acestora, analiza de *intelligence* constituie „un demers specializat de cunoaştere asupra unei problematici determinate (cea de securitate naţională), în care sunt utilizate, în forme şi modalităţi specifice, metode şi tehnici consacrate în analiza de tip ştiinţific, în scopul formulării de explicaţii, estimări şi prognoze argumentate, utile în fundamentarea deciziei politice".

[3] „Drumul de zece mii de li începe cu primul pas" (proverb chinez).

Astfel concepută, analiza reprezintă un element constitutiv *sine qua non* în activitatea generală de *intelligence* şi o condiţie necesară pentru obţinerea unor răspunsuri obiective şi conforme cu realitatea, reflectate în informaţii de securitate naţională, în temeiul cărora beneficiarul poate adopta decizii adecvate în raport cu evoluţiile domeniului din responsabilitate.

Analiza realizată pe delicatul palier al delimitărilor conceptuale (unele inedite în peisajul abordărilor teoretice cunoscute, la momentul actual, în cadrul comunităţii autohtone de *intelligence*), oferă, totodată, autorilor oportunitatea de realiza o clasificare a analizei de *intelligence*, după criterii structural-funcţionale şi grad de complexitate, fiind identificate trei mari „specii" analitice: analiza strategică, cea tactică şi cea operaţională.

Pe fondul creşterii, la nivelul factorilor de decizie, a „apetenţei" pentru analiza de tip proiectiv – capabilă să ofere scenarii alternative de evoluţie a unui fenomen, trend în domenii de importanţă/interes strategic –, în ultima perioadă se constată o semnificativă creştere în importanţă a **analizei de nivel strategic**.

În esenţă, acest tip de analiză constituie o abordare multisectorială şi multisursă a fenomenelor cu impact major în sfera securităţii naţionale (în plan politic, militar, economic, social), cu o consistentă dimensiune predictiv-anticipativă. Rezultatul acesteia se reflectă în evaluări, prognoze, estimări, menite să fundamenteze adoptarea unor decizii strategice sau să constituie suport pentru gestionarea unor situaţii/evenimente cu impact major[4].

Dimensiunea forte a acestui tip de analiză o constituie dimensiunea anticipativ-predictivă (de prognoză), care îşi propune să identifice posibile evenimente din viitor, gradul de probabilitate a apariţiei lor, precum şi potenţialul impact al acestora asupra intereselor de securitate naţională, comunicarea unor estimări/predicţii exacte, în timp util, conferind beneficiarilor baza pentru fundamentarea unor măsuri defensive destinate prevenirii şi contracarării unor ameninţări iminente.

Analiza de tip strategic reclamă analişti cu cunoştinţe pluridisciplinare şi expertiză variată, pentru creşterea performanţelor analitice fiind încurajată constituirea de *task forces* multidisciplinare şi multistructurale pe analize dedicate, eventual echipe mixte, întărite conjunctural prin experţi OSINT şi/sau specialişti din zona operaţională (de culegere a informaţiilor).

Un alt palier analitic – situat în circuitul/fluxul informaţional pe o treaptă imediat inferioară celui strategic – este reprezentat de **analiza**

[4] Adda Bozeman, *Strategic Intelligence and Statecraft*, Pergamon-Brassey's, Washington DC, 1992.

tactică. La acest nivel sunt procesate, de regulă, informații de securitate națională referitoare la evoluții ori indicatori de amenințare identificați pe o anumită problemă sau domeniu, la consecințele previzibile sau produse ale unor acțiuni care se constituie în riscuri şi amenințări ori la elemente ce pot susține promovarea intereselor României sau ale aliaților săi.

În raport cu cea de nivel strategic, analiza tactică se concentrează pe abordarea unor problematici şi evoluții sectoriale care pot afecta interesele naționale de securitate. Procesul analitic se derulează prin evaluarea datelor şi informațiilor despre actorii implicați, obiectivele vizate, coordonatele spațiale şi temporale şi formele concrete de manifestare a situației purtătoare de risc.

Demersul analitic reprezintă o realitate ce se manifestă inclusiv pe **palierul culegerii de informații**, în cadrul căreia se desfăşoară procesarea datelor şi informațiilor factuale, rezultate din investigarea mediului de securitate intern sau internațional şi cunoaşterea profilurilor de risc. La acest nivel, analiza constă în evaluarea datelor primare din perspectiva îndeplinirii criteriilor cumulative pe care trebuie să le respecte informația de securitate națională.

Într-o asemenea perspectivă, analiza poate fi considerată un „test de rezistență", menit să diferențieze datele/informațiile cu semnificație pentru securitatea națională de ştiri de anumite pseudoproduse informaționale având la bază date amorfe şi zvonuri.

Analiza operațională (primară) se concentrează pe emiterea unor judecăți de valoare în raport cu veridicitatea şi completitudinea *datelor primare* (*de primă sesizare*), contribuind în mod semnificativ la selectarea acestora şi, ulterior, la elaborarea informațiilor de securitate națională.

Un alt element caracteristic acestei „specii analitice" îl constituie faptul că se manifestă în toate etapele activității de culegere (căutare, identificare, colectare şi verificare a informațiilor), inclusiv prin precizarea „nevoilor de informare" (pot fi continue, secvențiale sau de termen lung). De asemenea, analiza primară se aplică tuturor datelor obținute, indiferent de modul în care le este apreciată veridicitatea, raportarea la sursa informației şi la atributele probate de aceasta.

Acest tip de analiză are ca principale obiective cercetarea analitică de detaliu, estimarea dinamicii şi a tendințelor situației operative şi evaluarea stării de securitate națională, pe segmentul/zona/domeniul de competență.

În majoritatea cazurilor, informațiile culese sunt fragmentare, ambigue şi susceptibile de interpretări divergente. De aceea analiza informațiilor reprezintă o componentă vitală a activității de *intelligence*,

având drept scop, într-o accepțiune limitată, emiterea de judecăți referitoare la capacitățile, intențiile şi acțiunile (prezente ori viitoare) cu potențial de afectare a intereselor de securitate.

Natura specifică a analizei pe această dimensiune a procesului de *intelligence* reflectată, cum precizam anterior, printr-o implicare consistentă în procesul de culegere efectivă a informațiilor, nu exclude elaborarea, în situații determinate, a unor estimări privind evoluția şi tendințele stării de securitate națională, în baza disfuncțiilor, vulnerabilităților, riscurilor şi amenințărilor identificate/prognozate.

În cea de-a doua secțiune a Ghidului (referitoare la specificul tipologiei şi dimensiunilor structural-formative ale analistului de *intelligence*), este abordată, între altele, problematica referitoare la „factorii care determină/influențează procesul analitic", o atenție specială fiind acordată decelării „limitelor şi erorilor de analiză".

Autorii reuşesc să surprindă, în acest punct al studiului, faptul – confirmat de psihologia cognitivă – că percepțiile oamenilor şi modul în care aceştia procesează informațiile sunt puternic influențate de educație, experiență, valori culturale, cerințe ale postului, norme organizaționale, precum şi de specificul informațiilor primite.

Toate acestea formează „lentile" (*modele*/*tipare*/*fixații mentale* sau *„presupoziții de ordin analitic"*) prin care indivizii se raportează la realitatea obiectivă, dar care pot distorsiona percepțiile, oferind nu mai mult decât o reprezentare (subiectivă) a ceea ce oamenii cred că ştiu despre lumea exterioară.

În condițiile incapacității de a asimila complexitatea realității, indivizii recurg la construcția de modele mentale simplificate ale lumii obiective, cărora le suprapun informațiile primite ulterior, fără să existe întotdeauna o compatibilitate între *input*-ul informațional şi propria schemă de gândire.

Nu toate capcanele pe care procesul mental le întinde analiştilor pot fi eliminate, pentru că sunt o parte din noi, singura soluție fiind cunoaşterea şi dezvoltarea unor proceduri de evitare sau înlăturare a lor.

Corelativ, elaborarea unui produs analitic prezintă, în general, un traseu bine determinat, caracterizat de următoarele etape: operații de *data mining*, sortare, clasificare, verificare, alocare şi evaluare a informațiilor; supunerea datelor obținute unor metode de analiză. În mod inerent, apar o serie de probleme şi erori de procesare analitică (imaginea în oglindă, paradigma eficienței, paradoxul specializării), ceea ce implică riscuri de alterare a diagnozelor şi prognozelor.

Din acest motiv, se impune auditarea produselor analitice. În scopul asigurării unei pregătiri şi adaptări continue, analistul trebuie să-şi dezvolte abilităţi practice de realizare şi prezentare a diferitelor materiale (sinteze, evaluări, rapoarte). Pentru asigurarea perceperii rapide şi unitare a informaţiilor din document, este nevoie de respectarea unor reguli ale arhitecturii *output*-ului (importanţa titlului şi a punctului central, tehnica piramidei inversate, construirea argumentaţiei etc.).

În contextul larg al dezbaterilor referitoare la necesitatea identificării de noi instrumente menite să crească acurateţea judecăţilor emise de analiştii de *intelligence*, unii gânditori care s-au aplecat mai îndeaproape asupra acestui proces, precum, de exemplu, Richards Heuer, insistă asupra **necesităţii ca analiştii să-şi conştientizeze propriul proces raţional**, respectiv să-şi împartă echitabil efortul între gândirea modului în care îşi construiesc judecăţile şi concluziile, respectiv gândirea judecăţilor şi concluziilor în sine.

Consonant, David T. Moore abordează conceptul de **gândire critică**, definită ca acţiune intenţionată, deopotrivă cognitivă (*gândire*) şi metacognitivă (*gândirea despre gândire*), prin intermediul căreia analistul reflectă simultan atât la procesul de raţionare, cât şi la raţionamentele prin care ajunge la o concluzie. Potrivit acestuia, gândirea critică subsumează două obiective la fel de importante: identificarea unei soluţii şi îmbunătăţirea raţionamentului.

Emiterea unei judecăţi ori formularea unei concluzii echivalează cu luarea unei decizii pe baza unor indicaţii şi probabilităţi, atunci când faptele analizate comportă un anumit grad de incertitudine/incompletitudine. Judecata presupune pătrunderea dincolo de informaţiile disponibile, fiind principala modalitate de gestionare a incertitudinii, utilizată cu predilecţie de analiştii de *intelligence*, care, cel mai frecvent, se află în situaţia de a opera cu date incomplete, ambigue şi/sau contradictorii.

Din această perspectivă, funcţia analistului de informaţii poate fi descrisă ca depăşire a limitelor informaţiei incomplete, printr-un exerciţiu de judecată analitică în care angrenează strategii de procesare a informaţiilor, la rândul lor importante pentru că pot influenţa direct rezultatul analizei.

Dimensiunea psihologică a analizei în sfera *intelligence* poate fi evidenţiată de abordarea descriptivă a celor cinci etape din componenţa procesului analitic, respectiv: definirea problemei, generarea ipotezelor, culegerea informaţiilor, evaluarea ipotezelor (utilizând strategii de selectare a celor mai probabile dintre acestea) şi monitorizarea continuă a informaţiilor noi.

Cu aceste considerații, intrăm, practic, în cea de-a treia secțiune a Ghidului, dedicată prezentării celor mai importante „metode şi tehnici în analiza de *intelligence*", consacrate în spațiul ştiințific, utilizate în scopul obținerii şi valorificării informațiilor de securitate națională.

În context, este prezentat, în detaliu, un spectru tipologic complex de procedee analitice, dintre care se detaşează: analiza de trend (sau de tendință), analiza contextuală, analiza comparativă, analiza SWOT, analiza cost-beneficiu, analiza de conținut, prognoza (ansamblu metodologic complex sub cupola căreia sunt abordate metoda scenariilor, metoda Delphi, analiza de impact transversal, metoda Brainstorming şi variantele ei).

Aşa cum observă şi autorii Ghidului, preocupările destinate sistematizării şi teoretizării activității de analiză a informațiilor consacră ideea potrivit căreia analiza informațiilor de *intelligence* trebuie să se desprindă de abordări empirice şi să revendice statutul de cunoaştere ştiințifică care să includă, în funcție de matricea analitică selectată, măsurători, calcule, comparații în termeni de cantitate/calitate, explicații şi anticipări.

Fie că este vorba de modalități de cunoaştere şi utilizare a unor resurse informaționale ori de proceduri de sistematizare a anumitor date şi cunoştințe, de metode de investigare (cantitative şi calitative) sau de instrumentare matematice, statice, dinamice şi tehnici electronice de calcul, folosirea procedeelor analitice condiționează în cel mai înalt grad corecta derulare şi succesul unui demers analitic obiectiv, cu şanse de a genera un diagnostic întemeiat asupra unei (unor) evoluții într-un domeniu sau altul de securitate națională.

Diversitatea subiectelor, a temelor şi problemelor supuse demersului analitic, precum şi a modalităților de abordare a acestora şi de elaborare a documentelor de informare către beneficiari face imposibilă aplicarea, într-o manieră predeterminată, a unor metode şi tehnici de analiză. În consecință, utilizarea metodologiei – atât de necesară şi importantă în orice act de cunoaştere – trebuie să se realizeze într-o modalitate cât mai flexibilă.

Această din urmă concluzie constituie, de altfel, caracteristica dominantă a desfăşurării efective a procesului analitic în zona de *intelligence*, în măsura în care o parte importantă a datelor şi informațiilor procesate este marcată de un grad ridicat de incertitudine şi incompletitudine. De aceea, se impune acordarea unei atenții cu totul speciale modalităților prin care sunt utilizate diverse metode sau tehnici consacrate în domenii în care gradul de incertitudine şi ambiguitate a bazelor de date utilizate este mai redus.

Potrivit autorilor, conştientizarea acestor limite presupune:

(1) evaluarea cât mai obiectivă a riscurilor induse de folosirea metodologiei analitice asupra unor baze de date incomplete, ceea ce impune o selectare judicioasă a metodelor şi tehnicilor utilizate în raport de specificul/particularităţile datelor procesate;

(2) adoptarea unei perspective accentuat critice în ceea ce priveşte validitatea judecăţilor analitice formulate asupra unor elemente informaţionale incomplete, lacunare, confuze, ceea ce favorizează recunoaşterea limitelor care pot marca – uneori într-un mod esenţial – demersul analitic.

Precaritatea datelor asupra cărora se exercită procesul analitic, precum şi limitele „naturale" ale metodelor şi tehnicilor utilizate favorizează una dintre cele mai accentuate tentaţii la care este supus analistul de *intelligence*: elaborarea unor explicaţii speculative prin „forţarea" limitelor de aplicabilitate/validitate ale metodei utilizate şi glisarea către abordări „intuitive", nesusţinute de realitate.

În multe situaţii, „fundamentarea" acestor construcţii speculative este explicată prin utilizarea aşa-numitelor *„metode şi tehnici specifice"*, sintagmă caracteristică jargonului profesional, lipsită de conţinut şi care poate „justifica", în fond, orice fel de concluzie.

În fapt, **miza/provocarea fundamentală ce caracterizează analiza informaţiilor de securitate constă nu în utilizarea – „de o manieră specifică", particulară, neîntâlnită în alte domenii – unui set de metode şi tehnici consacrate, ci în aplicarea inteligentă (versatilă, flexibilă) a acestora, în funcţie de limitele formulate mai sus.**

Această viziune este, de altfel, larg împărtăşită în comunitatea analiştilor de *intelligence*. Se admite, în genere, că pe lângă aptitudinile înnăscute şi cele dezvoltate în procesul de instruire, eficienţa activităţii analistului depinde, în mod esenţial, de metodologia (concepte, instrumente şi tehnici analitice) utilizată. **Aşadar, în acest plan, nu există soluţii universal valabile, cele mai bune evaluări fiind generate, de regulă, ca efect al combinării tehnicilor disponibile, în funcţie de specificul şi de complexitatea fenomenelor abordate.**

Justeţea acestei concluzii traversează, de altfel, întreg cuprinsul Ghidului, care se doreşte, din această perspectivă, o pledoarie pentru ideea de abordare a problematicii circumscrise analizei informaţiilor dintr-o perspectivă integratoare, flexibilă şi interdisciplinară. La fel de adevărat este, de asemenea, că – aşa cum aprecia un renumit teoretician al analizei de *intelligence* – **cea mai bună metodă analitică este, înainte de toate, un analist foarte bun.**

Dar cum reuşita unui *aggiornamento* în domeniul analitic depinde, în mod esențial, de configurarea unei relații dinamice între individ (analist) şi sistem (în acest caz, de comunitatea de informații în ansamblul său), schimbarea de paradigmă şi rafinarea instrumentarului metodologic în domeniu derivă, esențial, din modul în care acest proces se reflectă la nivelul principiilor de organizare şi funcționare a serviciilor de informații.

În aceeaşi ecuație relațională, este dezirabil ca analistul să adopte o conduită întemeiată pe tenacitate. El trebuie să-şi susțină opiniile (fundamentate pe o cunoaştere profundă a problemei investigate) indiferent cât de „inadecvat" ar putea „suna", într-o oarecare conjunctură, concluziile demersului analitic. O atitudine similară se impune a fi adoptată de către analist în demersul de reconsiderare/reformulare a concluziilor, atunci când apar noi elemente, de natură să modifice datele inițiale ale problemei.

Încurajarea unor astfel de atitudini se poate realiza prin promovarea tipurilor de activități care pun analiştii în confruntare cu perspective alternative, consultarea cu experți din exteriorul sistemului de securitate, dezbateri analitice, analize concurente, dezbateri interdisciplinare. Această abordare este cu atât mai necesară cu cât, deseori, beneficiarii informării solicită ca produsul finit de *intelligence* să includă scenarii alternative, pentru a se reduce cât mai mult elementele de incertitudine.

Nu în ultimul rând, o condiție *sine qua non* a asigurării adaptabilității sistemului de *intelligence* la valurile succesive de provocări ale mediului de securitate o reprezintă preocuparea în plan instituțional de a favoriza creativitatea şi spiritul inovativ. Situată în opoziție cu spiritul de rutină şi aflată în conflict cu birocrația excesivă, creativitatea (şi complementul ei, spiritul inovativ) în domeniul analizei informațiilor se manifestă prin capacitatea de a pune în valoare ipoteze, proiecte, teme ş.a.m.d. poziționate în afara „paradigmei consacrate" şi prin utilizarea de metodologii nespecifice/atipice, care însă se dovedesc utile procesului analitic.

Favorizarea acestor modalități de îmbogățire a activității de informații poate conduce nu doar la apariția unor remodelări de fond ale unor perspective explicative asupra evoluțiilor de securitate, ci şi la reconceptualizarea managementului şi a instrumentarului analitic.

Rezultă, astfel, cu puterea evidenței, că activitatea agențiilor de *intelligence* trebuie (re)configurată pentru a reflecta lumea în care trăiesc, astfel încât, atunci când lumea se schimbă, este important ca serviciile de informații să evolueze împreună cu ea.

În condițiile în care istoria ne oferă numeroase exemple că lipsa de preocupare pentru adoptarea unei paradigme flexibile, capabilă să răspundă eficient mutațiilor intervenite în contextul de securitate, a determinat disfuncții majore, cu impact în exercitarea actului de autoritate, este de la sine înțeles că o preocupare formală (superficială ori „mimată") generează, mai devreme ori mai târziu, acelaşi tip de repercusiuni.

Concluzia firească a acestor realități – concordantă, în esență, viziunii promovate de autorii Ghidului – este aceea că nu există, practic, alternativă la procesul de adaptare a structurilor de informații la evoluțiile mediului de securitate, a căror dinamică tinde să se situeze, de multe ori, cu precădere în sfera analitică, cu un pas în fața demersurilor instituționale de reconfigurare a arhitecturii de *intelligence*.

Bibliografie selectivă

1. *Ghidul analistului. Compendiu pentru analiştii de intelligence,* elaborat de un colectiv de analişti ai Serviciului Român de Informații (în curs de apariție).

2. Jeffrey R.Cooper*, Curing analytical pathologies – pathways to improved intelligence analysis,* Center for the Study of Intelligence, 2005.

3. Mihaela Stoica, „Studiile de intelligence în viziunea europeană şi națională", *Revista Română de Studii de Intelligence*, Nr. 1-2 / decembrie 2009, Bucureşti.

4. Moore T. David, *Gândirea critică şi analiza informațiilor*, Colegiul Mixt de Informații Militare, Washington DC, 2006.

5. Richards J.Heuer Jr., *Psychology of Intelligence Analysis*, Center for the Study of Intelligence, 1999.

6. William J.Lahneman (coord.), *The Future of Intelligence Analysis* (vol. I, II), Center for International and Security Studies, 2006.

7. Directoratul de Analiză al CIA, *Abecedarul Tehnicilor Informative: Tehnici Analitice Fundamentale*, martie 2008.

Adrian ENE este licențiat al Facultății de Filosofie din cadrul Universității Bucureşti şi specialist în analiza de intelligence.

Marius PERIANU este licențiat al Facultății de Istorie, respectiv al Facultății de Ştiințe Politice din cadrul Universității Bucureşti şi are un master în Ştiințe Politice. Este expert în analiza de intelligence, coordonator al unor programe de instruire profesională în domeniul analizei de informații şi autor al unor studii de specialitate.

Securitate şi dezvoltare durabilă
Informaţii strategice privind mediul înconjurător (I)

Ana Ligia LEAUA
Serviciul Român de Informaţii
e-mail: **analigialeaua@yahoo.com**

Abstract

The research on environment and security, while limited, has brought attention to the growing salience of non-conventional security threats. It has also stimulated discussion on issues of environment and human security. It appears that this latter discussion may provide a useful framework within which to address development issues, particularly since it recognises that environmental problems must be analysed from a broad perspective that encompasses economic, political, cultural and demographic systems. It, thus, emphasises the extent to which understanding the context is crucial to successful development and security strategies. Undertaking research on the role that environmental degradation plays in contributing to insecurity also assists in clarifying what other factors may be important contributors to insecurity and conflict. For example, research on environment and security often strengthens the conclusion that poverty is a key factor in causing tension, unrest and, eventually, conflict. In short, linking environmental change to a broad concept of security is a useful and insightful approach to many contemporary problems.

Keywords: Environment, human security and sustainable development, environment and conflict, environmental security, environmental and security risk, environmental security policies.

Studiul modului în care problemele legate de mediul înconjurător şi preocupările privind climatul de pace şi securitate interacţionează este departe de a fi o iniţiativă monolitică. Se consideră tot mai mult că precaritatea resurselor şi degradarea mediului înconjurător joacă un rol important în generarea sau amplificarea conflictelor. Epuizarea resurselor de apă, degradarea terenurilor arabile, decimarea pădurilor, precum şi intervenţia masivă asupra ecosistemelor reprezintă principalele procese de schimbare a mediului induse de activitatea umană. Schimbarea climatică sporeşte şi mai mult provocările cu care deja ne confruntăm, prin creşterea nivelului mărilor, schimbarea zonelor de vegetaţie, micşorarea habitatelor naturale, schimbarea regimului de precipitaţii şi generarea unor furtuni mai dese şi mai intense, inundaţii şi secetă.

Problemele privind mediul înconjurător sunt strâns legate de alți factori. Degradarea mediului poate fi determinată şi, uneori, sporită de diferențele sociale, rivalitățile etnice şi comunitare, precum şi de dinamica evoluțiilor politice. Numeroase presiuni (a căror formă variază de la caz la caz), inclusiv sărăcia persistentă, repartizarea disproporționată a resurselor, distribuția inegală a terenurilor, şomajul şi nesiguranța locurilor de muncă, creşterea populației, epidemiile, precum şi degradarea mediului înconjurător generează stresul social, nemulțumirea şi polarizarea, conducând astfel la conflicte politice în multe țări şi chiar la violențe devastatoare în unele dintre acestea.

Acestă lucrare se axează pe potențialele provocări cu care ne vom confrunta în viitor şi pe legătura dintre cercetarea în domeniul securității mediului, adaptată nevoilor de intelligence, şi politicile strategice. Deşi situația mediului înconjurător reprezintă una dintre cele mai importante preocupări actuale, totuşi, majoritatea analizelor nu abordează acest aspect. Prezenta dezbatere analizează nevoia de noi definiții în sfera securității în ceea ce priveşte securitatea mediului, în special rolul vulnerabilităților şi riscurilor în anticiparea schimbărilor critice ale mediului înconjurător. Spre deosebire de alte abordări din trecut ale problemelor legate de mediu, se subliniază faptul că este nevoie de o integrare mai accentuată a sistemelor energetice, de mediu, economice, sociale şi politice.

Energia, resursele de apă, securitatea alimentară şi bolile infecțioase se numără printre principalele preocupări în relația mediu-securitate-conflict. Întrebarea rămâne dacă presiunile crescânde asupra mediului şi resurselor vor submina securitatea şi stabilitatea sau dacă sistemele noastre politice, guvernamentale şi de securitate vor putea să le gestioneze paşnic.

> *„Avem oportunitatea de a formula şi de a urma o nouă agendă pentru securitatea națională şi globală. În primul rând, securitatea noastră este amenințată de criza globală a mediului înconjurător, ceea ce ar face ca şi celelalte progrese să fie neînsemnate, dacă nu gestionăm corespunzător această situație. Făcând parte din comunitatea internațională, trebuie să dovedim că suntem destul de înțelepți să controlăm ceea ce am fost destul de deştepți ca să creăm. Trebuie să înțelegem că vechea concepție de securitate globală – care se axează, aproape în întregime, pe armate, ideologii şi geopolitică – trebuie să fie extinsă."*
>
> (Al Gore, *Asaltul asupra rațiunii*, 2007)

I. Mediu, securitate şi dezvoltare

Cel puţin de la sfârşitul anilor ’80 şi începutul anilor ’90, relaţia dintre mediul înconjurător şi dezvoltare a fost promovată la nivelul politicilor guvernamentale interne şi externe, precum şi la nivelul relaţiilor internaţionale. În urma apariţiei Raportului Brundtland, în anul 1987, şi organizarea Summitului Pământului, în 1992, este dificil să identificăm vreun guvern sau o organizaţie internaţională/interguvernamentală care să nu recunoască oficial că protecţia mediului înconjurător şi dezvoltarea umană durabilă sunt interconectate şi care să nu includă, cel puţin la un anumit nivel, legăturile dintre aceste două obiective în cadrul legislaţiei, iniţiativelor, programelor sau proiectelor derulate.

Probabil, mai recent, o mai mare recunoaştere oficială a început să fie acordată unui alt tip de relaţie studiată timp de mai multe decenii, şi anume relaţia dintre dezvoltare şi securitate şi nevoia de politici şi practici de cooperare în domeniul contracarării conflictelor. Economiştii, cercetătorii în domeniul politic, şi acum politicienii, încearcă să înţeleagă mai bine cauzele generatoare de insecuritate în zonele subdezvoltate, precum şi relaţia pozitivă şi, în acelaşi timp, solidă, dintre securitate şi dezvoltare.[1]

În contextul în care comunitatea statelor dezvoltate renunţă să mai evalueze progresul, în principal, în termeni de creştere economică şi se îndreaptă spre o abordare mai holistică, aceasta devine conştientă de diversele modalităţi în care activităţile derulate – care, adeseori, conduc la o redistribuire a puterii – pot afecta ecosistemele, pot promova sau submina mecanismele de securitate locale, naţionale şi regionale.

Conştientizarea legăturilor existente între mediul înconjurător, conflicte şi securitate poate ajuta agenţiile de dezvoltare să furnizeze asistenţa necesară susţinerii altor obiective, având cât mai puţine efecte secundare negative.

În prezent, există o nevoie tot mai mare de a înţelege mai bine sursele umane ce produc schimbările de mediu şi modalităţile în care factorii de mediu se combină cu forţe economice, sociale şi politice cu scopul de a genera, amplifica sau cauza violenţe şi insecuritate. Comunitatea statelor dezvoltate a demonstrat deja faptul că a conştientizat importanţa

[1] Ronald A. Kingham, *Inventory of Environment and Security Policies and Practices, Objectives and Methodology*, Institute for Environmental Security, 2006.

acestor legături şi şi-a exprimat angajamentul de a găsi modalități eficiente de a le gestiona. Specialiştii în domeniul securității mediului pot contribui la această analiză, precum şi la acțiunile generate de aceasta.

Totuşi, ar fi greşit şi contraproductiv să sugerăm faptul că securitatea mediului reprezintă un simplu cuvânt-cheie pentru dezvoltarea durabilă, cu toate că, în practică, preocupările ambelor comunități s-ar putea adeseori intersecta. Dezvoltarea implică o îmbunătățire graduală a nivelului de trai şi extinderea oportunităților astfel încât indivizii să beneficieze de un mediu sigur, sănătos şi demn. Securitatea sugerează o eliberare de pericol. Uneori, acest lucru se traduce prin eliberarea de lucrurile care amenință procesul de dezvoltare sau rezultatele procesului de dezvoltare. Securitatea comportă, de asemenea, un aspect conservator: procesul de dezvoltare poate deveni o amenințare la adresa securității în măsura în care subminează neintenționat – sau intenționat – mecanismele tradiționale de menținere a securității prin redistribuirea puterii într-o societate sau regiune.

I. 1. Mediu, securitate umană şi dezvoltare durabilă

Definiția securității umane oferită de Programul Națiunilor Unite pentru Dezvoltare (UNDP)[2] include şapte categorii de amenințări:

- securitatea economică (asigurarea venitului de bază);
- securitatea alimentară (accesul din punct de vedere fizic şi economic la alimente);
- securitatea sanitară;
- securitatea mediului (accesul la rezerve de apă potabilă, aer curat şi un ambient natural nedegradat);
- securitatea personală (asigurarea securității împotriva violențelor şi amenințărilor);
- securitatea comunității (asigurarea securității împotriva epurărilor etnice);
- securitatea politică (protejarea drepturilor şi libertăților fundamentale ale omului).

UNDP este de acord cu ideea că securitatea umană nu trebuie echivalată cu dezvoltarea umană. „Dezvoltarea umană este un concept mai cuprinzător, definit drept un proces de extindere a opțiunilor aflate la

[2] UNDP (United Nations Development Program). *The Human Development Report*, Oxford: Oxford Univ. Press,1994.

dispoziția oamenilor. Securitatea umană se defineşte prin faptul că oamenii se pot bucura de aceste alegeri în libertate şi siguranță."

Utilizarea termenului „securitate umană" reprezintă o recunoaştere a interconexiunilor dintre mediu şi societate, confirmându-se în acelaşi timp că percepțiile noastre privind mediul înconjurător şi modul în care acesta este folosit sunt construite pe rațiuni istorice, sociale şi politice. O strategie complementară ar trebui să construiască un index al insecurităților umane sau al vulnerabilităților, ceea ce va contribui la identificarea țărilor care sunt „nesigure", furnizând o avertizare timpurie cu privire la faptul că un stat sau o regiune devine mai puțin sigură.

Există tot mai multe voci care susțin că degradarea mediului înconjurător poate şi, într-adevăr, generează, amplifică sau cauzează conflicte şi instabilitate, existând, de asemenea, şi o preocupare majoră potrivit căreia numărul conflictelor induse de problemele legate de mediu poate creşte. În prezent, instituțiile din sfera securității sunt solicitate să protejeze accesul la resursele mediului din alte state, precum şi la bunurile comune, şi să furnizeze sprijin în derularea operațiunilor umanitare, cauzele multora dintre acestea fiind generate de problemele mediului înconjurător. Pe viitor, s-ar putea folosi forța ca răspuns la poluarea transfrontalieră sau pentru a implementa legea internațională privind protecția mediului. Însă experții pe probleme de securitate recunosc faptul că aceste conflicte pot reprezenta o forță constructivă, semnalând nevoia de schimbare la nivelul instituțional sau consolidare a capacităților. Presiunile exercitate asupra instituțiilor din cauza degradării mediului înconjurător şi epuizării resurselor ar putea reprezenta un asemenea semnal. Iar, în era armelor cu o mare capacitate de distrugere, majoritatea ar prefera ca forța să fie folosită în ultimă instanță şi ca toate eforturile posibile să fie făcute pentru a consolida şi adapta instituțiile, astfel încât să fie capabile să gestioneze eficient conflictele, înainte să se transforme în violențe extinse şi în război.

Este o mare ironie faptul că multe dintre provocările cu care ne confruntăm în prezent reprezintă consecințele neintenționate ale eforturilor noastre de a spori securitatea şi bunăstarea umanității. Din nefericire, eforturile noastre s-au axat pe:

(a) epuizarea resurselor (precum peştele, apa şi cheresteaua) într-un timp mai scurt decât cel în care acestea se pot reface;

(b) deversarea unor materiale toxice şi deşeuri pe pământ, în apă şi aer mai rapid decât acestea pot fi dezintegrate sau neutralizate;

(c) modificarea drastică a marilor ecosisteme (de la pădurile tropicale la recifurile de corali), astfel încât acestea nu mai pot susține multe specii, prejudiciindu-se totodată echilibrul climateric.

Din perspectiva securității umane, schimbarea mediului înconjurător este importantă din două puncte de vedere. În primul rând, ea însăşi poate deveni o sursă de insecuritate. Chiar dacă statul nu consideră o anumită formă de schimbare a mediului înconjurător drept o amenințare la adresa valorilor sale fundamentale sau intereselor naționale, unele segmente ale populației ar putea avea o opinie diferită. Pe de altă parte, în cazul în care statul evaluează relevanța schimbărilor de mediu în planul securității, acesta poate fi totuşi constrâns să acționeze, în măsura în care problema are dimensiuni cu accente transnaționale. În al doilea rând, modurile în care au loc aceste schimbări ale mediului pot exacerba alte forme reale sau potențiale de insecuritate, precum sărăcia, discriminarea sau terorismul.

În acest sens, raportul Organizației pentru Cooperare şi Dezvoltare Economică (OECD), intitulat *Cheltuielile militare din statele dezvoltate: securitate şi dezvoltare*[3], susține corect, în primul rând, că „securitatea este necesară pentru dezvoltare" şi, în al doilea rând, că „adevăratele cauze fundamentale ale insecurității sunt adeseori legate de dezvoltare". Este dificil să promovăm dezvoltarea într-un climat de violențe şi insecuritate. În prezent, de exemplu, fluxurile de capital privat în statele în curs de dezvoltare sunt de cinci ori mai însemnate decât asistența externă pentru dezvoltare, devenind astfel cruciale pentru procesul de dezvoltare. Însă, influxul de capital privat tinde să se diminueze în regiunile de instabilitate. În acelaşi timp, dezvoltarea poate submina mecanismele tradiționale de gestionare a conflictelor şi poate crea noi forme de insecuritate.

Astfel, într-o anumită măsură, securitatea mediului şi dezvoltarea durabilă sugerează o finalitate similară, o condiție în care:

- indivizii şi comunitățile au acces echitabil şi echilibrat la lucrurile necesare existenței şi prosperității lor;
- disputele sunt soluționate corect;
- mediul este protejat împotriva comportamentului uman distructiv.

Însă, aceşti termeni descriu, de asemenea, procesele care, pe măsură ce se îndreaptă spre punctul lor de convergență, se pot consolida sau

[3] Organisation for Economic Co-operation and Development, *Military Expenditure in Developing Countries: Security and Development*, 1997.

submina reciproc. În aceste situații, este vital ca instituțiile care asigură securitatea să fie capabile mai degrabă să se adapteze şi să se plieze schimbării, decât să încerce să o împiedice.

Este, în egală măsură, foarte important ca procesele de dezvoltare să nu ignore instituțiile ce asigură securitatea şi mecanismele de gestionare a crizelor, redistribuind puterea în aşa fel încât să genereze conflicte puternice şi violențe. Privind lucrurile în perspectivă, conflictul şi violențele pot fi descrise drept mecanisme de adaptare, însă, într-o lume a tehnologiilor cu o mare capacitate de distrugere, aceste strategii adaptive trebuie folosite cu o maximă atenție.

Armonizarea securității mediului şi dezvoltării durabile, precum şi atingerea punctului final în care acestea converg necesită receptivitate şi cooperare, rezultate din respect reciproc şi dialog permanent. De exemplu, ar fi o tragedie ca eforturile depuse în scopul dezvoltării, care s-au dovedit eficiente la nivel local, să submineze înțelegerile regionale, atent negociate, în domeniul securității sau invers.

Conceptul de securitate umană contribuie la înțelegerea interacțiunilor complexe care determină distribuirea relativă a securității şi insecurității. Mai precis, la nivelul indivizilor şi grupurilor (de la comunități mici la întreaga omenire), securitatea şi insecuritatea reprezintă, în general, o variabilă a cinci sisteme interactive, după cum urmează:

Sistem	**Mecanism de promovare a securității**	**Mecanism de promovare a insecurității**
Economic	Bogăția Politicile de bunăstare	Sărăcia Inegalitatea
Politic	Legea Forța legitimă	Corupția Utilizarea nelegitimă a forței
Cultural	Identitatea socială Justiția	Discriminarea Injustiția
Demografic	Rata scăzută a natalității Urbanizarea	Rata crescută a natalității Depopularea rapidă
Ecologic	Materii prime necesare supraviețuirii	Lipsa resurselor Maladii

În multe alte situații, securitatea şi insecuritatea se vor afla într-o legătură mai strânsă cu sărăcia, epuizarea resurselor sau discriminarea socială. În aceste cazuri, instituțiile tradiționale ce asigură securitatea pot avea o contribuție minoră sau niciuna.

Conceptul de „securitate umană" oferă un cadru comprehensiv şi integrat pentru analizarea diferitelor insecurităţi cu care se confruntă populaţiile din întreaga lume. De asemenea, acesta indică modul în care sistemele interactive fie pot genera insecurităţi, neutralizându-se reciproc, fie pot consolida mediul de securitate. Nu este surprinzător faptul că, din perspectiva securităţii umane, dezvoltarea economică ce contribuie la reducerea sărăciei va tinde să fie considerată o strategie foarte oportună deoarece sărăcia interacţionează clar cu alte sisteme – precum sistemele ecologice –, sporind gradul de insecuritate a oamenilor.

Probabil, cel mai important aspect ce ar trebui evidenţiat este acela că securitatea umană oferă o oportunitate, fără precedent, de a interconecta strategia de securitate cu cea de dezvoltare, pentru că aceasta comportă o accepţiune mai extinsă, receptivă şi evoluţionistă a surselor de insecuritate, natura ameninţării contemporane şi vulnerabilităţii, precum şi modalităţile adecvate de limitare a acestora.

Dezvoltarea durabilă nu va fi întotdeauna strategia preferată a specialiştilor în domeniul securităţii, însă va fi întotdeauna considerată o parte integrantă a unui repertoriu de strategii utilizate cu scopul de a spori securitatea, pe termen lung, la nivel individual şi de grup. Însă, pentru a obţine acest rezultat, comunitatea statelor dezvoltate trebuie să devină receptivă la limbajul securităţii umane şi mai conştientă de preocupările sale şi măsura în care acestea sunt împărtăşite.

I. 2. Mediul înconjurător şi conflictele

Discuţiile generale privind natura securităţii şi contribuţia degradării mediului la generarea insecurităţii şi conflictelor sunt caracterizate de către Levy (1995) drept primul val al cercetării asupra mediului înconjurător şi conflictelor. Cercetarea empirică ce a încercat să demonstreze existenţa unei legături între mediul înconjurător şi conflict a fost denumită de Levy al doilea val de studii privind mediul şi conflictele. Cel de-al doilea val de cercetare privind mediul şi conflictele nu este nici pe departe complet, definitiv sau lipsit de critici. Totuşi, în urma acestuia a rezultat un set de afirmaţii cauzale ce oferă un punct de plecare pentru dezbaterea potenţialului rol al mediului şi stresului demografic în generarea conflictului. Aceste afirmaţii permit, de asemenea, alte discuţii privind formularea strategiilor anticipative care includ legăturile dintre mediul înconjurător şi conflict, furnizând o bază pentru continuarea investigaţiilor asupra legăturilor complexe şi totuşi puţin înţelese dintre acestea.

Este important să facem o distincție între termenii conflict şi securitate. Conflictul, şi în special conflictul violent, este un fenomen empiric şi observabil. Securitatea, pe de altă parte, reprezintă o percepție subiectivă, construită pe rațiuni sociale, care evoluează şi depinde în mare măsură de perspectiva entității (individ, grup, stat, de tip internațional sau transnațional) care este protejată şi/sau asigură securitatea. Conflictul este o condiție considerată, în mod curent, o amenințare la adresa securității. Deşi adesea analizați împreună, aceşti termeni nu ar trebui considerați sinonimi.

Se pare că o serie de amenințări asupra mediului pot contribui la crearea unui climat de insecuritate, putând genera, de asemenea, conflicte. Constrângerile privind resursele reprezintă un factor crucial care este, adeseori, discutat în literatura de specialitate (Choucri, 1991). Industrializarea rapidă şi creşterea populației în multe regiuni au contribuit la o cerere masivă atât în ceea ce priveşte resursele naturale organice, cât şi cele alternative şi, aşa cum Ullman (1983) şi alți cercetători au observat, competiția pentru resurse a reprezentat, de-a lungul timpului, o cauză majoră a conflictelor. Intuitiv, această simplă afirmație pare rezonabilă, totuşi există unele voci care consideră că aceasta supralicitează importanța resurselor şi a mediului ca factori determinanți ai conflictului (Lipschutz, 1995).

Alți câțiva autori au încercat să clarifice posibilele legături dintre mediu şi conflict sau securitate. Wallensteen (1992), de exemplu, propune o clasificare pe şapte niveluri a legăturii dintre distrugerea mediului înconjurător şi conflict şi/sau securitate. Deşi nu oferă exemple pentru a-şi susține tipologia, sistemul său de clasificare este următorul:

- distrugerea mediului înconjurător conduce la diminuarea resurselor aflate la dispoziția societății, având drept consecință intensificarea disputelor la nivelul societății, în ansamblu;
- distrugerea mediului înconjurător conduce la un transfer de putere între partidele deja constituite;
- distrugerea mediului înconjurător conduce la formarea de noi partide, ca reacție la distrugerea mediului înconjurător;
- distrugerea mediului înconjurător conduce la creşterea importanței acordate de partidele deja constituite problemelor privind mediul înconjurător;
- distrugerea mediului înconjurător conduce la acordarea unei atenții primordiale problemelor privind mediul înconjurător la nivelul afacerilor politice, spre deosebire de alte probleme cu care se confruntă societatea;

- distrugerea mediului înconjurător conduce la un comportament conflictual implicând grupuri de protecție a mediului înconjurător;
- distrugerea mediului înconjurător conduce la un comportament conflictual generat de probleme legate de mediul înconjurător, implicând grupuri de protecție a mediului înconjurător.

Cu toate acestea, cercetările de mai sus şi afirmațiile generale ne conduc la o concluzie inevitabilă: schimbarea climatică (şi alte ameninţări neconvenționale) este asociată cu insecuritatea prin situațiile de inegalitate şi sărăcie. Relația mediu înconjurător-securitate este doar unul dintre exemplele privind modul în care diferiți factori sau ameninţări sunt asociate cu particularități structurale ale inegalității şi sărăciei.

Conflictul poate fi generat de accesul la resurse naturale inepuizabile, precum apa, terenul arabil, pădurile, amenajările piscicole. Acest lucru poate fi rezultatul limitării rezervelor (epuizarea sau degradarea resurselor naturale), creşterii nesustenabile a cererii (datorată presiunilor populației sau creşterii consumului pe cap de locuitor, adesea asociată modelelor economice bazate pe export), inegalităților distributive sau al unei combinații între aceşti factori. Statele în curs de dezvoltare, în special cele ale căror economii sunt axate, în principal, pe agricultură şi alte sectoare care depind direct de starea bună a resurselor naturale, sunt afectate direct de problemele mediului înconjurător. În aceste cazuri, nevoile şi interesele grupurilor rivale, strâns legate de terenuri – agricultorii, păstorii nomazi, fermierii şi exploatatorii de resurse –, sunt adesea incompatibile.

Conceptul de securitate a mediului nu ar trebui echivalat cu argumentul potrivit căruia schimbarea climatică este singurul factor declanşator de conflicte sau alte probleme de securitate – nici măcar cu cel potrivit căruia schimbarea climatică este, în mod necesar, un mecanism direct de declanşare a conflictelor. Nu există, probabil, niciun conflict la nivel mondial care să poată fi considerat monocauzal.

Cauzele conflictelor şi insecurității sunt multiple, complexe şi bine integrate. În consecință, este extrem de dificil de realizat o distincție între rolul degradării mediului înconjurător şi epuizarea resurselor, drept factori responsabili şi cauze ale conflictului sau insecurității. Dovezile sugerează faptul că mediul înconjurător joacă un rol relativ minor în declanşarea directă a conflictelor violente. Cu toate acestea, unele dovezi indică, de asemenea, că variabilele legate de mediul înconjurător pot avea o contribuție indirectă, subiacentă, la declanşarea conflictelor, din cauza impactului lor

negativ asupra altor factori care pot provoca, în mod direct, conflicte violente. Este din ce în ce mai evident faptul că degradarea mediului înconjurător şi epuizarea resurselor joacă un rol important în generarea şi exacerbarea insecurităţii umane.

Această contribuţie a mediului înconjurător devine relevantă în special atunci când transferăm coordonatele de referinţă de la nivel naţional la un nivel inferior, de comunitate, sau la un nivel superior, internaţional.

I. 3. Mediul înconjurător şi securitatea

Care este legătura dintre mediul înconjurător şi securitate? La nivel internaţional s-a ajuns la un consens asupra faptului că degradarea mediului înconjurător, accesul inechitabil la resurse vitale, de care oamenii depind pentru a-şi satisface nevoile fundamentale, şi competiţia în vederea exploatării şi preluării controlului asupra bunurilor valoroase pot reprezenta, fiecare în parte, potenţiali factori favorizanţi ai conflictelor, care reduc capacităţile statelor de a gestiona situaţiile de criză. Aceşti factori pot, în multe situaţii, declanşa sau alimenta violenţele, sporind vulnerabilitatea în faţa dezastrelor naturale. Însă, cooperarea pe probleme privind mediul înconjurător poate reprezenta un instrument eficient în prevenirea conflictelor, contribuind la consolidarea încrederii reciproce şi promovând bune relaţii de vecinătate, inclusiv modele de cooperare şi conlucrare care pot fi, ulterior, extinse şi la nivelul altor regiuni.

Există mulţi factori de mediu care contribuie la insecuritate. Calamităţile naturale, precum cutremurele, erupţiile vulcanice, inundaţiile şi seceta, au fost întotdeauna considerate o ameninţare la adresa existenţei umane, iar impactul acestora la nivel uman a crescut considerabil, în contextul în care oamenii locuiesc în regiuni predispuse la dezastre. Ritmul altor forme de degradare a mediului înconjurător, provocate de activitatea umană, şi de epuizare a resurselor (de exemplu, despădurirea, deşertificarea, degradarea pământului, eroziunea, salinizarea, depunerea de aluviuni, schimbarea climei), deşi, adesea, progresiv, a crescut rapid în ultimele decenii din cauza unei combinaţii între creşterea cererii, perfecţionarea mijloacelor tehnologice de exploatare şi ritmul lent al conservării şi controlului. În acelaşi timp, capacitatea şi, poate, dispoziţia oamenilor de a se adapta la stresul mediului înconjurător sunt supuse unor provocări crescânde, în special în zonele în care resursele şi mediul înconjurător furnizează principalele mijloace de existenţă, aşa cum este cazul majorităţii statelor în curs de dezvoltare.

Eforturile de reducere a riscurilor ridicate de epuizarea resurselor, inechitate şi injustiţie pot aduce beneficii atât biosferei, cât şi oamenilor. Cooperarea în vederea realizării unui management sustenabil şi echitabil al resurselor naturale trebuie să consolideze coeziunea socială, creând punţi peste frontierele culturale şi politice şi reducând vulnerabilitatea în faţa crizelor. Într-adevăr, asigurarea unui mediu de securitate, în care oamenii îşi pot manifesta propriile opţiuni de dezvoltare în siguranţă şi libertate, reprezintă o precondiţie esenţială a sustenabilităţii.

De la sfârşitul anilor ’70 şi începutul anilor ’80 au existat discuţii permanente privind conexiunile dintre mediul înconjurător, resurse, securitate, conflicte şi instaurarea păcii. La sfârşitul anilor ’90, problemele privind mediul înconjurător au început să îşi facă loc pe agenda politicii externe şi de securitate. Ulterior, au apărut noi dificultăţi ca urmare a atacurilor de la 11 septembrie 2001. În Statele Unite, unde factorii de decizie politică au început să adopte noţiuni de securitate a mediului înconjurător în anii ’90, „războiul împotriva terorismului” a ajuns în centrul atenţiei, stopând, în mare parte, aceste eforturi.

Diverşi autori şi-au concentrat atenţia asupra unor aspecte diferite privind ansamblul conexiunilor. Unii au avut o abordare destul de limitată (rezumându-se, de exemplu, la legăturile dintre mediul înconjurător şi incidenţa conflictelor violente); alţii şi-au stabilit limite mai vaste (adoptând, de exemplu, o abordare comprehensivă asupra mediului înconjurător şi securităţii). Unele lucrări s-au concentrat asupra impactului schimbărilor climatice asupra securităţii naţionale a anumitor state, în timp ce alţii şi-au concentrat eforturile în principal asupra consecinţelor acestora la nivelul securităţii globale.[4]

Securitatea naţională vizează, în mod tradiţional, protejarea integrităţii teritoriale şi a suveranităţii politice a statului împotriva agresiunii militare a altor state. Acest lucru a condus, în general, la crearea de alianţe şi realizarea de investiţii militare, în scopul descurajării potenţialilor inamici şi al utilizării eficiente a forţei, atunci când era cazul.

În ultimii ani, s-a acordat o mare importanţă extinderii concepţiei tradiţionale de securitate în vederea includerii aşa-ziselor ameninţări neconvenţionale, precum epuizarea resurselor, abuzurile împotriva

[4] Michael Renner, *Inventory of Environment and Security Policies and Practices, - Introduction to the Concepts of Environmental Security and Environmental Conflict*, Institute for Environmental Security, 2006.

drepturilor omului, epidemiile şi degradarea mediului înconjurător provocată de contaminări cu substanţe toxice, subţierea stratului de ozon, încălzirea globală, poluarea apelor, deteriorarea solului şi diminuarea biodiversităţii. Aceste efecte devin motive de îngrijorare pe linie de securitate la nivel naţional atunci când sunt asociate cu o densitate mare a populaţiei sau cu un nivel ridicat de urbanizare, presiuni socioeconomice, structuri guvernamentale vulnerabile şi tensiuni între comunităţi ori dispute transfrontaliere.

În următoarele decenii vom asista la o diminuare drastică a resurselor, la o mai mare degradare a mediului înconjurător şi la o schimbare climatică pronunţată. De fapt, într-o lume din ce în ce mai nesigură, aceste trenduri sunt extrem de previzibile. Problemele de securitate, în care resursele şi factorii de mediu joacă roluri-cheie, sunt subiecte incluse pe agenda zilnică de politică externă. Potrivit estimărilor Băncii Mondiale, în ultimii 40 de ani statele în curs de dezvoltare care nu beneficiază de resurse naturale majore au înregistrat ritmuri de creştere de 2-3 ori mai rapide decât cele care deţin rezerve importante. Alocarea pe criterii politice a veniturilor rezultate din exploatarea resurselor naturale, ţinându-se cont de aspecte etnice, religioase şi regionale, a reprezentat o forţă motrice a conflictelor interne. Veniturile provenite din exploatarea resurselor naturale alimentează corupţia şi crima organizată, care destabilizează guvernele, iar în cele mai grave cazuri finanţează conflictele şi furnizează o infrastructură logistică pentru terorismul internaţional.

Europa de Sud-Est se confruntă, în principal, cu problemele reprezentate de poluarea industrială masivă în zonele urban-industriale, de agricultura intensivă, de lipsa unei tehnologii şi infrastructuri a apei şi de poluarea industrială cauzată de sectorul minier.

Eforturile transfrontaliere vizând protecţia mediului şi cooperarea regională pe probleme privind mediul înconjurător sunt importante, în contextul în care multe resurse naturale sunt vizate de mai multe state, iar degradarea mediului nu cunoaşte frontiere. Dincolo de efectele directe ale războiului împotriva poluării industriale cauzate de deversări şi distrugerea infrastructurii, contaminarea apei şi solului este, de asemenea, un rezultat al procesului de industrializare masivă derulat anterior conflictelor, precum şi al deficienţelor existente la nivelul procesului de tratare a apei şi al managementului şi depozitării deşeurilor solide şi periculoase.

Regiuni extinse din Europa de Sud-Est sunt puternic industrializate, însă măsurile de protecţie a mediului înconjurător sunt deficitare, având

drept consecință o gravă deteriorare a mediului înconjurător şi un impact negativ asupra sănătății. Poluarea aerului şi degradarea solului, ca urmare, în special, a industriei chimice şi mineritului, producției de ciment şi fertilizatori, au provocat daune majore asupra sistemului ecologic, având consecințe negative şi asupra sănătății oamenilor care locuiesc în zonele periculoase. Punctele importante de mare concentrare industrială din apropierea zonelor urbane reprezintă amenințări grave la adresa sănătății. În multe regiuni, producția agricolă este, de asemenea, caracterizată de practici ineficiente, existând o cerere ridicată de apă şi utilizându-se fertilizatori în exces. Rezervele de apă potabilă sunt amenințate de lipsa resurselor de apă şi de calitatea inferioară a apei, provocată, adesea, de deversarea apei uzate.

Cursurile de apă au fost grav contaminate în urma deversărilor poluante de substanțe periculoase provenind din uzinele industriale. Cu toate acestea, în multe cazuri, distrugerea instalațiilor industriale în timpul conflictelor a avut, de asemenea, efecte pozitive temporare asupra mediului înconjurător, reducând semnificativ poluarea aerului şi apei cauzată de ramurile industriale în regres şi/sau învechite. Sistemele de management al apei din regiune sunt afectate de structurile instituționale vulnerabile şi de deficiențele de administrare, de ineficiența în operare, lipsa planificării sau chiar a viabilității financiare. Managementul centralelor de energie nucleară şi securitatea nucleară reprezintă un motiv serios de îngrijorare la nivel regional din cauza potențialelor sale efecte transfrontaliere.

În vederea soluționării aspectelor socioeconomice ale problemelor legate de mediul înconjurător, în special a celor privind deficitul de resurse sau presiunile exercitate asupra resurselor, migrația şi tensiunile sociale, este necesară elaborarea unor modalități integrate de abordare. Aceste abordări trebuie să ia în considerare dimensiunea politică, economică, socială şi de mediu.

Cel puțin o parte a confuziei create în jurul identificării legăturilor dintre mediul înconjurător şi securitate este rezultatul diferitelor interpretări la nivel instituțional ale termenilor mediu înconjurător şi securitate. În prezent, aceste interpretări includ următoarele:

- securitatea mediului (sau securitatea beneficiilor oferite de mediul înconjurător) a fost, de asemenea, interpretată drept capital natural inepuizabil; include: instituțiile militare şi de informații care monitorizează şi aplică acordurile internaționale privind protecția mediului înconjurător; colectarea, analiza şi diseminarea datelor ştiințifice privind mediul înconjurător; acțiuni în vederea reducerii

efectelor crizelor şi dezastrelor naturale; implementarea programelor de dezvoltare sustenabilă a mediului; garantarea accesului la resurse naturale; dezvoltarea tehnologiilor de depoluare a mediului înconjurător; şi protecţia parcurilor şi rezervaţiilor naturale;
- degradarea sau epuizarea resurselor mediului înconjurător generate de pregătirile militare pentru un conflict armat, de modalitatea de derulare a conflictului armat şi de deversarea rezidurilor militare;
- degradarea mediului înconjurător şi epuizarea resurselor drept cauze potenţiale ale conflictelor violente;
- încălcarea la nivel instituţional a principiului suveranităţii în vederea diminuării degradării mediului înconjurător;
- degradarea mediului înconjurător şi epuizarea resurselor drept ameninţări la adresa prosperităţii naţionale (şi, în consecinţă, a securităţii naţionale);
- un concept comprehensiv privind mediul înconjurător inclus într-o serie de factori care afectează securitatea umană.[5]

II. Mediul înconjurător şi politicile de securitate

Legătura dintre mediul înconjurător, securitate şi dezvoltare a fost evidenţiată, în premieră, de către regretatul premier suedez Olof Palme, în cadrul Comisiei Naţiunilor Unite pentru Dezarmare şi Securitate. Palme a lansat un apel la adresa statelor membre în vederea redefinirii securităţii, incluzând atât securitatea colectivă (conceptul tradiţional şi militar de securitate) cât şi securitatea comună, care reflecta un concept mai vast de securitate, cuprinzând transformarea economică, degradarea mediului înconjurător şi epuizarea resurselor naturale printre factorii cauzali. Conceptul de securitate comună a evoluat, transformându-se în ceea ce majoritatea guvernelor numesc astăzi securitate comprehensivă.

II. 1. Modalitatea în care guvernele abordează conceptul de securitate a mediului

Unul dintre cele mai importante procese interguvernamentale care a influenţat modul în care guvernele abordează securitatea mediului înconjurător este raportul elaborat în anul 2004 de către Comisia la Nivel Înalt pe probleme privind Ameninţările, Provocările şi Schimbările,

[5] „Environment and Security, Transforming Risks into Cooperation, Environmental Risks in South Eastern Europe", UNEP, UNDP, OSCE, 2003.

constituită de Secretarul General al ONU. Beneficiind de susținerea multor guverne cu prilejul Summitului de Bilanț al Mileniului, din anul 2005, Comisia la Nivel Înalt defineşte o nouă viziune a securității colective, abordând şase tipuri de amenințări, care trebuie să reprezinte motive de preocupare la nivel mondial, atât în prezent, cât şi în deceniile care vor urma. Acestea includ:

- război între state;
- violență în interiorul statelor;
- sărăcie, boli infecțioase şi degradarea mediului;
- arme nucleare, radiologice, chimice şi biologice;
- terorism;
- crima organizată transnațională.

Comisia susține că aceste amenințări la adresa securității umane nu țin cont de frontiere naționale, iar, în lumina interconexiunilor lor intrinsece, acestea trebuie să fie soluționate la nivel internațional, regional sau național. În ceea ce priveşte dimensiunea securității mediului raportată la ansamblul noilor amenințări, raportul Comisiei la Nivel Înalt subliniază faptul că 90% dintre conflictele actuale au izbucnit în 30% dintre cele mai sărace țări, acestea confruntându-se cu cele mai mari provocări la adresa mediului înconjurător. De asemenea, raportul precizează că preocupările legate de mediu sunt de puține ori luate în calcul în cadrul strategiilor de securitate, de dezvoltare sau umanitare. Drept rezultat, Comisia susține că mecanismul de luare a deciziilor este fragmentat la toate nivelurile guvernării.

Acest lucru este destul de evident şi în modul incoerent în care guvernele naționale s-au organizat pentru a soluționa amenințările care nu mai pot fi considerate de sine-stătătoare, ci fenomene strâns interconectate. Într-adevăr, relevanța mediului în cadrul strategiei de securitate a fost reiterată în cadrul raportului Secretarului General al ONU, prezentat cu prilejul Summitului Mondial din anul 2005. Secretarul General a relaționat, în mod explicit, succesul în cadrul procesului de dezvoltarea umană şi asigurare a securității cu utilizarea sustenabilă a resurselor umane.

Pentru multe guverne, conceptul de securitate comprehensivă include nu numai probleme de securitate militară, ci şi factori care se raportează în special la securitatea umană şi la sănătatea mediului în care

trăiesc. Dihotomia ce caracterizează abordarea convențională a securității de cea comprehensivă este similară cu distincția adeseori făcută între puterea militară şi cea diplomatică, în contextul în care puterea militară denotă utilizarea forței, iar cea din urmă se referă la instrumente precum comerțul, asistența şi alte metode diplomatice de îndeplinire a scopurilor politice.

Scopurile securității nu numai că se raportează tot mai mult la controlul armelor şi dezarmare, ci sunt însoțite şi de eforturi de consolidare a păcii şi de dezvoltare a securității umane şi a sistemului ecologic.

Se pot trage deja câteva concluzii din abordările prezentate anterior referitoare la faptul că guvernele întreprind eforturi pentru a face față scenariilor privind amenințările emergente:

- În primul rând, este important să ne asigurăm de faptul că o întreagă serie de instrumente, structuri şi expertize la toate nivelurile guvernării sunt dispuse să gestioneze noua generație de amenințări la adresa securității. Rolul guvernelor locale, al societății civile şi sectorului privat este deosebit de important. Parteneriatele relevante între principalele părți interesate, precum şi guvernele şi alte agenții internaționale trebuie să fie consolidate şi să beneficieze de resursele corespunzătoare.
- În al doilea rând, mai multe eforturi ar trebui direcționate în vederea înțelegerii mai aprofundate a acestor noi amenințări la adresa securității, acumulând expertiză şi capacitatea de a analiza problemele şi potențialele zone de criză.
- În al treilea rând, guvernele ar trebui să discearnă mai bine în ceea ce priveşte alegerea instrumentelor strategice atunci când se confruntă cu conflicte. Este larg acceptată ideea potrivit căreia trebuie utilizat un dozaj echilibrat între instrumentele diplomatice şi cele militare, în funcție de scenariul conflictului.
- În al patrulea rând, voința politică trebuie mobilizată într-un stadiu timpuriu pentru a intensifica prevenirea conflictelor armate, precum şi pentru a detecta şi contracara efectele calamităților naturale într-o fază incipientă.
- În al cincilea rând, eforturile internaționale de gestionare a crizelor trebuie îmbunătățite. În acest scop, este necesară optimizarea cooperării dintre actori civili şi militari în domeniu, precum şi o tranziție mai lină de la operațiuni de menținere a păcii la operațiuni de consolidare a păcii, de la

gestionarea situațiilor de urgență la reconstrucția pe termen lung în perioada postconflictuală.[6]

Conştientizarea crescândă, în ultimii ani, a conexiunilor dintre conflicte, climatul de pace, sărăcie şi mediul înconjurător au determinat guvernele să se concentreze tot mai mult asupra rolului pe care asistența pentru dezvoltare îl poate juca atât în ameliorarea, cât şi în exacerbarea cauzelor fundamentale ale conflictelor violente.

Drept recunoaştere a eficienței limitate pe care au avut-o instrumentele tradiționale de politică externă în soluționarea conflictelor legate de mediu, o serie de guverne, instituții multilaterale şi ONG-uri au abordat tot mai mult problema prevenirii conflictelor la nivelul instrumentelor de evaluare a dezvoltării. Mai precis, aceştia au început să integreze în programele de asistență obiectivele de prevenire a conflictelor, inclusiv abordări precum instrumente de evaluare a impactului păcii şi conflictelor, creând departamente de avertizare timpurie şi capacități de reconstrucție în perioada postconflictuală şi dezvoltând rețele de prevenire a conflictelor.

II. 2. Riscuri la adresa mediului şi securității; evaluarea şi gestionarea necesităților

Recent, Departamentul de Reconstrucție şi Prevenire a Conflictelor (CPR) din cadrul Băncii Mondiale a însărcinat Comisia olandeză de Evaluare a Mediului să elaboreze instrucțiuni privind posibilele abordări ale Evaluării Strategice privind Impactului asupra Mediului (SEA) în țările afectate de conflict.

Au fost identificate trei precondiții necesare asigurării succesului acțiunilor întreprinse de SEA în zonele de conflict. În primul rând, trebuie să existe posibilitatea de a concretiza problemele legate de mediu printr-o decizie strategică ce poate fi implementată. În al doilea rând, toate părțile interesate să fie dispuse să participe la proces, manifestând încredere în acesta. În al treilea rând, implicarea unor parteneri importanți nu trebuie să reprezinte un risc, în special în situațiile postconflictuale, când este posibil ca instituțiile de asigurare a păcii şi securității să nu poată funcționa la

[6] Johannah Bernstein, *Inventory of Environment and Security Policies and Practices – How Governments Appproach the Concept of Environmental Security*, Institute for Environmental Security, 2006.

capacitatea maximă. Raportul Comisiei olandeze sublinia, de asemenea, următoarele elemente care ar trebui incluse într-o evaluare strategică asupra zonelor cu risc crescut de conflict:

- analiza conflictelor care reliefează factorii declanşatori şi motivaţionali ai conflictului ce identifică elementele cheie în procesul de instaurare a climatului de pace;
- analiza părţilor interesate ce evidenţiază poziţiile, interesele şi valorile acestora;
- identificarea locaţiei şi sincronizarea acţiunilor-cheie în vederea prevenirii conflictului;
- evaluarea contextului politic şi militar;
- evaluarea problemelor economico-sociale-cheie.

Concluzii rezultate în urma evaluării conflictelor:

- agenţiile trebuie să se asigure că structurarea şi implementarea procesului de evaluare a conflictelor sunt realizate prin colaborarea deplină atât a actorilor statali, cât şi a celor nestatali; trebuie să se întreprindă mai multe eforturi pentru a îmbunătăţi capacitatea de analizare a conflictelor în cadrul organizaţiilor societăţii civile;
- agenţiile trebuie să depună mai multe eforturi pentru a se asigura că procesul de evaluare a conflictelor este bine integrat în programul de dezvoltare;
- experienţa în domeniul evaluării vulnerabilităţilor a relevat că trebuie întreprinse mai multe eforturi pentru soluţionarea interacţiunii dintre sistemul uman şi cel ecologic;
- experienţa în domeniul evaluării vulnerabilităţilor a reliefat că un număr redus de abordări tratează solicitările multiple şi că indicatorii şi indicii care sunt utilizaţi nu au legătură cu un cadru conceptual fundamental clar;
- o provocare majoră constă în abordarea aşa-numitei „unităţi expuse" ca şi sistem socioecologic integrat şi identificarea interacţiunilor care pot genera conflicte;
- de asemenea, evaluările vulnerabilităţilor tind să furnizeze imagini ale situaţiilor existente la un anumit moment, fără a oferi detalii precise privind riscul cumulativ şi factorii de vulnerabilitate;

• experţii susţin, de asemenea, că interacţiunile la diverse niveluri şi legăturile geografice trebuie mai bine surprinse şi evaluate.[7]

II. 3. Politici de dezvoltare şi practici la nivelul NATO şi UE

Timp de mai mulţi ani, NATO, şi în special Comisia privind Provocările la adresa Societăţii Moderne (CCMS), a fost implicată în activităţi pe probleme de mediu şi securitate. Recent, Comisia pentru Ştiinţă şi CCMS au convenit asupra efectuării unei restructurări. „Ştiinţă pentru Pace şi Securitate" (SPS) este denumirea atât a noii Comisii unice create în urma restructurării, cât şi a noului program rezultat din emergenţa unor priorităţi comune Programului NATO de Securitate prin Ştiinţă şi activităţilor CCMS, ca urmare a schimbărilor rapide la nivelul climatului global de securitate.

CCMS a fost implicată în numeroase studii şi proiecte legate de securitatea mediului:

- Evaluarea Calamităţilor Naturale;
- Proiectul Sistemului de Monitorizare a Bazinului Mării Caspice;
- Strategii Eficiente de Reacţie în Situaţii de Criză;
- Mecanismul de Luare a Deciziilor privind Mediul Înconjurător din Zona Asiei Centrale;
- Educaţia privind Protecţia Mediului la Nivelul Forţelor Armate;
- Perfecţionarea Prognozelor Meteo;
- Securitatea Căilor Navigabile Înguste.

Printre subiectele abordate recent se numără:

- Evaluarea Incidenţei Cazurilor de Cancer;
- Plan de Reducere a Poluării Aerului şi aplicarea sa;
- Produse şi Procese Ecologice;
- Protecţia Ecosistemelor Lagunelor;
- Terorism Ecologic;
- Sisteme de Gestionare a Problemelor privind Mediul în Sectorul Militar;
- Securitatea Lanţului Alimentar;

[7] Verheem Rob, et al. "Strategic Environmental Assessments: Capacity Building in Conflict-Affected Countries", Report prepared by the Netherlands Commission for Environmental Assessment for the Conflict Prevention and Reconstruction United in the Social Development Department of the Environmentally and Socially Sustainable Development Network of the World Bank, 2005.

- Gestionarea Integrată a Apelor;
- Rolul Ştiinţei Peisagistice în Evaluarea Mediului;
- Gestionarea Deşeurilor Industriale şi Toxice;
- Probleme privind Prevenirea şi Remedierea;
- Evaluarea Riscurilor generate de Accidentul de la Cernobîl;
- Consolidarea Infrastructurii Militare.

Iniţiativele recente ale NATO s-au axat pe:

- Comisia NATO pentru Ştiinţă;
- Securitatea prin Programul de Ştiinţă;
- Programul NATO Parteneriat pentru Pace;
- Răspuns NATO în caz de Calamitate;
- Cooperarea NATO cu ENVSEC (Environment and Security).[8]

Abordarea europeană privind securitatea a evoluat considerabil în ultimii ani. În timp ce esenţa politicii europene de securitate este fundamentată în Politica Externă şi de Securitate Comună, UE promovează activ soluţionarea problemelor de securitate prin intermediul „strategiilor diplomatice". Într-adevăr, diferitele politici şi strategii europene în domeniul mediului, în sfera dezvoltării şi securităţii reflectă un angajament ferm faţă de conceptul securităţii multidimensionale şi comprehensive.

Există o legătură indisolubilă între politicile externe şi de securitate ale UE, precum şi strategiile privind mediul şi dezvoltarea, în efortul de a sublinia şi legăturile potenţiale sau deja existente în cadrul relaţiilor externe ale UE la nivelul acestor domenii.

Potrivit Tratatului Uniunii Europene, obiectivul PESC este acela de a „menţine pacea şi de a consolida securitatea internaţională, în conformitate cu principiile Cartei ONU, precum şi cu principiile Documentului Final de la Helsinki şi obiectivele Cartei de la Paris, pentru a promova cooperarea internaţională." PESC are cinci obiective principale:

- protejarea valorilor comune, intereselor fundamentale, independenţei şi integrităţii Uniunii;
- consolidarea securităţii Uniunii la toate nivelurile;
- menţinerea climatului de pace şi consolidarea securităţii internaţionale;

[8] Catalogul complet al publicaţiilor CCMS este disponibil la: http://www.nato.int/ccms/publi.htm.

- promovarea cooperării internaţionale;
- dezvoltarea şi consolidarea democraţiei şi a statului de drept, respectarea drepturilor omului şi a libertăţilor fundamentale.

Strategia Europeană de Securitate a fost aprobată de Consiliul European organizat la Bruxelles, la data de 12.12.2003, şi elaborată sub îndrumarea Înaltului Reprezentant european Javier Solana. Strategia Europeană de Securitate este documentul care direcţionează strategia UE de securitate internaţională. Acesta abordează necesitatea unei strategii de securitate comprehensive care cuprinde atât măsurile de securitate civile, cât şi cele de apărare. Strategia în sine nu este un document operaţional cu un plan de acţiune detaliat.

Acesta mai degrabă formulează obiectivele generale ale acţiunilor externe ale UE şi principalele modalităţi de realizare a acestora. Prin apariţia Strategiei, Europa a formulat pentru prima dată o strategie de securitate comună.

Strategia Europeană de Securitate cuprinde o serie de referinţe care creează o legătură între securitate, dezvoltare şi mediu, printre care şi declaraţia potrivit căreia „Securitatea este o precondiţie a dezvoltării. Conflictele nu numai că distrug infrastructura, inclusiv infrastructura socială, ci încurajează şi criminalitatea, descurajează investiţiile şi creează un climat impropriu derulării activităţilor economice. O serie de state şi regiuni sunt prinse într-un proces ciclic de conflicte, insecuritate şi pauperitate. Concurenţa pentru resursele naturale – în special apă – care se va agrava în contextul încălzirii globale în următoarele decenii, este posibil să conducă la tensiuni suplimentare şi la migraţia populaţiei în diferite regiuni."

Potrivit Strategiei, „dezvoltarea unei societăţi internaţionale mai puternice, a unor instituţii internaţionale eficiente şi a unei ordini internaţionale bazate pe respectarea normelor" reprezintă unul dintre obiectivele strategice ale politicii europene de securitate. Preocupările şi obiectivele legate de mediu şi dezvoltare capătă o pondere tot mai mare la nivelul politicii externe şi de securitate a UE, însă, recent, politicile, programele şi proiectele europene privind mediul şi dezvoltarea s-au axat pe preocupările şi obiectivele legate de securitate. Următoarele exemple sunt, probabil, elocvente în acest sens:

- Procesul Kimberley;
- Iniţiativa UE privind apa;
- Planul de acţiune UE referitor la aplicarea reglementărilor forestiere, guvernare şi schimburile comerciale;
- Iniţiativa UE în domeniul energiei pentru eradicarea sărăciei şi dezvoltarea durabilă;

➢ Monitorizarea globală pentru mediu şi securitate (GMES);

➢ Integrarea problemelor privind mediul înconjurător în cooperarea CE în domeniul dezvoltării;

➢ Reţeaua europeană de diplomaţie ecologică – Integrarea mediului înconjurător în politica externă.

Protecţia mediului, utilizarea prudentă şi gestionarea adecvată a resurselor naturale nu sunt singurele valori de sine stătătoare care sunt promovate. Adesea poate exista o puternică relaţie cauză-efect între utilizarea şi gestionarea resurselor naturale, şi situaţia socioeconomică şi chiar politică, inclusiv cea de securitate, dintr-o ţară sau regiune. Degradarea resurselor naturale, ce poate fi exacerbată prin utilizarea lor nesustenabilă, epuizarea lor sau, dimpotrivă, abundenţa şi competiţia pentru preluarea controlului asupra acestora sunt printre cele mai cunoscute conexiuni.

Efecte posibile ale schimbărilor climei asupra ecosistemelor, mijloacelor de trai şi dezvoltării economice necesită, de asemenea, o atenţie sporită în contextul analizării situaţiei resurselor naturale din perspectiva unui potenţial conflict. Nu ar trebui neglijată nici dinamica conflictelor care conduce la continuarea degradării mediului. Aceasta poate fi o consecinţă directă a activităţilor militare sau, de exemplu, a influxurilor masive de refugiaţi şi a impactului acestora la nivel ecologic sau a utilizării imprudente a resurselor naturale pentru reconstrucţie etc. Dimpotrivă, colaborarea în vederea gestionării resurselor comune poate contribui la consolidarea încrederii reciproce şi a relaţiilor paşnice.

În cazul terenurilor şi al apei, problemele legate de calitate şi disponibilitate sunt vitale. Cauzele care stau la baza limitării sau diminuării resurselor pot fi variate: deficitul concret, distribuirea inechitabilă, accesul nereglementat sau drepturile de posesiune, deficienţele instituţionale sau ale infrastructurii, cererile sporite generate de presiunile demografice etc. Accesul populaţiei sărace din mediul rural şi urban la resurse necesită o atenţie deosebită, iar, în multe cazuri, principiul de egalitate a sexelor şi oportunităţilor este, de asemenea, relevant.

Strategia de răspuns în vederea prevenirii conflictelor trebuie să aplice acţiuni similare atât pe plan local, cât şi regional. Acestea cuprind, în mod tradiţional, instituţionalizarea procedurilor de luare a deciziilor, consolidarea unei abordări participative la scară largă, cu accent pe reprezentarea grupurilor vulnerabile şi abilitarea părţilor interesate la nivel local, promovarea dialogului şi a schimbului de informaţii.[9]

[9] EC Study on Inter-linkages between Natural Resources Management and Conflict, 2006.

Bibliografie

1. *Common Security, Uncommon Challenges: Managing Risks in an Age of the Unthinkable*, Carol Dumaine, Geneva, Switzerland, Global Energy & Environment Strategic Ecosystem, US Department Energy, May 2009.

2. *Enabling Strategic Intelligence on Energy and Environmental Security Impacts and Consequences*, International Design Team Meeting, Scotland, 2007.

3. *Environmental security, abrupt climate change and strategic intelligence,* Chad Michael Briggs, Global Energy & Environment Strategic Ecosystem, US Department Energy, February 2009.

4. *Energy and Environmental Insecurity - Global strategic assessment 2009*, Institute for National Strategic Studies.

5. *Environment and Security, Transforming Risks into Cooperation, Environmental risks in South Eastern Europe*, ENVSEC Cooperation, 2006.

6. *Energy & Environmental Risks: Defining Security and Vulnerability,* Institute for Environmental Security, 2009.

7. *Environment and Security Policy*, International Institute for Sustainable Development, 2009.

8. *Inventory of Environment and Security Policies and Practices*, Institute for Environmental Security, 2007.

9. *Introduction to Strategic Intelligence Analysis*, Government Training Inc, 2009.

10. *State-of-the-Art Review On Environment, Security and Development Cooperation*, IUCN, The World Conservation Union, 2007.

11. *Meeting 21st Century Transnational Challenges: Building a Global Intelligence Paradigm*, Central Intelligence Agency, 2009.

12. *Scanning the Horizon on Food, Water, Energy, and the Environment*, Centre for Strategic and International Studies, 2009.

13. *Global monitoring for environment and security (GMES)*, Commission of The European Communities, 2008.

14. *The Intelligence Community's Neglect of Strategic Intelligence*, Central Intelligence Agency, 2009.

Ana Ligia LEAUA este asistent universitar în cadrul Academiei Naţionale de Informaţii *„Mihai Viteazul”*, absolventă a Facultăţii de Drept şi a cursurilor postuniversitare ale Colegiului Naţional de Apărare, Colegiului Superior de Securitate Naţională şi ale Institutului Diplomatic Român, a publicat articole şi studii pe teme specifice dimensiunii de mediu a securităţii naţionale, dezvoltării durabile şi relaţiilor internaţionale.

Intelligence – de la teorie către ştiinţă

Lector univ. dr. Ion IVAN
Academia Naţională de Informaţii *„Mihai Viteazul”*
e-mail: **ion_ivan@mymail.ro**

Abstract

Since intelligence helps to manage risk and uncertainty, provides forewarning and establishes conditions in which threats are eliminated or kept at a distance, the standard model of the relationship between intelligence analysis and decision-making needs to be permanently re-evaluated.

This paper aims to move the tradecraft of intelligence analysis closer to a science, therefore, it has identified some guidelines that can lead toward creation of a solid intelligence infrastructure and laid out in a clear and concise language. It represents a distillation and clarification of the intelligence principles, their theory and application.

As a discipline, intelligence seeks to remain an independent, objective advisor to the decision maker. Understanding each other's views on intelligence is the first step toward improving the relationship between them.

Keywords: theory of intelligence, knowledge intelligence, intelligence processes, principles of intelligence.

Aparent există o contradicţie între comunitatea academică şi cea din domeniul securităţii naţionale, prima caracterizată prin deschidere şi libertatea exprimării, iar cea de a doua prin secret şi mister. Totuşi, ambele sunt preocupate de respectarea principiilor democratice şi acurateţea informării, fie că este vorba de publicul larg sau de beneficiari anume desemnaţi, însă, cu privire la cerinţele de confidenţialitate şi păstrarea secretului, din punct de vedere practic, pentru serviciile de informaţii există necesitatea realizării unui compromis pentru a păstra un echilibru acceptabil într-o societate democratică.

Intelligence-ul este în mod direct asociat practicii politicilor care ţin de sectorul social al activităţilor secrete, implicit unor aspecte specifice de legalitate, moralitate şi responsabilitate, considerate factori esenţiali în cadrul dimensiunilor acestui concept.

Deopotrivă, transparența și responsabilitatea, precum și fenomenul deschiderii serviciilor de intelligence, din vechile și noile democrații, suprapuse tradițiilor secretului și opacității acestora, desemnează un spectru care presupune politici sigure, promovarea confidențialității, credibilității și acordului, în contextul angajamentelor publice nu numai la nivel guvernamental, dar și al celorlalte tipuri de organizații fie de afaceri, fie nonprofit.

1. Cunoașterea – fundamentul intelligence-ului

În prezent, datorită dezvoltării noilor tehnologii informaționale și de comunicare, există o cantitate enormă de informații și multe instrumente sofisticate pentru culegerea, procesarea și analizarea acestora.

Cu deosebire, intelligence-ul relevă un mod de cunoaștere particular în cadrul ierarhiei moderne care stă la baza managementului cunoștințelor și care începe cu datele, conduce la informații, apoi la cunoștințe și culminează cu înțelepciunea. Astfel, intelligence-ul este o chestiune de interpretare specifică numai ființei umane care poate transforma datele în informații, informațiile în cunoștințe și pe acestea din urmă în înțelepciune, fără a garanta obținerea acesteia, furnizând doar avantaje comparative.

Prin încărcătura majoră de idei, informații, cunoștințe, știință și înțelepciune, inteligența constituie factorul central, esențial, al punerii în mișcare și desfășurării proceselor adaptative la cotele de performanță și eficacitate într-un mediu dinamic și complex. În mod real, serviciile intelectuale constituie furnizorii și, în mare măsură, și principalii consumatori ai resurselor reprezentate de informație, cunoaștere, știință, înțelepciune, acestea detașându-se ca fiind cele mai avansate purtătoare ale factorului investițional material.

Procesul de evaluare a informațiilor în vederea obținerii de cunoștințe speciale, caracteristice intelligence-ului, este de natură foarte personală, întrucât implică, de obicei fără a fi explicite și evidente, credințele și sistemul de valori proprii analistului. Fiind o construcție a minții umane, el este, în mod clar, diferit de la o persoană la alta, chiar dacă sunt utilizate aceleași instrumente și tehnici de cunoaștere.

Prin cunoaștere o problemă complexă este rafinată și transformată, sub acțiunea unui set de metode specifice și a psihicului individual, într-un set de probleme simple interconectate într-o structură logică sub forma unor informații de bază și variabile, astfel încât să permită îndeplinirea sarcinilor și luarea deciziilor.

Dacă informația dintr-un sistem a fost văzută de Norbert Wiener[1] ca măsură a gradului de organizare a acestuia, comparativ cu entropia care măsoară gradul său de dezorganizare, atunci putem afirma că intelligence-ul reflectă conectarea informațiilor dintr-o structură de sisteme cu nivelul de relaționare al acestora.

În timp ce, uneori, informația poate fi inutilă sau chiar poate aduce mai multă incertitudine/nesiguranță, intelligence-ul – ca suport al deciziilor umane raționale – are, întotdeauna, rolul de a clarifica viziunea asupra realității şi de a determina, prin utilizarea unor reguli proprii, funcție de context, gradul de certitudine al informațiilor analizate.

De aceea, cunoaşterea reflectă nu doar însuşirea unor informații, ci şi capacitatea de a înțelege şi a folosi mecanismul producerii de noi informații folosindu-le pe cele deja existente, iar intelligence-ul conferă utilizatorului şi starea necesară pentru a reacționa funcție de relevanța acestora.

2. Ştiința intelligence-ului

Conceptul de intelligence este polisemic şi se bazează pe diferite definiții ale procesului care construieşte cunoştințe într-un act conştient de creație, colectare, analiză, interpretare şi modelare a informațiilor. Mai mult chiar, deopotrivă teoreticienii şi practicienii domeniului sunt de acord cu necesitatea continuării dezbaterii privind clarificarea definirii intelligence-ului.

De ce, totuşi, distingem între intelligence şi informație, cu atât mai mult cu cât ştiința informației este deja un domeniu bine definit şi mare parte a publicului poate considera că există semnul egal între informație şi intelligence. Ambele noțiuni definesc procesul şi rezultatul procesului în sine, însă intelligence-ul reflectă şi ceva în plus, care presupune conducerea, dirijarea operațională în mod discret sau secret, incluzând atât culegerea şi procesarea de informații cu scopul de a informa, dezinforma sau influența, cât şi protejarea ori ascunderea unor informații, precum şi manipularea şi transmiterea intenționată în mod acoperit de informații false ori falsificate pentru a facilita atingerea obiectivelor securității naționale.

Noțiunea de intelligence, definită ca un proces/produs care reflectă abilitatea/facilitatea aflată în legătură directă cu competența general cognitivă aplicabilă pentru rezolvarea problemelor, diferă de termenul de

[1] Wiener, Norbert, *Cybernetics: or Control and Communication in the Animal and the Machine*, second edition, Cambridge, MIT Technology Press, 1985 (first edition 1948), p. 11.

informație prin două caracteristici principale: *raritate* (furnizare limitată şi beneficiari selectați) şi *exclusivitate* (păstrarea controlului asupra difuzării).

Prin faptul că presupun păstrarea secretului, cele două caracteristici concură la obținerea avantajului competitiv. În plus, putem caracteriza intelligence-ul ca un mod secret de acțiune prin care beneficiarul/deținătorul este înzestrat cu capacitatea care îi permite înțelegerea sau modificarea comportamentului celorlalți.

Pentru identificarea diferitelor niveluri ale abordării teoretice a intelligence-ului propunem spre exemplificare câteva dintre conexiunile cu diferite ştiințe umane[2]:

• *comportamentul organizațional* – este în prezent foarte bine cercetat, soluționarea problemelor şi deciziilor fiind bine clarificate; referitor la intelligence-ul organizațional numeroase modele au fost elaborate pentru adecvarea resurselor, protejarea datelor, cunoaşterea impactului ierarhiei, studiul centralizării specializării etc., care cresc profund valoarea politicilor firmei/instituției;

• *antropologia structurală* – abordează domeniile identitare şi interculturale care afectează comportamentul individual; rolul cunoaşterii percepțiilor şi psihologiei individului este determinant pentru interpretarea datelor obținute în special prin prisma efectelor secundare ce pot fi induse;

• *sociologia* – are multe de oferit intelligence-ului în studierea rețelelor sociale; după cum şi studiul colaborării dintre diversele instituții care concură la asigurarea securității este important, iar intelligence-ul poate furniza decidenților clarificări privind mecanismul social necesar controlului şi supravegherii tuturor rețelelor sociale;

• *comunicarea şi relațiile publice* – asigură competitivitate prin informare; intelligence-ul este important ca factor de comunicare, prin transparentizarea activităților, cu privire la ceea ce este permis şi ceea ce este interzis în comunitate, nu doar furnizând securitate ci şi schimbări ale mentalităților în interiorul societății.

În domeniul intelligence se reflectă, cu precădere, metodele de cercetare pe bază descriptivă, inductivă şi deductivă, metodele comparativă, explicativă şi estimativă, metodele generate de intelligence ca proces

[2] Gill, Peter, „Theories of intelligence: where are we, where should we go and how might we proceed?", *Intelligence theory: Key questions and debates (Studies in intelligence)*, Routledge, 2009, pp. 220-221.

cognitiv legat de o gamă complexă de variabile care țin de psihologia analistului individual.

Dacă ştiința înseamnă cunoştințe organizate, ca răspuns la noi descoperiri şi dezvoltarea de noi metode de cercetare, pentru a ajuta să se înțeleagă ceea ce este deja cunoscut şi ceea ce nu a fost încă dar poate fi descoperit, am putea vorbi despre ştiința intelligence-ului, însă… această ştiință aşteaptă să se inventeze prin efortul colaborativ al teoreticienilor şi practicienilor din domeniu.

Pentru că nimic nu are valoare în ştiință dacă nu este comunicat, constatăm că un prim pas s-a realizat pentru identificarea intelligence-ului ca ştiință prin faptul că au fost elaborate criterii şi liste, chiar dacă, uneori, s-au dovedit artificiale şi rigide. Însă, acestea, prin parametrii identificați, au permis direcționarea şi clarificarea tematicilor pentru cercetări viitoare, care, prin diseminare în literatura de specialitate, odată rafinate vor fi transformate şi interconectate într-o structură fluidă la nivel global, astfel încât după testare să se poată confirma validitatea rezultatelor ce vor fi preluate în cadrul exercițiilor de formare profesională a novicilor şi de specializare a experților.

David Kahn în *An historical theory of intelligence* arată că, deşi, *intelligence-ul* a devenit o disciplină academică în urmă cu jumătate de secol, totuşi, încă se resimte lipsa avansării pe tărâmul teoriei ştiințifice aferente acesteia, iar, până azi, chiar dacă unii autori şi-au intitulat lucrările „teoria intelligence-ului", nimeni nu a propus suficiente concepte care să poată fi testate în mod real. De aceea, în opinia sa, definirea intelligence-ului, în sensul cel mai larg al noțiunii, trebuie să se bazeze pe câteva principii care trebuie fixate cu privire la trecutul, prezentul şi viitorul acestei discipline ştiințifice[3].

În acelaşi timp, dezvoltarea unei taxonomii de intelligence este complicată de faptul că literatura de specialitate este, de regulă, cantonată pe zone de interes strict pentru rezolvarea unor probleme specifice mediului public sau privat şi mai puțin pe analiza generală a domeniului de intelligence ca furnizor de expertiză pentru o profesie. Aceasta cu atât mai mult cu cât, comparativ cu alte tipuri de activități care folosesc informațiile, intelligence-ul se bazează pe două variabile distinctive: înşelăciunea intenționată şi păstrarea secretului; în plus, constrângerile sub care se acționează în domeniul

[3] Kahn, David, *Intelligence theory: Key questions and debates (Studies in intelligence)*, Routledge, 2009, p.4.

intelligence-ului obligă la angajarea unor decizii încă înainte ca datele şi informaţiile analizate să fie complete, presupunând, inclusiv, luarea în calcul a unui posibil eşec.

Aşadar, este necesar ca intelligence-ul, ca sistem analitic complex în sine, să fie supus unui proces de analiză şi descompunere în caracteristici şi variabile, pentru a fi identificate cele mai mici şi simple elemente şi componente funcţionale care pot fi supuse studiului individual.

Un prim criteriu pentru evoluţia ştiinţifică şi dezvoltarea unei discipline este legat de utilizarea în mod stabil a unor denumiri distincte prin care toţi cei care studiază domeniul să înţeleagă permanent acelaşi lucru. Susţinem că intelligence-ul nu reprezintă un alt termen pentru informaţii. În fond, informaţiile sunt utilizate printr-o tratare activă pentru obţinerea de intelligence care furnizează cunoştinţe cu un important potenţial util pentru o acţiune în perspectivă.

Intelligence-ul nu este doar o informaţie care există pur şi simplu. Prin intelligence înţelegem, adesea, condiţiile în care se află o structură complexă constituită din acţiuni şi reacţii, în care cauzele şi efectele nu sunt cunoscute în mod clar şi unde impactul unor decizii poate fi disproporţionat comparativ cu intenţia, iar consecinţele pot fi foarte rar anticipate cu certitudine[4].

Totuşi, nu numai din motive de securitate, clasificarea şi secretizarea produselor de intelligence le învăluie în mister şi le face mult mai puţin concrete decât sunt cunoştinţele care presupun mai multă certitudine.

Peter Gill defineşte intelligence-ul astfel: numai activităţile secrete – căutarea ţintelor, culegerea, prelucrarea, analiza şi diseminarea – cu scopul de a îmbunătăţi starea de securitate şi/sau pentru a menţine controlul/puterea în faţa competitorilor prin prevenirea ameninţărilor şi valorificarea oportunităţilor[5].

Intelligence-ul înseamnă informaţii şi cunoştinţe obţinute prin operaţiuni derulate în mod direct într-un mediu ostil, mai puţin cunoscut şi controlat decât orice altă zonă de conducere şi comandă, implică înţelegerea şi interpretarea informaţiilor, discernerea semnificaţiilor corecte ale informaţiilor colectate. Astfel, chiar o bună cunoaştere şi înţelegere a

[4] Warner, Michael, „Intelligence as risk shifting", *Intelligence theory: Key questions and debates (Studies in intelligence)*, Routledge, 2009, p. 19.

[5] Gill Peter, „Theories of intelligence: where are we, where should we go and how might we proceed?", *Intelligence theory: Key questions and debates (Studies in intelligence)*, Routledge, 2009, p. 214.

mediului ostil nu presupune o bună cunoaştere a ceea ce se va întâmpla. În plus, intelligence-ul asigură nu doar înțelegerea condițiilor prezente ci şi a intențiilor, estimând toate posibilitățile şi probabilitățile de evoluție. Pentru aceasta, pe lângă utilizarea integrată a celor cinci simțuri umane dovedite (văz, auz, simțul tactil, gust şi miros) este necesară şi capacitatea de a judeca intuitiv, care ne permite să elaborăm predicții.

De regulă, pornind de la rezultatele cercetărilor ştiințifice, s-a creat presupunerea falsă că, în mediul înconjurător, nu există decât ceea ce noi percepem cu ajutorul propriilor simțuri. Cu toate acestea, este evident că multe dintre elementele din mediul înconjurător şi multe dintre circumstanțele care le determină ne rămân necunoscute, chiar şi folosind cele mai sofisticate instrumente de cunoaştere. Aşadar, putem accepta faptul că un fenomen poate exista şi poate produce efecte chiar dacă noi nu îl percepem.

Desigur, limitele percepției pot speria pe necunoscători sau pot intriga cercetătorii ştiințifici, însă ele reprezintă, totodată, granița de unde începe manipularea prin înşelarea aşteptărilor simțurilor umane.

De aceea, intelligence-ul nu este o simplă informație care ne aduce date despre mediul înconjurător, ci un mod de cunoaştere care ne permite înțelegerea fenomenelor, intențiilor şi manifestărilor componentelor acestuia, investigând inclusiv mijloacele, conexiunile şi mecanismele care scapă controlului simțurilor umane comune, prin interpretarea logică şi intuitivă a interferențelor conştiente şi inconştiente.

Cel mai simplu spus, conflictul dintre instincte produce incertitudine, sentimentul de neliniște fiind direct proporțional cu importanța problemei, iar omul încearcă să rezolve dificultatea cu care se confruntă cu ajutorul cunoştințelor deținute, pe care, de altfel, se şi bazează soluția aleasă.

Pentru luarea deciziilor, cei care au acces la rapoarte de intelligence trebuie să cunoască aceste specificități, precum şi faptul că ei trebuie să întregească aceste cunoştințe prin propriile percepții ale contextului.

Chiar dacă noțiunii de intelligence nu i s-au conferit prin definițiile date de-a lungul timpului preocupările privind transparența şi responsabilitatea procesului, P. Gill consideră că acestea sunt intrinseci şi, totodată, parte esențială a teoriilor democrației, după cum sunt extrinseci problematicii în cazul definirii intelligence-ului de către regimurile totalitariste unde responsabilitatea şi transparența sunt considerate parte internă a securității şi nu de interes civic[6].

[6] Ibidem, p. 222.

3. Către o infrastructură a intelligence-ului colaborativ

Dacă rădăcinile intelligence-ului se regăsesc în domeniul biologic, fiind reprezentate de mecanismul de percepere a stimulilor, prezentul este caracterizat de principiul asigurării obținerii optimului prin folosirea resurselor existente. Acesta reprezintă, în notarea lui D. Kahn, principiul O'Brien sau primul dintre cele trei principii ale intelligence-ului, în stadiul actual. Al doilea principiu este considerat a fi faptul că intelligence-ul este auxiliar unui scop, nu elementul principal al acestuia. Intelligence-ul ajută la obținerea victoriei, competitivității, dar succesul/câştigul aparțin întotdeauna oamenilor, grupului, trupelor, forței care îl utilizează, deoarece acțiunea intelligence-ului este indirectă. Al treilea principiu arată că intelligence-ul joacă un rol mult mai important, esențial, în defensivă decât în ofensivă. De aceea, pentru victorie în ofensivă este necesară surpriza.

În viitor, intelligence-ul trebuie să răspundă/să găsească soluții unor probleme fără sfârşit, de pildă, schimbarea comportamentului uman, astfel încât faptele şi logica prezentate de intelligence să fie acceptate şi atunci când acestea contravin presupozițiilor/dorințelor beneficiarului. În plus, se aşteaptă ca potențialul beneficiilor provenind din intelligence să fie larg răspândite, aşa cum, astăzi, la cunoaştere (reprezentând o formă incipientă a sa) au acces toți oamenii.

Dacă în război intelligence-ul scurtează durata conflictelor, în timp de pace poate reduce incertitudinea, poate relaxa tensiunile dintre state şi poate ajuta, prin cele mai importante binefaceri pe care acest serviciu le poate aduce păcii umane, la stabilizarea sistemului global[7].

În timp, intelligence-ul a devenit un factor de producție, generator şi determinant al rezultatelor economice şi chiar un mod de aplicare practică a modului de a trăi viața. De aceea, pentru a evita excluderea sau marginalizarea populației de la producerea resurselor de cunoaştere şi de la utilizarea rețelelor de intelligence trebuie să se insiste pe furnizarea de educație de bază şi formarea profesională, dezvoltarea abilităților cognitive şi stabilirea competențelor şi abilităților necesar a fi dezvoltate, în perspectivă.

În acest context intelligence-ul trece de la formula de structură la cea de infrastructură.

---

[7] Peter, Gill; Stephen, Marrin and Mark Phythian, *Intelligence theory: Key questions and debates (Studies in intelligence)*, Routledge, 2009, pp. 8-13.

Descrierea conceptului de guvernare, valorificând cunoaşterea specifică domeniului intelligence, în contextul integrării economice transnaționale, care nu mai oferă politicilor economice şi sociale naționale capacitatea de a evada prin forțe proprii din stagnarea economică şi de a reduce numărul, altfel tot mai mare, al persoanelor afectate de şomaj, se transformă în identificarea unei crize de legitimitate, generată atât de reconfigurarea spațiilor asupra cărora este exercitată puterea cu consecințe în planul reglementării mai accentuate a fluxurilor financiare, prin decizii ale unor structuri supranaționale consolidate, cât şi de întărirea identității şi apartenenței teritoriale, prin încercarea actorilor locali, naționali şi regionali de a proiecta propriile strategii pentru a găsi o cale de a depăşi vulnerabilitățile, prin descentralizare şi o autonomie decizională în definirea politicilor publice.

O mai bună înțelegere a dependenței reciproce şi a necesității de a coopera şi negocia pe mai multe niveluri, atât orizontal între actori din domenii diverse cât şi vertical între diferite agenții cu decizie în variate planuri teritoriale, reflectă o reducere a rolului de reglementare al statului, transferarea viziunii asupra proiectelor teritoriale dincolo de simplul spațiu geografic şi centrarea interesului asupra interdependențelor fizice, economice, sociale, culturale şi politice, transformând comportamentul sistemic al teritoriului într-o construcție socială cu o capacitate variabilă care cuprinde un sistem în care sunt reprezentați concomitent actori de la nivel local, național şi mondial, public şi privat, comercial şi sociopolitic.

De fapt, infrastructura de intelligence pentru o bună guvernare permite o acțiune autoalimentată, prin instrumente şi metodologii de lucru participative care asigură schimbarea şi valorificarea coordonată şi coerentă a cunoştințelor, producând noi cunoştințe care sunt împărtăşite prin învățare, conducând la dezvoltarea şi îmbunătățirea acțiunii comune în care sunt implicați nu numai factorii instituționali de decizie ci, mai ales, actorii individuali care gestionează informații pe care le transformă prin mecanismele activității lor curente în cunoaştere pentru intelligence, fapt ce permite evaluarea, direcționarea şi remodelarea propriilor acțiuni.

Consecvent acestor perspective, constatăm că evoluția cunoaşterii este un proces rapid în care nimeni nu se poate declara deținătorul tuturor cunoştințelor şi în care toți participanții au unele contribuții proprii. Prin urmare, în activitatea de educare/predare organismele abilitate nu mai au funcțiuni exclusiviste, acestea devenind doar facilitatori pentru învățare şi emițători de metode li se reduce rolul de transmitere a cunoştințelor de bază,

esențiale sau fundamentale şi sunt obligate să se concentreze mai mult pe rolul de transmițător/coordonator cu precădere al învățării cu privire la metodele şi mijloacele de obținere a noilor cunoştințe. Astfel, ceea ce este important nu este cunoaşterea în sine, care este disponibilă, ci îmbunătățirea inteligentă a propriei condiții prin adaptarea mai bună la schimbările din mediul înconjurător.

În aceste situații, în care subiectele sunt mai multe şi mai complexe, şi în care informațiile şi cunoştințele sunt răspândite pretutindeni, cercetării îi revine rolul de a descoperi, de a inova şi de a reflecta critic asupra problemelor cu care se confruntă omenirea, aspecte cu privire la care, şi prin intelligence, rezultatele ştiințifice sunt deschise unor multiple interpretări.

Pentru toate aceste scopuri cercetarea participativă (colaborativă) poate avea un impact mai mare întrucât elaborarea, producerea, analizarea informațiilor şi interpretarea rezultatelor în mod colectiv, pe de o parte, conduce la creşterea capacității individuale a actorilor, iar mobilizarea capacităților individuale de a produce şi a procesa cunoştințe, pe de altă parte, poate contribui la favorizarea consensului sau cel puțin la o bază comună de informații şi cunoştințe.

Întotdeauna, însă, pentru o acțiune dinamică şi eficientă este indispensabilă o conexiune corelativă între cercetare şi munca de teren, între analiză şi decizie, precum şi un sistem de intelligence bine structurat.

4. Concluzii

Peter Gill, în „Theories of intelligence: where are we, where should we go and how might we proceed?”[8], subliniază că importanța intelligence-ului nu este doar aceea legată de studiul ştiințific, ci este generată de un context în care percepția insecurității, sub multiplele ei forme (terorism, crimă organizată, trafic), obligă la realizarea de performanțe în domeniu, ca necesitate pentru crearea posibilităților de asigurare a menținerii securității şi siguranței publice prin mijloace democratice.

De ce este importantă această dezbatere? Diferite agenții şi instituții folosesc diverse modalități de definire şi înțelegere teoretică, legislativă şi practică a activității de intelligence. Funcție de acest concept sursele, metodele şi mijloacele sunt tratate, caracterizate şi explicate distinct.

[8] Gill, Peter, „Theories of intelligence: where are we, where should we go and how might we proceed?”, *Intelligence theory: Key questions and debates (Studies in intelligence)*, Routledge, 2009, p. 213.

Într-o lume în care ameninţările şi oportunităţile în plan naţional şi internaţional devin mai degrabă transnaţionale (incluzând nu doar terorismul, crima organizată, proliferarea armelor nucleare, cyber-criminalitatea şi pandemiile sanitare, cucerirea spaţiului cosmic, dezvoltarea economică, progresul în domeniul sănătăţii umane), aceasta implică şi schimbarea modalităţilor de cunoaştere, tratare şi răspunsuri contrapuse acestor riscuri şi posibilităţi reale.

Ca parte a sarcinii de a servi interesul naţional şi de a proteja cetăţenii propriului stat, devine tot mai mult necesară găsirea de soluţii prin mecanisme de cooperare şi colaborare a serviciilor de intelligence din ţările democratice ale lumii.

De altfel, după 11 septembrie 2001 asemenea activităţi nu mai reprezintă fenomene singulare, ci o funcţie cu o creştere exponenţială care generează schimbări majore şi noi direcţii de acţiune globală pentru fiecare stat şi agenţie în parte, de la forme de schimb de informaţii ad hoc, punctuale, până la modalităţi instituţionalizate, bilaterale şi multilaterale, aspecte care presupun, în primul rând, un limbaj cu noţiuni şi sensuri comune. Lock K. Johnson, în „Sketches for a theory of strategic intelligence", sugerează că, cu cât este mai deschisă globalizării, o naţiune are mai mare nevoie de intelligence[9].

Îngrijorările experţilor cu privire la lipsa coerenţei definirii intelligence-ului sunt exprimate prin faptul că intelligence-ul este, adesea, folosit ca un termen mult prea cuprinzător pentru orice activităţi de procesare a informaţiilor[10]; iar când totul pare a fi intelligence, atunci nimic nu este, de fapt, intelligence[11].

În plus, în scopul unei mai bune înţelegeri a intelligence-ului disputa pentru identificarea elementelor-cheie definitorii ale procesului trece în prim plan, deşi mult mai importante sunt, pentru a sublinia rolul acestui demers ştiinţific, îmbunătăţirea eficacităţii şi eticii intelligence-ului[12].

---

[9] Lock K., Johnson, „Sketches for a theory of strategic intelligence", Intelligence theory: Key questions and debates (Studies in intelligence), Routledge, 2009, pp. 36-40.

[10] Philip H. J., Davies, „Theory and intelligence reconsidered ", *Intelligence theory: Key questions and debates (Studies in intelligence)*, Routledge, 2009, pp. 194-200.

[11] Warner, Michael, „Intelligence as risk shifting", *Intelligence theory: Key questions and debates (Studies in intelligence)*, Routledge, 2009, pp. 17-19.

[12] Gill, Peter, „Theories of intelligence: where are we, where should we go and how might we proceed?", *Intelligence theory: Key questions and debates (Studies in intelligence)*, Routledge, 2009, p. 213.

Mai mult chiar, într-o perspectivă care vizează interese globale comune, eliminarea confuziilor şi găsirea răspunsurilor nu ţin atât de complexitatea subiectului sau de lipsa abilităţilor experţilor, cât mai ales de păstrarea secretului cu privire la instrumentele care permit funcţionarea activităţilor de colectare, prelucrare, integrare, analiză, evaluare şi interpretare a informaţiilor.

Bibliografie

1. Davis, Jack, „A Policymaker's Perspective On Intelligence Analysis", *Studies in Intelligence*, No. 5/1995, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications /csi-studies/studies/95unclass/Davis.html, 30 aprilie 2010.

2. Devlin, Keith, *Confronting context effects in intelligence analysis: How can mathematics help?*, Center for the Study of Language and Information, Stanford University, 2005, http://www.stanford.edu/~kdevlin/Context_in_Reasoning.pdf, 30 aprilie 2010.

3. Gill, Peter; Stephen, Marrin and Mark, Phythian, *Intelligence theory: Key questions and debates (Studies in intelligence)*, Routledge, 2009.

4. Kent, Sherman, *Strategic Intelligence for American World Policy*, NJ: Princeton University Press, Princeton, 1951, revised edition 1966.

5. Krizan, Lisa, *Intelligence Essentials for Everyone*, Joint Military Intelligence College, (June 1999), http://www.scip.org/2_getinteless.php, 30 aprilie 2010.

6. Odom, William E., *Fixing Intelligence: for a More Secure America*, New Haven, Yale University Press, 2003.

7. Robert, M. Clark, *Intelligence Analysis: A Target-Centric Approach*, CQ Press – A Division of Congressional Quarterly Inc., Washington DC, 2006.

8. Rob Johnston, "Developing a Taxonomy of Intelligence Analysis Variables", *Studies in Intelligence*, No. 3/2003, second edition, www.iwar.org.uk, 30 aprilie 2010.

9. Wiener, Norbert, *Cybernetics: or Control and Communication in the Animal and the Machine*, Cambridge, MIT Technology Press, second edition, 1985.

Ion IVAN este lector universitar, secretar ştiinţific al Senatului Academiei Naţionale de Informaţii *„Mihai Viteazul"*, doctor în economie, autor/coautor al unor articole şi studii în domeniul prevenirii şi combaterii finanţărilor frauduloase şi al teoriei informaţiei şi intelligence-ului.

Despre intelligence (II)

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

Abstract

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

Keywords: intelligence/OSINT, open/secret.

Introducere

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

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

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

III. Influența factorilor identificați tradițional („știință şi tehnologie") şi mai ales a interacției de natură cibernetică între aceştia.

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

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

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

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

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

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

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

paradigma secretului, şi un atribut al acţiunii şi exploatării informaţiei şi cunoaşterii cu *circuit deschis*, manifestat prin *paradigma deschiderii*.

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

Consolidarea activităţilor de *intelligence al informaţiei* se face numai prin coordonarea eficientă a proceselor de *intelligence al cunoaşterii*. Până acum două decenii serviciile şi agenţiile de intelligence deţineau supremaţia ştiinţifică şi tehnologică, situaţie care în ultimele două decenii s-a modificat dramatic, astfel încât astăzi această supremaţie o deţine sectorul privat, mult mai competitiv şi adaptat la nevoile şi trendurile pieţei globale.

Mai există însă un element hotărâtor. Orice domeniu ori disciplină pentru a fi completă are nevoie de o teorie, strategie, doctrină[1] şi tehnologia aferentă necesară atât trecerii de la teorie la acţiune, cât şi mai ales dobândirii unui sens suficient de flexibil pentru semnificaţia cuvântului „practic" asociat acestuia. Dacă unul dintre elemente este omis ori neglijat şi se reduce semnificaţia cuvântului „practică" la elementele rămase, atunci este afectat potenţialul de relansare a ciclului de cunoaştere necesar mai ales în intelligence-ul contemporan. Cine nu reuşeşte din diverse motive să îşi asigure o astfel de viziune, în sensul unei implementări identitare şi integrate, se poate considera, dacă nu un învins al viitorului, cu siguranţă un perdant al prezentului. Acesta este sensul discursiv pe care noi l-am asociat ideii „knowledge intelligence".

Al treilea reper se referă la un nou concept menit a reuni şi integra procesele de gestiune şi administrare a cunoaşterii şi informaţiei la nivel de organizaţii, reţele şi meta-reţele de intelligence, atât la nivel de stat-naţiune, cât şi la nivel de coaliţii. Este ceea ce numim intelligence sistemic.

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

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

Principiul de dualitate şi ISD – informația din surse deschise

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

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

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

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

Ca o consecinţă directă, în cadrul acestui tip de mecanism al dezvoltării globale şi, prin urmare, al relaţiilor internaţionale s-a produs o mutaţie dinspre zona geopolitică către cea geoeconomică. Conceptul cheie al acestei mutaţii este reprezentat de avantajul competitiv, ce acum constă în abilitatea de a gestiona cunoaşterea la nivel strategic, în special prin sisteme deschise, în toate sectoarele societăţii (administraţie publică, industrii etc.), pentru crearea de bunăstare economică şi socială, privite drept potenţial de intelligence necesar garantării securităţii. Acest mod de a concepe lucrurile provine din gândirea legată de modelarea matematică: acolo în cadrul ciclului de avans al cunoaşterii reprezentat de modelare se identifică o înlănţuire de factori cauzali de naturi distincte, se compun în mecanisme furnizându-se nu doar o descriere a fenomenului, ci o funcţionare a acestuia. Această funcţionare permite cel puţin două construcţii esenţiale pentru fenomenul decizional: simularea şi generarea scenariilor. Simpla descriere ori identificare are un caracter static ori cel mult cinematic şi, deşi, este absolut necesară, devine total insuficientă după criteriile acţiunii politice în timp real. Problematica sustenabilităţii avantajului competitiv a impus extinderea şi rafinarea precedentului mod de abordare şi chiar în acest proces apare necesitatea ca intelligence-ul să migreze către intelligence/OSINT.

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

Dualitatea închis/deschis

Primul fapt relevant ce transpare din scurta discuție introductivă ce deschide prezenta secțiune constă în aceea că o întreagă concepție asupra semnificației cuvântului „securitate" trebuie adaptată cel puțin în raport cu toate cele patru elemente menționate drept precondiții ale unui domeniu complet. Pentru a da un exemplu, domeniile clasice ale geopoliticii ori relațiilor internaționale, azi şi cu atât mai mult mâine, nu mai au nicio valoare în forma lor pur clasică – moştenită de la Morgenthau[2] spre exemplu pe paradigma realistă. Aceasta nu înseamnă, vreun moment, că trebuie omise, însă adaptările pe cele patru componente (cel puțin, teorie, strategie, doctrină, tehnologie) modifică din temelii sensul respectivelor cuvinte. Cum anume s-ar raporta cineva la cadrele actuale ale geopoliticii fără nicio cunoştință privitoare la ştiința regională a lui Isard[3], reconceptualizările geoeconomice ale lui Krugman[4] ori fără a face apel la reprezentările de tip GIS (Geographic Information System). În mod dual, cum anume s-ar angaja în analiză cineva fără a deține în propriul orizont de cunoştință consistentele contribuții ale lui Morgenthau, Rosenau[5] etc. ori problemele deschise perene identificate de Alker[6] în domeniul relațiilor internaționale – este ca în cazul şahului cu portofoliul de partide celebre. Pe scurt, paradigma deschiderii nu conține numai problema de natură informațională, ci şi modul în care ştim ca națiune să alocăm rolul corect componentei clasice în contextul turbulent al provocărilor viitoare. Iar asta din componenta teoretică, deoarece cuvântul practic de acolo îşi trage semnificația – cum legăm teoria de acțiune. Din nefericire, mentalul practicat în România în ultimii 60 de ani are foarte puțin de a face cu această concepție, iar acest fapt face şi mai dificilă implementarea ei.

[2] Hans Morgenthau – unul dintre inițiatorii şi principalii contributori ai realismului în relațiile internaționale.

[3] Walter Isard – unul dintre inițiatorii şi principalii contributori ai domeniului "Regional Science".

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

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

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

Rolul sistemelor deschise

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

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

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

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

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

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

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

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

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

Atributele ISD

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

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

Gestionarea ISD devine o componentă a unei noi funcţii de intelligence la nivel naţional: **intelligence-ul „deschis”** care presupune în primul rând **transfer de cunoaştere** a procesului de intelligence în interiorul şi între toate **sectoarele societăţii.** Acest fapt a determinat lansarea unor iniţiative de către guvernele statelor occidentale, precum:

- înfiinţarea unor departamente de intelligence, denumite intelligence competitiv, conduse de un ministru adjunct sau implementarea unui concept de intelligence teritorial, astfel încât toţi prefecţii să urmeze cursuri de pregătire în domeniu – cazul Franţei fiind cel mai uşor de studiat dar relevant pentru statele cu mental societal compatibil cu această cultură;
- dezvoltarea conceptului de intelligence competitiv la nivelul mediului de afaceri – SUA, Marea Britanie, Suedia, Franţa, Germania, iar în ultimul deceniu ţările BRIC – Brazilia, Rusia, India, China – dar şi ţări precum Singapore, Africa de Sud etc.

Având în vedere spectrul larg de distribuţie la nivel global, abordarea eficientă a ISD va putea fi realizată doar printr-un angajament comun al tuturor actorilor interni ai unui stat – fapt ce prelungeşte şi adaptează conceptul de „intelligence organizaţional” lansat în anii ’70. De altfel, nicio entitate din această lume (organizaţie privată sau publică, stat sau organism internaţional) nu va putea să acopere ISD decât printr-o organizare de tip reţea. Reuşita unui asemenea demers implică identificarea nodurilor importante din reţea, prin intermediul cărora un serviciu de informaţii se poate conecta la sistemul deschis. Parteneriatele incheiate cu aceste noduri vor conduce la gestionarea eficienta a ISD şi la decizii cheie privitoare la participarea în procesele cerute de intelligence-ul alianţelor.

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

În funcţie de aria de interes şi zonele de responsabilitate în care se poziţionează actorii naţionali, OSINT se transformă dintr-o sursă de informaţii a sistemului de surse intelligence într-un domeniu, o resursă, un proces, un produs, o organizaţie şi o capabilitate de interes naţional. În realitate vorbim despre apariţia unui nou tip de intelligence ce poate fi derulat la nivelul

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

Redefinirea intelligence

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

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

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

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

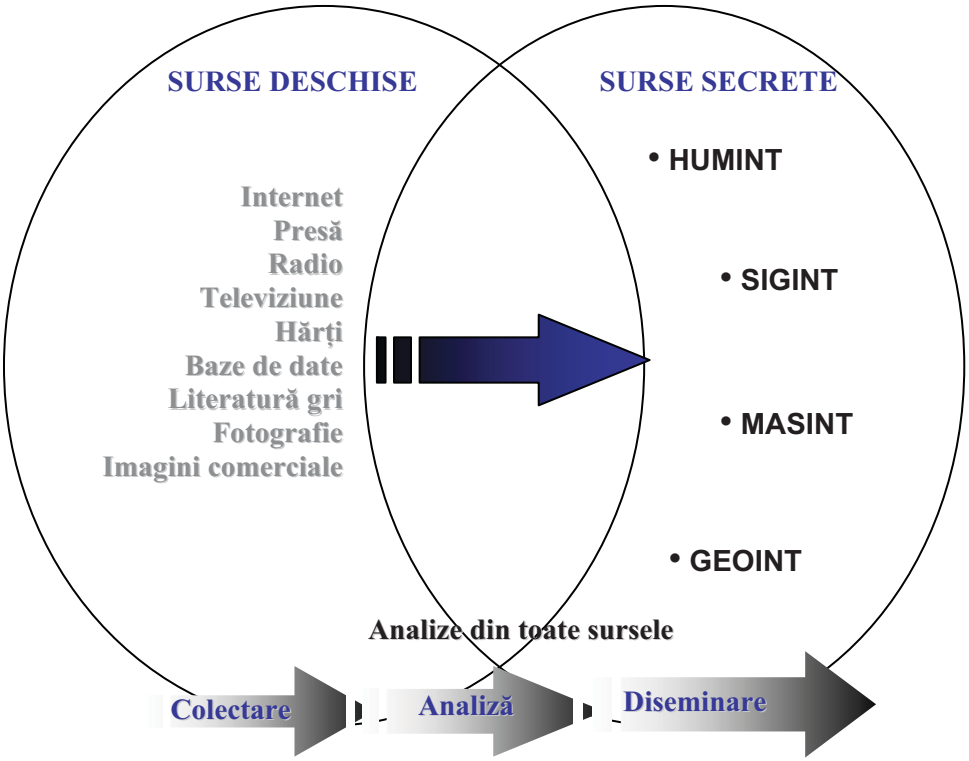


Fig. 1 Exploatarea focalizată a Open Source va conduce la eficientizarea cheltuielilor oricărei Comunități de Intelligence

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

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

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

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

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

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

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

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

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

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

Bibliografie

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

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

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

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

Tendințe în managementul informațiilor în domeniul prevenirii şi combaterii terorismului

Laura-Loredana CHELMUŞ
Serviciul Român de Informații
e-mail: **cloredan@yahoo.com**

Abstract

The information revolution witnessed today requires more and more a real-time process of coordination in order to make the best of the available information.

The dynamics of the terrorist phenomenon have revealed the importance of prevention and, thus, a need to review the ways of approaching it.

In time, we have noticed the willingness of states to draft strategic documents designed to ensure an appropriate management of information and, thus, to develop intelligence analysis.

In practical terms, there is an increasing number of states setting up antiterrorist coordination centers to integrate terrorism-related information and to draft threat assessments.

Moreover, further strengthening of the cooperation remains a prerequisite for success in the fight against terrorism.

Keywords: management of information, terrorism prevention.

Articolul de față a fost scris având ca obiectiv principal identificarea unor tendințe în managementul informațiilor în domeniul prevenirii şi combaterii terorismului – fenomen ale cărui proporții şi nivel de risc la adresa securității cetățeanului determină o abordare integrată în plan național şi eforturi similare la nivel regional sau internațional.

Acest demers este parte a unui proces de cercetare care a urmărit să analizeze procesele de coordonare unitară a informațiilor în domeniul prevenirii şi combaterii terorismului şi nivelul până la care pot fi fezabile modelele operaționalizate până în prezent.

Evoluțiile din ultimii ani denotă că – în pofida unor succese notabile – experienței acumulate de comunitatea internațională i se contrapune

perfecționarea permanentă a mijloacelor şi metodelor (prin lărgirea paletei de obiective vizate, creşterea gradului de complexitate a mijloacelor utilizate, tehnologiile avansate şi rețele de comunicații, sabotaj economic etc.) utilizate de teroriști pentru comiterea de atentate.

„Lecțiile învățate" din evenimentele dramatice, precum 11 septembrie 2001 sau 11 martie 2004, au contribuit la reconfigurarea politicilor aferente, dublată de o relativă, dar necesară, armonizare în plan global şi regional şi de o consolidare a cooperării în domeniu, după ce acestea au relevat existența unor breşe în abordările naționale. Totodată, incidentele de această natură au indicat că, în pofida deținerii unor informații relevante, absența unei integrări corespunzătoare a puzzle-ului informațional, care să ofere tabloul general, nu permite gestionarea adecvată a situației.

Pornind de la aceste rațiuni, considerăm că dinamica actuală a acestui fenomen implică condiția *sine qua non* a unui management adecvat şi eficient al exploziei informaționale cu care ne confruntăm, atât la nivel național, cât şi regional sau internațional, în aceste planuri, în formate agreate de părți.

Acest lucru este cu atât mai necesar cu cât tendința ascendentă a amenințărilor asimetrice, atipice necesită o abordare avangardistă, având în prim-plan activitatea de informații şi un rol sporit pentru structurile cu atribuții în culegerea de informații. La nivelul comunității internaționale, amenințări precum terorismul au determinat, deopotrivă, factorii de decizie şi autoritățile competente să-şi reevalueze capacitatea de acțiune şi prioritățile operaționale.

În ultimii ani, raportările la acest fenomen au înregistrat mutații semnificative, determinând o schimbare de viziune: de la o dimensiune pronunțată de combatere la o consolidare a componentei preventive în lupta împotriva terorismului, cu accent pe relevanța şi utilitatea resurselor informaționale care fundamentează această dimensiune.

Lupta împotriva terorismului, cu precădere în ceea ce priveşte componenta preventivă, are la bază informația şi, implicit, activitatea de informații. Rolul acesteia este de a asigura cunoaşterea multivalentă a adversarului, în acest caz, a entităților teroriste – organizații sau indivizi – iar evaluarea corectă a amenințării este esențială pentru nivelul decizional care trasează liniile directoare pentru autoritățile competente.

Explozia informațională fără precedent, implicit fluxul informațional de proporții către autorități, reliefează necesitatea derulării în parametri de

eficiență a ciclului de *intelligence* şi, în principal, direcționarea adecvată pentru a obține o utilitate concretă.

Pentru contracararea acestei amenințări, statele şi organizațiile colective îşi canalizează eforturile pe consolidarea componentei preventive, prin alocarea de resurse pentru:

- elaborarea unor documente strategice punctuale destinate asigurării unui management adecvat al informațiilor cu privire la amenințările teroriste;

- dezvoltarea componentei analitice, îndeosebi a analizei de intelligence;

- crearea centrelor de coordonare antiteroristă;

- consolidarea activității de cooperare.

Strategiile naționale de securitate – sau în cazul statelor care au elaborat documente strategice privind combaterea terorismului – trasează liniile directoare şi facilitează colaborarea strânsă între autoritățile naționale responsabile în domeniul de referință.

În lupta împotriva terorismului, statele în care nivelul amenințării este ridicat dispun inclusiv de o *strategie privind difuzarea de informații* la nivel național, pentru asigurarea transferului informațiilor disponibile de la nivelul unei autorități competente către celelalte structuri cu responsabilități. Un exemplu, în acest sens, este SUA. Astfel de documente strategice pot fi dublate de *modele de management al informațiilor*, precum *National Intelligence Model* – NIM sau *Intelligence Led Policing* – ILP, care coboară, în planul tactic şi operațional, pe dimensiunea de infracționalitate.

O astfel de tendință este vizibilă nu numai la nivel național, ci şi în cadrul unor organizații supranaționale de tipul Uniunii Europene. Pornind de la acelaşi considerent, pentru îndeplinirea unui deziderat important al Uniunii Europene – asigurarea „spațiului libertate, securitate şi justiție" – documentele strategice elaborate la nivel comunitar cu sprijinul statelor membre, precum Programul multianual Stockholm (care trasează liniile directoare în domeniul cooperării polițieneşti şi judiciare – cunoscut ca Justiție şi Afaceri Interne – căruia i se subsumează lupta împotriva terorismului), invocă deja necesitatea elaborării unei *Strategii UE de management a informațiilor.*

Strategia de securitate internă a UE, document adoptat în acest an, care decurge, de asemenea, din Programul Stockholm, merge chiar mai departe stabilind ca prioritate elaborarea unui *Model european privind schimbul de informații în domeniul Justiție şi Afaceri Interne (JAI)*, care să includă toate

bazele de date europene relevante şi să asigure interoperabilitatea acestora, ca instrument necesar pentru facilitarea schimbului de informaţii între statele membre (cu precădere în domeniul JAI).

Astfel de repere vizează facilitarea procesului de selectare a informaţiilor disponibile şi direcţionarea acestora către planul operaţional sau cel analitic.

În paralel cu aceste documente, se constată o asumare de responsabilităţi în domeniul analizei în plan comunitar, care se reflectă în elaborarea de evaluări şi tendinţe ale ameninţării teroriste la adresa Europei, elaborate în cadrul a diferite instituţii sau agenţii comunitare, destinate unor beneficiari comunitari.

Regăsim, în cadrul structurii organizatorice a Comisiei Europene, *Directoratul de Securitate* cu responsabilităţi şi în domeniul antiterorism, care realizează evaluări asupra ameninţării generate de organizaţiile teroriste la adresa sediilor şi funcţionarilor instituţiilor europene şi menţinerea legăturii cu serviciile partenere.[1]

La nivelul Consiliului UE, *Grupul de Lucru pentru Terorism – TWP* are în atenţie aspecte interne din fiecare stat membru cu privire la terorism. Analizele elaborate la nivelul acestui organism – prin corelarea datelor din statele membre – sunt transmise, spre informare, Consiliul Justiţie şi Afaceri Interne şi asigură identificarea unor măsuri individuale, regionale sau chiar la nivel comunitar. *Grupul de Lucru pentru Terorism (Aspecte internaţionale) – COTER* elaborează evaluări similare, pe dimensiunea externă, dar şi propuneri de politici de combatere a terorismului destinate Consiliului de Afaceri Generale şi Relaţii Externe.

Unul dintre cele mai relevante organisme, la nivel comunitar, cu atribuţii în elaborarea de evaluări este SitCen - structura analitică din cadrul Secretariatului General al Consiliului UE, ce reuneşte analişti din cadrul serviciilor de informaţii externe şi produce evaluări ale tendinţelor în domeniul terorismului în state din exteriorul UE.

Adăugarea componentei de analiză a informaţiilor la procesul de elaborare a politicii UE în domeniul antiterorist a fost decisă în anul 2004, de către Consiliul European. „Statele membre decid ce informaţii transmit

[1] Tiberiu Tănase, „Rolul şi atribuţiile de coordonare ale UE pentru combaterea terorismului", http://cssas.unap.ro/ro/pdf_carti/stratxxi_2007_vol2.pdf http://www.sie.ro/Evaluari/evaluari5.html.

către SitCen. Inițial, analiștii Centrului evaluau amenințări generate din afara teritoriului european. Începând din ianuarie 2005, au combinat acele evaluări externe cu informații de la serviciile interne şi Europol."[2]

Pe de altă parte, dintre agențiile comunitare, Europol realizează – anual – o evaluare generală a situației de securitate, din prisma riscurilor generate de amenințarea teroristă, sub forma unui raport, cunoscut sub acronimul TE-SAT (Terrorism Situation and Trend Report). TE-SAT-ul poate fi considerat, în bună măsură, un indicator pentru nivelul cooperării multilaterale privind un segment de informații (cele referitoare la infracționalitate) din domeniul de referință, iar Europol este coordonatorul acestui segment de activitate.

Aşadar, în plan comunitar, evoluțiile indică o preocupare pentru asigurarea managementului unitar al informațiilor care vizează fenomene precum terorism, criminalitate organizată. Componenta „analitică" nu constituie o structură integrată, produsele analitice, îndeosebi evaluările privind amenințarea teroristă, fiind elaborate – aşa cum menționam anterior – în mod disparat, prin contribuțiile statelor membre, pe segmente de competență. Scopul este, însă, acelaşi: informarea factorilor decizionali care, astfel, se realizează pe diferite „canale". În prezent, produsele analitice au un caracter strategic, urmând evoluțiile din mediul de securitate care pot genera implicații pentru spațiul comunitar.

Nu putem vorbi despre un nivel „operațional" sau tactic, dar în cooperarea polițienească şi judiciară destinată combaterii fenomenului terorist există un flux informațional, cu particularitățile conferite de organizarea națională şi comunitară specifică: poliția către Europol, reprezentanții sistemului judiciar către Eurojust.

În acest moment, nu se poate vorbi despre o coordonare unitară a informațiilor în domeniul de referință la nivel comunitar: nu există mecanisme cuprinzătoare de gestionare şi evaluare colectivă a informațiilor care provin de la diferite structuri şi agenții naționale cu atribuții din statele membre.

Totuşi, instituțiile UE, prin prerogativele de care dispun, pot contribui la asigurarea unui dialog eficient între statele care se confruntă cu amenințări teroriste şi a cooperării în domenii precum schimbul de informații, arestarea, extrădarea sau incriminarea indivizilor sau grupărilor teroriste, precum şi suprimarea finanțării acestora.

[2] Daniel Keohane, „The EU and counter-terrorism", http://www.cer.org.uk/pdf/ wp629_terrorism_ counter_keohane.pdf, May 2005.

În acest stadiu, UE poate susține şi recomanda statelor membre să-şi întărească cooperarea între structurile omologe de profil şi să utilizeze, de o manieră eficientă, informațiile de interes comun şi capacitățile de analiză-sinteză comune, dat fiind faptul că mare parte din statele membre se pronunță pentru schimbul de informații pe bază bilaterală.

Europolul tinde să devină un depozitar al informațiilor şi datelor referitoare la prevenirea şi combaterea amenințărilor transnaționale, transmise, în general, de către toate organele de aplicare a legii din statele membre. Putem, aşadar, extrapola acest sistem şi la alte structuri, cu respectarea unei relații omoloage între structura comunitară şi statele membre.

Dintre structurile menționate, SitCen prefigurează cel mai bine tendințele legate de consolidarea componentei multilaterale a cooperării informative, cu atât mai mult cu cât beneficiază de resurse informaționale de la serviciile de informații şi securitate.

Pe termen scurt şi mediu, nu sunt întrunite condițiile pentru crearea unui mecanism integrat de coordonare unitară a informațiilor în domeniul prevenirii şi combaterii terorismului, chiar şi în condițiile acutizării acestui fenomen. Evaluarea este aplicabilă, în egală măsură, dimensiunii analitice şi are la bază următoarele considerente:

- informațiile aferente provin din cadrul unor instituții ale statelor membre, diferite din punct de vedere structural şi al competențelor (poliție, servicii etc);
- un organism central cu componență diversă nu oferă garanții solide privind protecția surselor de informații sau a metodelor utilizate de furnizorii de intelligence (serviciile de informații), existând riscul unor scurgeri de informații;
- schimbul de informații se derulează pe bază de încredere reciprocă, dobândită în timp şi verificabilă, ceea ce este mai dificil de realizat în plan multilateral;
- un organism care să stocheze toate informațiile referitoare la terorism, din cele 27 state membre, este dificil de controlat.

Pe de altă parte, creşte numărul statelor care optează pentru constituirea unor comunități de informații, în sensul realizării unui ansamblu funcțional sinergic în care acționează totalitatea entităților structurale dintr-un stat abilitate în colectarea, prelucrarea şi diseminarea de informații de securitate.

O astfel de abordare s-a translatat – fără să existe o conexiune temporală obligatorie – şi la problematicile specifice aflate în competența

entităţilor structurale respective. Tot mai multe state concentrează informaţiile pe profil antiterorism în centre de coordonare antiteroristă care interconectează structurile abilitate interne (componenţa variind de la stat la stat, în funcţie de particularităţile interne) şi se conectează, la rândul lor, cu organisme similare externe.

Tipologia centrelor de cooperare este diversă: unele state au creat *centre de coordonare antiteroristă* care acoperă ansamblul activităţilor – de la prevenire la combatere – în vreme ce altele au optat pentru separarea componentelor şi axarea activităţii centrelor exclusiv pe evaluarea ameninţării teroriste în plan intern (prin coordonarea unitară a informaţiilor referitoare la terorism şi, implicit, elaborarea unei analize de *intelligence* care să previzioneze riscuri şi să anticipeze evoluţii sau evenimente relevante).

O parte din statele UE – Marea Britanie, Spania, Danemarca etc. – dispun de centre care, în funcţie de specificul naţional, realizează mai multe tipuri de evaluări ale ameninţării teroriste (de la cele generale la cele specifice privind infrastructura critică, anumite evenimente, locaţii, grupări teroriste etc)[3].

La sfârşitul anului 2009, Coordonatorul UE pentru Contraterorism, Gilles de Kerchove, într-un document de discuţie referitor la Strategia UE de combatere a terorismului, făcea următoarea recomandare: „toate statele membre ar trebui să aibă un centru de coordonare antiteroristă *(fusion centre)*, iar statele ar trebui să creeze o reţea care să le interconecteze”[4].

Un prim pas în această direcţie pare să fi fost făcut odată cu intenţia exprimată de Spania – după preluarea preşedinţiei rotative a UE – de a înfiinţa un Comitet european de coordonare antiteroristă, din care să facă parte agenţii naţionale specializate.[5]

De cealaltă parte a Atlanticului, încă din anul 2005, în SUA se identifica, în documentul „Noua arhitectură a informaţiilor” necesitatea existenţei în fiecare stat american a unui *„centru de culegere, analiză şi stocare la care să participe structurile de aplicare a legii prin furnizarea şi primirea de informaţii, pentru sprijinirea luptei împotriva terorismului*

[3] CTA Danemarca, „What is the Center for Terror Analysis?” http://www.pet.dk/English/ Operational_tasks/ Terrorism/CTA.aspx.

[4] http://register.consilium.europa.eu/pdf/en/09/st15/st15359-re01.en09.pdf - 15359/1/09 REV 1 din 26 noiembrie 2009 - EU Counter-Terrorism Strategy - discussion paper.

[5] http://www.adevarul.ro/international/europa/UE-spania-presedintie-lupta_antiterorista_0_182381852.html şi http://www.eubusiness.com/news-eu/spain-attacks.24h/.

prin accesul la numeroase baze de date publice şi private pentru colectarea şi analizarea informaţiilor şi prin elaborarea de produse analitice care să ofere imagini de ansamblu asupra grupărilor criminale şi să fie diseminate către agenţiile participante".[6]

Astfel, pe lângă schimbul de informaţii şi cooperarea operaţională – esenţiale prin contribuţia specifică pe care fiecare dintre parteneri o poate aduce la eforturile concrete de contracarare a unor riscuri – este necesară, în paralel, o consolidare a cooperării analitice.

Relevanţa centrelor creşte cu atât mai mult cu cât principala dimensiune a acestora – cea analitică – traversează o perioadă de transformare şi schimbare de paradigmă. Indiferent de transformările procesuale şi metodologice, evaluarea ameninţării teroriste rămâne fundamentul adaptării politicii în domeniu, iar analiza de intelligence reprezintă o componentă esenţială pentru conturarea unei imagini comprehensive asupra surselor, nivelului ameninţării şi factorilor favorizanţi, în plan naţional sau internaţional.

„Imaginea" reflectată determină, astfel, formularea de noi politici şi strategii în domeniu, care se concretizează, ulterior, în acţiuni şi măsuri destinate protejării cetăţenilor proprii şi, implicit, promovării intereselor naţionale, prin realizarea proiecţiei de factor de stabilitate în plan regional şi comunitar.

Această abordare integrată, care se realizează în cadrul centrelor antiteroriste, constituie un avantaj, în termeni de anticipare a unor potenţiale incidente sau evoluţii, întrucât facilitează elaborarea de produse analitice multi-sursă care sunt puse la dispoziţia factorilor decizionali în mod oportun. Specializarea permanentă a experţilor din cadrul acestor centre asigură o creştere proporţională a capacităţii de interpretare a elementelor disponibile.

Analiza cere competenţă şi experienţă pentru utilizarea instrumentelor, metodelor şi a tehnicilor adecvate, structurarea informaţiilor în funcţie de domeniile de realizare a securităţii naţionale şi de relevanţa acestora, eliminarea incertitudinilor şi analizarea informaţiilor prin diferite metode analitice.

Această realitate este expresia practică a concluziei că „premisele analitice ale procesului de planificare a informaţiilor constau în diferenţierea

[6] http://www.semp.us/publications/biot_reader.php?BiotID=474 - Intelligence-Led Policing in the United States.

dintre cerințele imediate şi tendințele pe termen lung, informațiile legate de terorism fiind evaluate dintr-o perspectivă dublă:

- furnizarea unor evaluări actualizate (zilnic sau chiar mai frecvent) necesare operațiunilor şi reacțiilor imediate; şi

- analiză de tendință şi modele, esențială pentru riposta operațională imediată, precum şi pentru rapoartele solicitate de beneficiarii politici şi, de asemenea, pentru planificarea strategică în general."[7]

Unele insuccese puternic mediatizate ale analiştilor (incapacitatea de anticipare a atacurilor de la 11 septembrie 2001, problematica armelor de distrugere în masă deținute de Irak sau analiza de impact asupra perioadei ulterioare intervenției din Irak) au produs conştientizarea necesității unei reforme şi în cazul analizei. De asemenea, eşecurile înregistrate în prevenirea şi contracararea unor incidente teroriste nu au avut întotdeauna drept cauză lipsa de informații, ci mai degrabă o conexare necorespunzătoare a informațiilor disponibile.

Estimarea corectă a amenințării este importantă, deoarece va fi factorul principal în adoptarea deciziei de către autorități, în legătură cu măsurile care urmează a fi întreprinse.

În consecință, informațiile asociate unei problematici ar trebui să fie procesate, evaluate şi analizate de o structură specializată. Rezultatul activității de procesare a informațiilor se materializează în produsele informaționale destinate factorilor decizionali stabiliți de lege potrivit principiului „nevoii de a şti" şi individualizate în documente şi forme de evidență specifice.

Un alt element foarte important care trebuie luat în calcul este beneficiarul final al analizei, în speță, decidentul politic care nu este întotdeauna familiarizat, cu subiectul analizei şi, implicit, cu situația în care trebuie să ia o decizie. În funcție de pregătirea profesională sau alte caracteristici de personalitate, decidentul trece produsul analitic prin propriul proces de analiză.

Provocarea – în ceea ce priveşte produsul finit – nu constă numai în a şti modalitatea de a furniza beneficiarului o anumită informație, dar şi în a organiza şi plasa informația respectivă în contextul, momentul, şi locul potrivite şi în detaliul corespunzător[8]. De aceea, decidentul şi analistul nu

[7] Steve Tsang, *Serviciile de informații şi drepturile omului în era terorismului global*, Editura Univers Enciclopedic, 2008, p. 259.
[8] Idem.

trebuie să perceapă situațiile analizate din perspective total diferite, ceea ce, mai ales în domeniul prevenirii şi combaterii terorismului, este vital.

Pentru o acțiune preventivă eficientă este vitală informarea cu operativitate şi în timp util a factorului de decizie. De altfel, avem convingerea că furnizarea operativă de astfel de documente (care includ evaluări periodice referitoare la situația internă, în domeniul antiterorist) rămâne preocuparea constantă a majorității structurilor cu responsabilități în domeniu.

Activitatea este dinamică, relaționarea cu beneficiarii informațiilor permite obținerea unui feedback şi, ulterior, formularea de noi nevoi de informare, precum şi reorientarea activității de informații în funcție de evoluția situației în domeniul antiterorist.

Integrarea informațiilor din toate sursele disponibile a fost dintotdeauna o provocare atât la nivelul instituțiilor cât şi în esența activității ca atare. Instituțional, activitatea era executată destul de bine, dar coordonarea şi integrarea aveau de suferit. Identificarea celei mai bune soluții pentru integrarea optimă a informațiilor disponibile relevante pentru un subiect sau set de subiecte date în evaluări analitice coerente şi utile beneficiarilor reprezintă cea mai importantă dilemă a analizei de intelligence contemporane.

Viabilitatea comunicării informațiilor depinde de existența unui sistem de comunicare eficient bazat pe canale de comunicații, mijloace, tehnici şi proceduri specifice între componentele cu atribuții în domeniul prevenirii şi combaterii terorismului, precum şi între structuri similare din sistemul securității naționale.

Centrele focale naționale pot asigura monitorizarea centralizată, continuă şi operativă a obiectivelor urmărite şi pot fi, implicit, un punct unic de gestionare a informațiilor din domeniul de referință, aflate în continuă expansiune în termeni de volum şi complexitate. Aceste centre sunt un avantaj indubitabil în lupta împotriva terorismului, în plan național, întrucât diminuează semnificativ posibilitatea unui eşec al analizei de *intelligence* pe fondul unei coordonări neunitare a informațiilor disponibile.

Procesul modern de analiză-sinteză, sprijinit de tehnologiile informaționale performante, este intrinsec legat de un management eficient al resurselor informaționale, care rămâne una dintre condițiile fundamentale pentru eficiența activității de informații şi – implicit – a măsurilor de prevenire şi contracarare a amenințărilor. Este, totodată, esențială găsirea

unui echilibru în folosirea resurselor informaționale, care să nu neglijeze o anumită categorie sau să profite în mod exagerat de o alta.[9]

În fine – dar nu în ultimul rând – evoluțiile înregistrate consolidează importanța analizei multisursă, ca instrument de procesare şi valorificare integrată a multitudinii de resurse informaționale aflate la dispoziția unei agenții de intelligence. Acest tip de analiză trebuie să includă şi capabilitățile specifice în domeniul surselor deschise, asigurând condițiile practice pentru îndeplinirea principalului deziderat al activității de informații pentru securitatea națională: asigurarea accesului la toate sursele de informații, integrarea tuturor elementelor de cunoaştere a unei situații generatoare de risc şi fundamentarea, în baza unei analize pertinente, a unor măsuri adecvate de prevenire sau contracarare a amenințării.

Bibliografie

1. Tiberiu Tănase, „Rolul şi atribuțiile de coordonare ale UE pentru combaterea terorismului", http://cssas.unap.ro/ro/pdf_carti/stratxxi_2007_vol2.pdfhttp://www.sie.ro/ Evaluari/ evaluari5.html.

2. Daniel Keohane, „The EU and counter-terrorism", http://www.cer.org.uk/pdf/ wp629_terrorism_ counter_keohane.pdf, May 2005.

3. Steve Tsang, *Serviciile de informații şi drepturile omului în era terorismului global*, Editura Univers Enciclopedic, 2008.

4. Ionel Marin, *Comunitatea de Informații, soluția problemelor de securitate*, Bucureşti, Editura Academiei Naționale de Informații *„Mihai Viteazul"*, 2004.

Laura-Loredana CHELMUŞ este absolventă a Academiei de Poliție „Alexandru Ioan Cuza" şi a urmat cursuri postuniversitare, specializarea relații internaționale. Este doctor în „informații şi ştiințe militare" şi specialist în analiza de intelligence.

[9] Ionel Marin, *Comunitatea de Informații, soluția problemelor de securitate*, Bucureşti, Editura Academiei Naționale de Informații *„Mihai Viteazul"*, 2004, p. 240.

Politica europeană comună de intelligence în impas?

Drd. Sorin APARASCHIVEI
Academia Națională de Informații *„Mihai Viteazul"*
e-mail: **saparaschivei@dcti.ro**

Abstract

The members of the European Union have good reasons to want to engage in intelligence sharing. Common policies, including the development of a single economy and common foreign policy, mean that the member states increasingly face similar threats to their internal and external security.

In this context it appears necessary to re-think the role of national intelligence agencies in the EU context and the possibility of enhancing multilateral intelligence cooperation.

It is not surprising, then, that they have developed institutions such as the Club of Berne, Europol, and the Military Staff to facilitate the exchange of intelligence.

But full and effective intelligence sharing requires that participants either hold a strong degree of trust in other participants' promises not to defect, or the creation of effective rules and institutions designed to counter concerns about such defection.

The available evidence indicates that mistrust is a substantial barrier to full sharing in the European Union. The member states have insisted that intelligence sharing remains voluntary, therefore, they have declined to create European institutions with the capacity to monitor and punish violations of promises to share, and in their public comments suggest that the trust among them is too low to allow full sharing.

Keywords: sharing intelligence, Club of Berne, Europol, intelligence cooperation.

Introducere

Este cert că, în momentul actual, Uniunea Europeană cu cele 27 de state şi aproape o jumătate de miliard de locuitori nu poate rămâne imună în fața consecințelor unor crize sau amenințări. Instituirea unui spațiu economic comun şi a unei piețe interne, libera circulație a persoanelor,

a mărfurilor şi a capitalului, au redus controlul naţional asupra activităţilor de frontieră, fapt ce a creat o anumită breşă de securitate, astfel că noile ameninţări încearcă să profite cât mai mult de situaţia creată. Toate aceste transformări au implicaţii majore pentru activitatea europeană de intelligence, întărind nevoia unei circulaţii a informaţiei secrete.

Evenimente şi procese, precum: căderea comunismului, schimbările politico-economice din Europa Centrală şi de Est, migraţia forţei de lucru, tensiunile din Balcani, atacurile şi ameninţările teroriste de la Madrid şi Londra, gripa aviară şi cea „porcină", sprijinul pentru miile de cetăţeni ai UE prinşi de tsunami în sud-estul Asiei sau pentru evacuarea acestora în timpul conflictului din Liban din anul 2006, criza gazelor ruseşti, criza economico-financiară actuală etc., au arătat că la nivelul Uniunii a fost creată, deja, o adevărată identitate de securitate societală[1].

În condiţiile în care chestiunea securităţii societale se află în răspunderea autorităţilor guvernamentale, firesc ar fi ca atunci când discutăm despre securitatea UE să înţelegem un sistem politic supranaţional bazat pe un set de tratate, instituţii, ierarhie şi proceduri. Atunci când au aderat la Uniune, statele membre au cedat de bunăvoie o parte a autorităţii şi suveranităţii naţionale ca semn al încrederii reciproce. Mai mult, prin Tratatul de la Lisabona, Uniunea Europeană a dobândit de la statele membre şi apanajul politicii externe şi securităţii comune.

Însă, chestiunea politicii externe şi a securităţii comune este legată indispensabil de existenţa unui intelligence eficient şi dinamic, de constituirea unor mecanisme instituţionale de cooperare şi schimb de informaţii.

Charles Baker, un analist al domeniului, consideră că intelligence-ul este fără echivoc legat de apărare, iar orice schimbare survenită în apărare implică şi schimbări în intelligence. Oriunde ar fi, superioritatea militară trebuie să fie completată cu capabilităţi de informaţii eficiente, în scopul prevenirii conflictelor sau câştigării bătăliilor. Baker dă ca exemplu EADS (Compania spaţială de apărare europeană) şi forţa europeană de reacţie rapidă, ca iniţiative unionale în domeniul apărării, care se potrivesc deja conceptului european de uniune şi consolidare[2].

---

[1] The Henry L. Stimson Center, *New Information and Intelligence Needs in the 21st Century Threat Environment*, Report no. 70, september 2008, disponibil: http://www.stimson.org/domprep/pdf/SEMA-DHS_FIIVAL.pdf.

[2] Charles Baker, *The search for a European intelligence policy*, Capitolul I, disponibil: http://www.fas/irp/eprint/baker.html.

De aceea, în noul context furnizat de Tratatul de la Lisabona, dar şi pentru a fi credibilă în exterior ca mare putere, UE trebuie să treacă printr-un amplu proces de restructurare instituțională care să aibă ca finalitate şi sporirea cooperării în domeniul intelligence-ului european. Ca niciodată, Uniunea Europeană are nevoie de structuri comune de intelligence, care să o protejeze şi care să-i dea capacitatea şi capabilitatea de a duce o politică externă viguroasă, în concordanță cu nevoile şi interesele statelor membre.

Argumente pentru o politică europeană comună de intelligence

Necesitatea unei politici europene comune de intelligence se referă la noile amenințări transnaționale, dar şi la problemele care țin de ordinea internă a acestui organism politic: nevoia de apărare în fața terorismului, a traficului cu diferite tipuri de arme, inclusiv a celor de distrugere în masă, acordarea de sprijin pentru activitățile diplomatice, asigurarea activității de contraspionaj, penetrarea agențiilor străine ostile, acordarea de sprijin împotriva activităților de crimă organizată, a traficului ilegal cu diferite substanțe etc.

Ca entitate colectivă, Uniunea Europeană are nevoie de suport informativ în negocierile economice guvernamentale, în probleme de contraspionaj economic şi apărare în fața competiției neloiale, în domeniul protejării infrastructurilor critice şi a corporațiilor de interes strategic, dar şi pentru monitorizarea entităților economice ostile sau pentru a sprijini companiile europene în efortul de a pătrunde pe alte piețe etc.

Totodată, cooperarea şi schimbul de intelligence sunt ocazii pentru națiunile cu resurse mai mici de a avea acces la surse importante de intelligence, beneficiile fiind evidente. Nicio agenție de intelligence nu poate face şi nu poate cunoaşte totul, de una singură. În momentul actual nu există nicio agenție națională europeană care să facă față exploziei informaționale globale. Potrivit lui John Roper, un academician de la Universitatea din Birmingham, bugetele însumate alocate agențiilor naționale de intelligence de statele UE s-ar ridica la o treime din suma alocată de SUA propriilor structuri[3]. În aceste condiții, individual, agențiile europene sunt puse în umbră de către cele americane.

Nu în ultimul rând, informația înseamnă şi putere. Cooperarea şi schimbul de intelligence pot aduce Uniunii o creştere a influenței politice

[3] Ibidem.

care poate decide, în beneficiul statelor membre, schimbarea cursului unor evenimente sau conflicte în desfăşurare pe scena internaţională.

Eforturi instituţionale privind cooperarea şi schimbul de intelligence

Una dintre întrebările la care Bruxelles-ul încearcă să răspundă este: Cum pot dezvolta statele membre iniţiative şi parteneriate în vederea unui intelligence unional şi cum pot facilita acest demers instituţiile UE?

Preocuparea, mai veche, s-a aflat şi în dezbaterea summit-ului UE de la St. Malo (1998) unde a fost adoptată o declaraţie privind apărarea europeană comună, în care se menţiona că „UE trebuie să aibă capacitatea de a acţiona autonom, să fie susţinută de o forţă militară credibilă, să fie pregătită şi capabilă de a răspunde crizelor internaţionale". Se avea în vedere ca UE să-şi dezvolte propriile structuri şi capacităţi de analiză, surse de intelligence şi capabilităţi de planificare strategică.

În consecinţă, Uniunea Europeană a urmărit extinderea sau crearea de noi instituţii care să încurajeze şi să faciliteze schimbul de informaţii între membri, cele mai importante fiind: Clubul de la Berna, Europol-ul şi Statul Major Militar al UE.

Clubul de la Berna a luat fiinţă în anul 1965 din nevoia unui schimb de intelligence între cele „şase state ale arcului alpin". Apoi, Clubul s-a extins şi a devenit o organizaţie elitistă de intelligence a statelor membre ale UE[4], la care s-au alăturat Elveţia şi Norvegia. Statele Unite au statut de observator în cadrul Clubului de la Berna, dar participă cu drepturi depline în problemele legate de combaterea terorismului.

Clubul a devenit un instrument de lucru împotriva terorismului, a criminalităţii organizate, interceptarea comunicaţiilor, criptare şi cyberterorism şi beneficiază de propria reţea de comunicaţii[5]. Conducerea organizaţiei este asigurată prin rotaţie, în tandem cu cea a Uniunii. Clubul de la Berna serveşte şi ca forum principal pentru contactul şefilor serviciilor de securitate naţională, aceştia întâlnindu-se regulat.

[4] În anul 2002 s-a decis ca, pe viitor, Clubul de la Berna să includă toţi membrii Uniunii Europene; conf: The new challenges facing European intelligence – reply to the annual report of the Council, A 48-a sesiune a Adunării WEU, 4 iunie 2002, Document A/1775, p. 10.

[5] Stéphane Lefebvre, „The Difficulties and Dilemmas of International Intelligence Cooperation", *International Journal of Intelligence and Counterintelligence*, 16, 2003, pp.530-531, disponibil la: http://www.scribd.com/doc4566522/Lefebvre-The-Difficulties-and-Dilemmas-of-International-Intelligence-Cooperation.

Sub auspiciile Clubului, a fost constituit Grupul pentru Combaterea Terorismului (*Counterterrorist Group* – CTG) în care statele membre, inclusiv SUA, realizează evaluări comune privind ameninţările, fac schimb de informaţii clasificate despre terorism şi se consultă reciproc. Şefii serviciilor de informaţii membre constituie comitetul de conducere al CTG, întâlnirile lor având loc la un interval de şase luni.

Clubul de la Berna a fost mandatat de UE să asigure îndrumare şi Europol-ului în probleme de contraterorism, UE şi NATO semnând un acord (2003) privind securizarea şi schimbul de informaţii între cele două organizaţii.

Clubul de la Berna nu are o agendă formală, publică, pentru activităţile sale, el îşi desfăşoară activitatea în afara instituţiilor UE[6]. „Baza legală" a Clubului este considerată „top secret".

Biroul European de Poliţie (Europol) şi-a început activitatea în anul 1999, organismul fiind înfiinţat în anul 1995 printr-o convenţie semnată de toate statele membre. Predecesorul Europol-ului a fost Grupul Trevi[7], creat în anii 1970 ca parte a Politicii Europene de Cooperare dar şi ca forum interguvernamental separat de Comisia şi Parlamentul European. Statele membre utilizau Grupul Trevi pentru a-şi coordona eforturile antiteroriste şi problemele traficului de frontieră.

Asemenea Clubului de la Berna, Grupul Trevi nu a avut o bază formală privind cooperarea şi schimbul de intelligence, ba mai mult nu a avut nici măcar un secretariat comun sau un staff şi nici nu era angajat în activităţi independente de intelligence.

Prioritățile Europol-ului se referă la combaterea traficului de droguri, traficului cu fiinţe umane, traficului ilegal cu autovehicule, migraţiei ilegale, terorismului, spălării şi falsificării banilor, cybercriminalităţii internaţionale. Europol furnizează *intelligence strategic* şi pregăteşte rapoarte generale. La cererea statelor membre, organizaţia constituie echipe ad-hoc pentru a colecta intelligence despre grupările teroriste.

---

[6] James Igoe Walsh, *Security Policy and Intelligence Cooperation in the European Union*, Paper prepared for the biennial meeting of the European Union, Studies Association, Los Angeles, aprilie 2009, p. 8, disponibil: http://www.unc.edu/euce/eusa.2009/papers/walsh-12c.pdf.

[7] Acronimul Trevi provine de la cuvintele: Terrorisme, Radicalisme, Extrémisme et Violence Internationale.

Obiectivul major al Europol-ului este acela de a îmbunătăți schimbul de intelligence[8], de a încuraja diseminarea intelligence-ului între statele membre şi de a notifica statele atunci când informațiile furnizate şi-au dovedit utilitatea şi valoarea în cazuri concrete.

Staff-ul Europol-ului numără aproximativ 65 de analişti, la care se adaugă ofițerii care asistă deciziile pentru guvernele naționale. Fiecare stat membru este reprezentat la cartierul general al organizației de către un ofițer de legătură, responsabil de cererea şi furnizarea de intelligence între Europol şi guvernul național şi invers. Cheia acestui schimb de intelligence poartă denumirea de Sistemul Informatic European (TECS), el conține două tipuri de intelligence:

1) Europol Information" care centralizează informații despre indivizi şi grupuri suspecte;

2) „Dosarele de lucru" referitoare la informații şi activități specifice întocmite de către staff-ul Europol şi ofițerii de legătură.

În ianuarie 2010, prin decizia Consiliului UE, Europol a fost ridicat în rang, devenind agenție a UE. Noul cadru legal aduce o sporire a responsabilităților, un buget propriu, iar la nivel de decizie procedura a fost simplificată prin introducerea votului majoritar cu două treimi din totalul de membri. Preşedintele va fi ales pe o perioadă de 18 luni şi va fi sprijinit de un grup format din trei state membre. Se aşteaptă ca Europol-ul să fie capabil să furnizeze statelor membre intelligence şi analize în legătură cu evenimente internaționale majore, beneficiind în acest sens de un nou sistem IT şi de accesul la noi surse de informații (inclusiv informații furnizate de surse private).

Cea de-a treia instituție a intelligence-ului european, menită să sprijine Politica Europeană de Apărare şi Securitate, este Statul Major Militar al Uniunii Europene, care operează sub coordonarea directă a Comitetului Militar. Acesta include şi Departamentul de Intelligence responsabil cu avertizările timpurii, întocmirea evaluărilor şi asigurarea suportului operațional în securitatea externă pentru probleme care includ terorismul.

Fiecare stat membru a desemnat cel puțin un ofițer care lucrează cu Comitetul Militar şi care asigură legăturile de comunicare cu agențiile naționale de securitate. Departamentul de Intelligence al Comitetului

[8] La 1 octombrie 2009, Europol şi Eurojust au încheiat un acord privind cooperarea în schimbul de intelligence.

utilizează informaţiile furnizate de statele membre, produce intelligence şi evaluări proprii, la care se adaugă informaţiile procesate de instituţiile europene. Toate acestea pentru a sprijini Comitetul Militar, Înaltul Reprezentant pentru Afaceri Externe, precum şi celelalte instituţii europene.

Un rol important în informarea Comitetului Militar revine şi intelligence-ului de la SitCen[9], care informează decidenţii politici despre ultimele tendinţe în privinţa ameninţărilor şi riscurilor. Anterior anului 2005, SitCen era focusat exclusiv pe ameninţările provenite din afara UE, dar în ultimii ani acesta şi-a concentrat atenţia pe ameninţările din interiorul Uniunii, devenind una dintre cele mai de încredere surse UE pentru analiştii terorismului strategic.[10] SitCen-ul combină informaţiile adunate la nivel naţional de serviciile de informaţii interne şi externe cu cele furnizate de Clubul de la Berna. Analizele sunt adesea distribuite şi Europol-ului.

Problemele cooperării actuale – soluţii propuse

Spre deosebire de multe alte domenii (economic, social, cultural, politic etc.), cooperarea europeană în domeniul intelligence a fost limitată de ascendenţa suveranităţii naţionale asupra schimbului de informaţii.

Piedicile se datorează numeroaselor suspiciuni legate de domeniul sensibil al activităţii informative, printre acestea numărându-se problema schimbului de informaţii operative, protecţia surselor şi a metodelor, diseminarea informaţiilor către terţi, secretul tehnologic, folosirea informaţiilor în alte scopuri etc.

Există contradicţii şi cu privire la modul de abordare a relaţiilor UE cu lumea musulmană sau chiar cu Federaţia Rusă. Sunt state membre care au afinităţi speciale cu cei din afara Uniunii, de natură politică, economică sau culturală, de care ceilalţi membri trebuie să ţină seama. Apoi, lipsa de omogenitate internă în distribuţia puterii este de natură să nască alte suspiciuni şi acuzaţii de inechitate. Abordări diferite, fie şi nuanţate, există şi în domeniul legalităţii şi respectării drepturilor fundamentale ale omului. De pildă, problema protecţiei datelor personale şi a interceptării corespondenţei.

[9] SitCen – Centrul de Situaţii este structura responsabilă de asigurarea operativă de informaţii, analize şi avertizare timpurie, pe bază de resurse deschise sau clasificate, provenite din partea statelor membre sau a instituţiilor europene.
[10] The Henry L. Stimson Center, op. cit.

La ora actuală, din cauza neîncrederii reciproce, Uniunea nu are la dispoziție un mecanism coerent, instituționalizat, care să monitorizeze şi să controleze procesul de intelligence. Nu există un cadru juridic comun care să pedepsească abuzurile şi neîndeplinirea obligațiilor asumate. Uniunea Europeană nu are un rol direct în asigurarea securității statelor membre. Instituțiile UE nu sunt angajate activ, zi de zi, în activități de prevenire a atacurilor teroriste sau a altor amenințări.

Rapoartele de constatare indică faptul că membrii UE nu par a se folosi de Clubul de la Berna pentru colaborări şi schimburi semnificative în domeniul informațiilor operative. Clubul este utilizat mai mult doar pentru a împărtăşi idei despre instrumente şi politici folosite împotriva noilor amenințări sau pentru a înțelege mai bine perspectivele etc.

Demoralizator este că nici „viitorul nu sună bine". Deşi Clubul de la Berna a planificat ca în următorii cinci ani să-şi constituie propria bază de date privind terorismul şi crima organizată, demersul se anunță a fi unul de pionierat, deoarece baza respectivă nu va conține informații sensibile, ci doar „intelligence contextual" privind suspecții.[11] Practic, nu există pretenția sau aşteptarea ca un stat membru să dorească să difuzeze din informațiile sensibile deținute.

Schimbul voluntar de intelligence înseamnă că nu există o cale directă pentru statul receptor de a-şi asigura necesarul de informații relevante, nu există certitudinea că va intra la timp în posesia acestora şi nu se poate determina dacă şi cât din intelligece-ul respectiv a fost modificat sau distorsionat în scopul servirii interesului furnizorului. Totuşi, de regulă activitatea şi evaluările produse de staff-ul şi ofițerii de legătură ai Clubului de la Berna, Europol-ului şi Comitetului Militar permit detectarea unor intoxicări deliberate, însă nu există garanții în sensul acesta[12].

Europol-ul şi-a detaliat restricțiile față de modul în care poate fi accesat un dosar. Dacă analiza este de natură generală, ea poate fi accesată de toți membrii. Dacă este un caz specific, el va fi preluat doar de cei implicați. Terții au acces la dosar numai dacă există consensul părții implicate. Însă, statele membre pot refuza colaborarea informativă cu Europol-ul, dacă se consideră că le sunt periclitate interesele esențiale de securitate națională.

[11] James Igoe Walsh, op. cit.
[12] Ibidem, p.17.

Schimbul de informaţii via Departamentul de Intelligence şi Comitetul Militar prezintă la fel de multe probleme ca şi cele ale Clubului de la Berna şi Europol-ului. Practica Departamentului de Intelligence de a colecta intelligence sensibil, furnizat de către autorităţile naţionale şi de a-l folosi la realizarea unor analize adiţionale cu caracter general, poate genera anumite suspiciuni privind deconspirarea şi identitatea surselor, fapt ce pune adesea în situaţii delicate agenţiile naţionale. Apoi, nu toate statele au capacităţile şi capabilităţile necesare demersului. Puţine state ale Uniunii au şi servicii de informaţii externe, cu sursele aferente, care pot acoperi evoluţiile internaţionale transmiţând intelligence către Departamentul unional.

Uniunea Europeană dispune totuşi de propriile capabilităţi de colectare şi analiză de intelligence, chiar dacă acestea sunt modeste în comparaţie cu cele ale statelor membre.

Uniunea întreţine misiuni diplomatice peste tot în lume şi are desemnaţi reprezentanţi speciali pentru diferite crize şi regiuni, precum Balcanii, Caucazul, Africa şi Orientul Mijlociu. Aceştia sunt capabili să colecteze în mod deschis informaţii din surse guvernamentale, publicaţii etc., iar prin contactele lor locale pot, ocazional, să obţină şi informaţii confidenţiale. Reprezentanţii Uniunii, asemenea oficialilor care activează în serviciile de informaţii, cunosc foarte bine ce înseamnă formulele politice, politica dusă în spatele uşilor închise, şcolile şi curentele de gândire, camarilele şi facţiunile politice, grupurile de interese transnaţionale, conexiunile şi interdependenţele internaţionale etc. De multe ori, aceştia au oportunităţi unice de a vedea lumea altfel de cum se înfăţişează ea decidenţilor politici sau oamenilor obişnuiţi. Însă, statutul diplomatic nu le permite să se angajeze în activităţi sistematice de colectare şi analiză de intelligence.

În raportul său pentru UE, James Walsh[13] atrage şi el atenţia că, în prezent, schimbul şi cooperarea în intelligence se bazează doar pe bunăvoinţa statelor membre. El consideră că problema ar putea fi rezolvată prin mecanismul unei mai bune integrări, prin delegarea de către state a unor puteri către Uniunea Europeană. Walsh dă ca exemplu Comisia Europeană

[13] James Igoe Walsh, *Security Policy and Intelligence Cooperation in the European Union*, aprilie 2009, disponibil: http://www.unc.edu/euce/eusa.2009/papers/walsh-12c.pdf; J.I. Walsh este profesor la Department of Political Science, University of North Carolina at Charlotte.

şi Curtea de Justiţie, instituţii care se asigură că statele membre implementează şi îndeplinesc cu bună credinţă obligaţiile asumate, fără discriminare.

Soluţia avansată se referă la imaginarea unei „organizaţii europene" (unionale), însărcinată cu activităţi de monitorizare şi culegere de intelligence, care să colaboreze şi să schimbe informaţii cu serviciile naţionale de intelligence şi care să se asigure că acestea îşi vor îndeplini cu bună credinţă obligaţiile de a furniza toate informaţiile relevante către toţi partenerii. Primul pas, ar consta în a cere în mod explicit şi imperativ tuturor statelor membre să schimbe informaţii relevante, deci nu voluntar; următorul pas, este de a aloca acestei agenţii resursele şi posibilitatea de a monitoriza statele membre, în scopul asigurării că ele se achită de obligaţii. Sunt necesare garanţii solide că statul furnizor nu a „modificat" informaţia, că se asigură comunicarea surselor şi a mijloacelor, că informaţiile nu ajung la alţi destinatari sau că vor fi folosite în alte scopuri. La ora actuală, Departamentul de Intelligence al UE primeşte din partea statelor membre foarte puţine date „neprocesate", majoritatea intelligence-ului fiind „finisat", ceea ce înseamnă că detaliile sensibile, sursele şi metodele folosite la colectare au fost „mascate". De aceea, obligaţia de a schimba intelligence va cere Uniunii Europene capabilitatea de a procesa şi analiza întreaga cantitate de informaţii colectată de statele membre şi de a supraveghea operaţiunile şi procedurile de securitate internă.[14]

James Walsh, dar şi alţii, consideră că, în prezent, doar anumite state din cadrul Uniunii au capacitatea de a coordona sau de a conduce acest demers, deoarece un asemenea stat trebuie să îndeplinească o serie de condiţii. În primul rând, acesta trebuie să participe activ la proiect şi să fie în stare să exercite presiuni în vederea implementării acordurilor privind schimbul de intelligence. În al doilea rând, statul respectiv trebuie să convingă ceilalţi membri de necesitatea implicării şi a finanţării proiectului, să garanteze că integrarea le va aduce beneficii substanţiale şi riscuri minime. Şi nu în ultimul rând, trebuie asigurată independenţa mecanismului faţă de orice presiune politică, deoarece numai aşa va fi obţinută încrederea şi cooperarea tuturor membrilor.

La ora actuală Uniunii Europene îi lipseşte, însă, un asemenea membru care să îndeplinească toate criteriile enumerate, dar există cel puţin trei state care ar putea să se apropie de aceste condiţii: Marea Britanie,

[14] Ibidem, pp. 21-22.

Franța şi Germania – participarea lor fiind, probabil, vitală pentru un acord european în domeniu. Cele trei state au capacități mari şi diversificate, atât pentru intelligence-ul național, cât şi pentru cel extern, şi greu se poate imagina o asemenea organizație fără participarea totală a acestora.

Dar dacă procesul integrării nu reuşeşte pe deplin?

Una dintre soluțiile vehiculate ar fi aceea ca statele membre să se grupeze în funcție de interesele comune. Demersul ar însemna dezvoltarea unor „relații speciale" între statele membre cu suficientă încredere reciprocă în a-şi împărți „secretele" şi interesele, care se pot angaja în schimbul de intelligence prin excluderea celorlalți. Astfel, se pot coaliza grupuri informale focusate pe anumite probleme (cooperare consolidată). Statele respective vor „înțelege" mai bine interesele partenerilor, ducând indirect la sporirea schimbului de intelligence şi în viitor la facilitarea unor înțelegeri pentru toate statele membre.

Deşi sunt voci care contestă acest tip de cooperare (integrare în mai multe viteze) pe motiv că el nu prezintă la fel de multă eficiență aşa cum ar putea fi în cazul deplinei integrări, există deja state membre cu interese similare şi capacități mai dezvoltate care se întrunesc pentru a schimba intelligence operativ. Acestea şi-au stabilit diverse aranjamente ad hoc, cum ar fi acela de a urmări grupările teroriste care operează pe teritoriul lor. Astfel, înaintea întrunirii în cadrul Consiliului pentru Afaceri Interne şi Justiție, miniştrii de interne din Marea Britanie, Franța, Germania, Spania şi Italia se întâlnesc regulat pentru a discuta problemele şi a-şi preciza poziția comună. Apoi, prin persuasiune, membrii acestui grup îi determină pe ceilalți să adopte aceleaşi poziții. Practica a demonstrat că acest veritabil „G5" este mult mai eficace decât dacă s-ar fi acționat în mod singular, fiind de notorietate buna colaborare împotriva terorismului şi a altor amenințări între serviciul britanic (MI5), serviciul francez (DST) şi serviciul german (BfV). Nu întâmplător, pe acest model, cooperarea dintre DST-ul francez şi CIA a fost catalogată de americani ca fiind „cea mai bună din lume".[15]

O altă soluție, ar fi ca statele membre să se inspire din experiența fostului Imperiu roman. Asemenea UE, Imperiul roman era un organism politic extins şi destul de eterogen. Pentru a contracara diversele amenințări la securitatea sa, statul roman şi-a împărțit armata în două componente:

[15] Hugo Brady, *Intelligence, emergencies and foreign policy: The EU's role in counter-terrorism*, Published by the Centre for European Reform (CER), 14 Great College Street, London, iulie 2009, pp. 4-6, disponibil: http://www.cer.org.uk/pdf/essay-912.pdf.

centrală şi de graniță (regionale). Experiența dobândită în teatrele de luptă a demonstrat decidenților romani că amenințările, interne sau externe, pot fi rezolvate mai eficient şi rapid de către un corp de armată deja familiarizat cu situația din zona amenințată. Doar în cazul unui atac masiv, căruia armata de graniță nu-i putea face față, organismul statal central roman se mobiliza şi intervenea direct pentru a rezolva situația. Această practică, a delegării de atribuții şi responsabilități de la nivel central la nivel local, este cunoscută astăzi în cadrul UE sub numele de „principiul subsidiarității".

Astăzi, nu întâmplător, constatăm că timidele realizări în domeniul schimbului european de intelligence par a fi legate tocmai de aplicarea acestui vechi principiu. Serviciile naționale de intelligence au devenit destul de refractare atunci când li s-a cerut în mod imperativ să coopereze. Nu acelaşi lucru s-a întâmplat atunci când, urmând principiul subsidiarității, UE a încredințat atribuții şi sarcini agențiilor naționale în deplină libertate şi independență. Bineînțeles, logic şi eficient ar fi ca sarcinile şi atribuțiile să fie delegate în funcție de specificul fiecărui stat membru, de zona geografică şi poziția ocupată la frontiere, precum şi de originea, natura şi nivelul amenințărilor la adresa UE.

De altfel, Comisia Europeană sugera, încă din anul 1975, că Uniunea Europeană nu trebuie să conducă la realizarea unui super-stat centralizat, nu vor fi atribuite Uniunii decât sarcinile pe care statele membre nu le vor putea îndeplini în mod eficace. Să nu uităm nici faptul că Tratatul de la Lisabona este foarte restrictiv în privința politicii externe şi de securitate comună. Sarcina Uniunii fiind doar aceea de a defini orientările generale în domeniu (art. 12, a)[16]. Practic, Uniunea ca autoritate centrală nu poate interveni foarte mult la nivelul intelligence-ului local sau regional.

Printre cei care au criticat actualul impas al colaborării europene se numără şi coordonatorul UE pe probleme de contraterorism, Gilles de Kerchove. La mijlocul anului 2009, el considera că statele membre au eşuat deja în demersul de implementare a legilor destinate combaterii grupurilor teroriste, inclusiv a legilor privitoare la spălarea banilor, a arhivării datelor din telecomunicații, cybercriminalității şi a înghețării fondurilor şi proprietăților ilicite din străinătate. Eşecul este explicat prin faptul că UE, prin coordonatorul respectiv, nu poate să impună politici sau să oblige un stat membru să implementeze legislația unională în domeniu aşa cum face,

[16] Tratatul de la Lisabona, disponibil la: http://eur-lex.europa.eu/LexUriServ/.

de exemplu, Comisia Europeană în reglementarea pieței interne, cu toate că sarcina oficialului UE este tocmai aceea de a stimula cooperarea informativă împotriva amenințărilor comune a guvernelor statelor membre cu instituții precum Europol şi SitCen. Conform lui Kerchove, „fiecăruia îi place să coordoneze dar nimănui nu-i place să fie coordonat".[17] Ca soluție, el a recomandat ca toate statele membre să demareze „centre de fuzionare", asemănătoare Centrului britanic de analiză a terorismului (JTAC), Centrului german de contraterorism (GTAZ) sau Centrului francez de coordonare antiteroristă (UCLAT).

Preocupări interesante în domeniul schimbului de intelligence regăsim şi la specialistul Hugo Brady de la Centre for European Reform. Brady observă că Franța este considerată a fi un model de succes în prevenirea terorismului[18]. Explicația constă în faptul că statul are puteri sporite în a reține suspecții şi în a intercepta convorbiri private, puteri care în alte state democratice sunt considerate a fi excesive. Mai mult, procurorii au la dispoziție un cadru legal destul de larg, aşa-numitele legi conspirative, care le permite să ancheteze orice intenție a unui act terorist. Oficialii francezi sunt de părere că această combinație a puterilor legale a contribuit la succesul țării lor în prevenirea atacurilor teroriste. Realizările francezilor se bazează pe cooperarea dintre serviciile de intelligence, poliție şi procurori, care lucrează împreună pe tot parcursul anchetei. Investigațiile antiteroriste sunt apoi centralizate în mâna unui magistrat (unic), desemnat special pentru terorism. Acesta se poate adresa direct Poliției, Jandarmeriei şi Direcției Generale a Securității Externe (DGSE). Menționăm că, la acest succes e posibil să fi contribuit şi reforma din anul 2008, prin care Direcția Generală de Informații a Poliției franceze s-a unificat cu Direcția de Supraveghere a Teritoriului (DST), formând Direcția Centrală de Informații Interne (DCRI) cu atribuții depline privind contraspionajul, contraterorismul şi supravegherea potențialelor amenințări asupra teritoriului francez.

Prin contrast, absența unei astfel de ierarhii clare este una din principalele probleme în eforturile antiteroriste din multe state europene şi din SUA.

[17] Hugo Brady, op. cit., p. 18.
[18] Ibidem, pp. 4-20.

Între timp, inspirându-se din modelul francez, Marea Britanie a încercat să implementeze sistemul şi a instituit un responsabil guvernamental la Poliția Metropolitană din Londra pentru a coordona investigațiile naționale împotriva terorismului; de asemenea, britanicii au încercat (fără succes) să extindă perioada de detenție pentru suspecții de terorism la 42 de zile.

O altă problemă este legată şi de atribuțiile agențiilor de intelligence. Spre deosebire de FBI american, cele mai multe servicii naționale de intelligence din statele Uniunii nu au puteri în privința arestării şi detenției. Activitatea acestora constă doar în a obține cât mai multe informații posibile, după o îndelungată şi sofisticată perioadă de supraveghere şi monitorizare. Prin contrast, poliția, care are puteri în privința arestului şi a detenției, va dori să acționeze imediat încă de la primele informații privind amenințarea. Astfel, diferența de abordare dintre cele două organizații creează o anumită reținere a serviciilor de intelligence în a distribui informații către poliție încă din faza incipientă a amenințării, din teama de a nu fi distruse conexiunile cazului respectiv. Aşa se explică faptul că, deşi, în Marea Britanie forțele de poliție şi serviciile de intelligence sunt destul de numeroase prevenția unor atacuri lasă de dorit, sau cazul Spaniei, unde lipsa de relaționare interagenții a împiedicat eforturile antiteroriste. Insurmontabilă pare a fi şi situația când statul este o republică federală alcătuită din mai multe state, fiecare cu propriile structuri independente de securitate, cum este cazul Germaniei. Aici, recent a fost stabilită o anumită ierarhizare între structurile de securitate federale şi cele statale, deşi constituția interzice deplina centralizare a puterilor în materie de securitate.

În pofida acestor neconcordanțe, din cauza luptei împotriva terorismului internațional, ministerele de interne din Marea Britanie, Germania, Franța, Italia, Polonia, Spania, Olanda sau Danemarca au fost implicate tot mai mult în activități de intelligence, constituindu-şi adevărate sisteme naționale de luptă antiteroristă. Asta înseamnă că ministerele din statele respective au agenții şi resurse specifice alocate culegerii de informații, ele pot răspunde rapid în eventualitatea unui atac terorist pentru a proteja civilii şi infrastructura şi, de asemenea, ele şi-au integrat prioritățile antiteroriste în politica lor externă.

În Marea Britanie, serviciul de poliție joacă un rol tot mai important în sprijinirea celor patru piloni ai Strategiei de luptă contrateroristă (CONTEST) – protecție, prevenire, pregătire şi urmărire. Întrucât poliția are o mai bună cunoaştere a străzii, a comunității şi a vecinilor, a interacțiunilor

zilnice, s-a considerat că eşecul de intelligence este mai puţin probabil dacă ar exista o colaborare mai strânsă între poliţie şi agenţiile de intelligence. Astfel, guvernul britanic a crescut continuu responsabilităţile poliţiei în materie de securitate naţională, în parteneriat cu celelalte agenţii de securitate. Nu numai că a fost construită o nouă conlucrare între instituţiile de ordine publică şi serviciile speciale, dar s-a construit şi o nouă relaţie de încredere reciprocă între comunitatea de intelligence şi parteneri nontradiţionali, precum sectorul privat şi autorităţile locale. Avem de a face cu o „spargere" a monopolului intelligence-ului guvernamental, care acum s-a mutat spre sectorul privat cu beneficii în planul securităţii naţionale[19].

În acest context, ministerele de interne ale statelor UE au depus eforturi pentru a-şi armoniza legislaţia privind definirea ameninţărilor teroriste (măsură necesară poliţiei în urmărirea internaţională a teroriştilor), fiind accelerată şi procedura de extrădare a suspecţilor între membrii UE.

De altfel, începând cu acest an (2010), noi reguli vor reglementa activitatea ofiţerilor europeni de poliţie. Ei vor avea acces la baze electronice comune de date, care vor lega ministerele de interne ale statelor membre; la rândul lor, aceştia vor trebui să alimenteze în timp util aceste baze cu informaţiile pe care le deţin. Bazele respective vor fi asemănătoare Sistemului Informatic Schengen şi vor fi dotate la cel mai înalt nivel tehnologic[20]. Toate acestea, pe fondul intrării în vigoare a Tratatului de la Lisabona care prevede ca Uniunea şi statele membre să acţioneze în spirit de solidaritate în cazul în care un stat membru este ţinta unui atac terorist. Se pare că respectiva „clauză de solidaritate" va „obliga" statele membre la sporirea cooperării şi schimbului de intelligence, conform principiului clasic: este mai uşor să previi decât să combaţi.

Totodată, se mizează şi pe întărirea relaţiilor dintre serviciile de informaţii ale UE cu cele americane. Se aşteaptă ca la summit-ul UE-SUA din acest an (2010), sub preşedinţia Spaniei, să fie adoptată o strategie antiteroristă care să includă o mai bună cooperare între FBI şi Europol, respectiv între CIA şi SitCen. Acordul se referă şi la schimbul de informaţii privind pasagerii, protecţia datelor şi monitorizarea tranzacţiilor financiare internaţionale.

---

[19] Kevin A. O'Brien, *The Changing Security and Intelligence Landscape in the 21st Century*; apărut la: International Centre for the Study of Radicalisation and Political Violence (ICSR), King's College London, octombrie, 2008, pp. 2-4, disponibil: http://www.icsr.info/publications/papers/ 1236602590ICSRKevinOBrienReport.pdf.

[20] Hugo Brady, op.cit. p. 18.

Concluzii şi implicaţii

Teoretic, membrii Uniunii Europene au cele mai bune motive pentru a se angaja şi a coopera în schimbul de intelligence. Politicile comune, piaţa economică internă şi politica externă şi de securitate comună fac ca în domeniul securităţii statele membre să se confrunte cu ameninţări similare.

Pentru a se apăra, membrii UE au decis să faciliteze cooperarea şi schimbul de intelligence dezvoltând instituţii comune, precum Clubul de la Berna, Europol şi Comitetul Militar. Însă, funcţionarea eficientă a acestora presupune sporirea încrederii reciproce, garanţii comune, impunerea unor reguli şi obligaţii, crearea unor instituţii destinate să monitorizeze şi să controleze acest proces.

Experienţa europeană de până acum indică „lipsa de încredere" ca fiind principalul obstacol în schimbul de intelligence. Statele membre au insistat ca acest schimb să fie voluntar, evitând să se implice în crearea unor mecanisme instituţionale de monitorizare şi control.

În prezent, instituţiile europene de intelligence nu au capacitatea şi nici dreptul de a stopa „defectarea" sau încălcarea „înţelegerilor convenite". Ele s-au angrenat doar în construirea de mecanisme tehnice – baze de date, întruniri regulate, mijloace de legătură – care să faciliteze schimbul de informaţii între statele membre.

Nu ne rămâne decât să sperăm că decidenţii politici europeni au învăţat lecţia trecutului şi că necesităţile impuse de intrarea în vigoare a Tratatului de la Lisabona şi situaţia internaţională vor accelera acest demers deosebit de complex.

P.S. Cotidianul „International Herald Tribune" ne informează că la „Dezbaterea online pe probleme de securitate – 2010", ţinută sub „egida NATO, UE, a guvernelor şi a grupurilor de analiză", una dintre recomandări a fost ca UE să-şi creeze „propria agenţie de informaţii".[21]

Bibliografie

1. Politi, Alessandro, *Towards a European Intelligence Policy*, Institute for Security Studies, Western European Union, Paris, Chaillot Papers 34, 1998.

2. Aldrich, R. J., *Transatlantic intelligence and security cooperation*, International Affairs, 80 (4), 2004.

[21] Steven Erlanger, „NATO şi UE vor să pună la punct noi concepte strategice", cotidianul *International Herald Tribune* (Statele Unite ale Americii), 6 mai 2010.

3. Born, Hans, *International Intelligence Cooperation: The Need for Networking accountability*, Speaking notes for Hans Born (Senior Fellow, DCAF, Geneva), 2007.

4. NATO Parliamentary Assembly Session at Reykjavik.

5. The Henry L. Stimson Center, *New Information and Intelligence Needs in the 21st Century Threat Environment*, Report no. 70, september, 2008, disponibil: http://www.stimson.org/domprep/pdf/SEMA-DHS_FIIVAL.pdf.

6. Baker, Charles, *The search for a European intelligence policy*, 2001, disponibil: http://www.fas/irp/eprint/baker.html.

7. *The new challenges facing European intelligence – reply to the annual report of the Council*, a 48-a sesiune a Adunării WEU, 4 iunie 2002, Document A/1775.

8. Lefebvre, Stéphane, „The Difficulties and Dilemmas of International Intelligence Cooperation", *International Journal of Intelligence and Counterintelligence*, 16, 2003, disponibil la: http://www.scribd.com/doc4566522/Lefebvre-The-Difficulties-and-Dilemmas-of-International-Intelligence-Cooperation.

9. Walsh, James Igoe, *Security Policy and Intelligence Cooperation in the European Union*, Paper prepared for the biennial meeting of the European Union, Studies Association, Los Angeles, 2009, disponibil: http://www.unc.edu/euce/eusa.2009/papers/walsh-12c.pdf.

10. Brady, Hugo, *Intelligence, emergencies and foreign policy: The EU's role in counter-terrorism*, Published by the Centre for European Reform (CER), 14 Great College Street, London, 2009, disponibil: http://www.cer.org.uk/pdf/essay-912.pdf.

11. *Tratatul de la Lisabona*, disponibil la: http://eur-lex.europa.eu/LexUriServ/.

12. Kevin A. O'Brien, *The Changing Security and Intelligence Landscap in the 21st Century*; apărut la: International Centre for the Study of Radicalisation and Political Violence (ICSR), King's College London, 2008, disponibil: http://www.icsr.info/publications/papers/1236602590ICSRKevinOBrienReport.pdf.

13. Villadsen, Ole. R., *Prospects for a European Common Intelligence Policy*, 2007, http://209.85.129.132/search?q=cache:_4XYDPsdyA0J:https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csistudies/studies/summer00/art07.html+for+a+European+intelligence+policy&cd=2&hl=ro&ct=clnk&gl=ro&client=firefox-a.

Sorin APARASCHIVEI este doctorand la Universitatea din Bucureşti, Facultatea de Istorie, master în Drept Internațional şi Comunitar, licențiat în Ştiințe Politice şi Istorie. Este autor/coautor de studii, documentare şi comunicări ştiințifice în domeniul securității şi intelligence-ului, publicate în diverse reviste de specialitate.

Reconfigurări sistemice ale Comunității americane de Informații din perspectiva *„creării avantajului decizional”*

Corin VÎLCEANU
Ioana BELCIU
Serviciul Român de Informații
e-mail: **ani@sri.ro**

Abstract

In July 2008, the Office of the Director of National Intelligence released a document entitled "Vision 2015". The vision charts a new path forward for a globally networked integrated Intelligence Enterprise for the 21st century, based on the principles of integration, collaboration and innovation and establishes some core concepts.

This article reveals the present concerns in the US National Intelligence Community regarding new means of remodeling intelligence structures by adapting them to the realities of the security environment in order to provide decision advantage to the decision-makers (policymakers, military commanders, law enforcement and homeland security officials).

Keywords: modeling intelligence structures, US Intelligence Community.

Prefigurarea schimbării priorităților Comunității americane de Informații

Momentul 11 septembrie 2001 a determinat reconsiderarea unor concepții şi structuri funcționale, precum şi schimbări semnificative în privința priorităților informative şi a reformei sistemice a Comunității americane de Informații (CI), aflate, de un deceniu în stadiul de intenție. Drept urmare, în 2004, a fost creată funcția de Director al Comunității de Informații (DNI) în încercarea de a unifica şi consolida agențiile de informații americane şi de a le forța să realizeze schimbul de informații necesar îndeplinirii noilor obiective de securitate națională.

CI a fost înființată în 1947, odată cu adoptarea Legii Securității Naționale, deşi fusese deja concepută la 7 decembrie 1941, în urma atacului surpriză de la Pearl Harbor şi a luat forma sa actuală abia în 1981.

La 3 februarie 2010, fostul director al Comunității de Informații a Statelor Unite, Dennis Blair, a prezentat în fața Comisiei Speciale a Senatului raportul privind *„Evaluarea anuală a amenințărilor la adresa securității naționale"*[1]. Raportul DNI concluzionează: *În urmă cu un an, economia globală, aflată într-o situație în degradare, amenința să atragă după sine o instabilitate politică generalizată. Sunt bucuros să vă informez că, deşi redresarea economică rămâne în continuare slabă, norii care umbreau perspectiva strategică în acest domeniu s-au risipit parțial. În pofida nenumăratelor incertitudini şi a provocărilor continue, situația economică şi politică cu care ne confruntăm astăzi ar fi putut fi mult mai gravă în cazul în care căderea economică liberă nu ar fi fost stopată. Aşa cum am arătat în urmă cu un an, mediul internațional de securitate este complex. SUA nu se confruntă cu niciun adversar dominant care să-i amenințe existența prin forța militară. Mai degrabă, complexitatea problemelor şi multitudinea actorilor – statali şi nonstatali – constituie, din ce în ce mai mult, una din cele mai mari provocări cu care ne confruntăm*[2].

Demisia lui Blair (la sfârşitul lunii mai a acestui an), după 16 luni de mandat, a survenit după o perioadă tulbure în activitatea serviciilor secrete americane, marcată de eşecuri precum tragedia de la baza militară Fort Hood (Texas), atentatul de la bordul avionului de pe ruta Amsterdam-Detroit, maşina capcană din Times Square (New York), ce au demonstrat că, în realitate, colaborarea dintre serviciile CI nu funcționează.

În luna decembrie 2009, cetățeanul nigerian Umar Farouk Abdulmutallab, în vârstă de 23 ani, a reuşit să urce la bordul unei aeronave a companiei Northwest Airlines cu material explozibil, în pofida măsurilor antiteroriste extrem de stricte impuse în aeroporturi. Presa americană a dezbătut pe larg declarațiile consilierului preşedintelui american, specializat pe probleme de securitate, John Brennan, potrivit căruia *nu a existat nicio informație care să fi permis să ştim că Abdulmutallab va comite acest atentat la bordul acestui avion*[3]. Totodată, potrivit oficialului, tatăl

[1] „Annual Threat Assesment of the United States Intelligence Community for the Permanent Select Commitee of Intelligence" (3 februarie 2010) publicat pe https://www.dni.gov/testimonies/ 20100203_testimony.pdf.
[2] Ibidem, p. 45.
[3] „SUA nu putea preveni tentativa de atentat de pe 25 decembrie" publicat pe http://www.evz.ro/detalii/stiri/sua-nu-putea-preveni-tentativa-de-pe-25-decembrie-881358.html, 4 ianuarie 2010.

atentatorului ar fi avertizat forţele de securitate din SUA cu privire la plecarea tânărului în Yemen unde intrase în contact cu extremişti. Consilierul preşedintelui a fost obligat să admită că sistemul de alertă teroristă nu a funcţionat.

Comisia pentru Informaţii a Senatului a apreciat, în raportul emis la 1 mai 2010, că *greşeli sistematice ale serviciilor* [4] au permis nigerianului să urce la bordul aeronavei şi să detoneze explozibilul.

În publicaţia *Studies in intelligence*, vol. 46, nr. 1/2002[5], **Aris A. Pappas şi James M. Simon jr.**, ofiţeri superiori în Staff-ul Managementului CI, au susţinut o revizuire şi o schimbare fundamentală a Comunităţii dintr-o structură cu un caracter profund tradiţional, alcătuită din organizaţii independente şi „orgolioase", într-un organism configurat pentru a reflecta realitatea în care se desfăşoară activitatea de informaţii.

Autorii apreciau că, pe fondul perimării metodelor tehnice şi umane de culegere a informaţiilor, este necesară realizarea de ajustări şi reconfigurări, întrucât natura izolată şi episodică a ameninţărilor contemporane impune o monitorizare mai precisă şi constantă.

În fapt, recunoşteau că informaţiile sunt culese din aceleaşi medii ca şi înainte de 11 septembrie 2001 când serviciile americane se bazau pe tehnologia avansată, cu toate că trebuia accentuată dimensiunea de procesare, exploatare şi analiză în condiţiile în care avantajele tehnice acumulate în ultimele decenii au ajuns să fie cunoştinţe publice.

Două dintre cele mai importante capacităţi de culegere de informaţii ale CIA s-au perimat: obţinerea imaginilor prin satelit, afectată de revoluţia din domeniile digital şi al fibrelor optice şi de creşterea marcantă a accesibilităţii comerciale a codificării, dar şi operaţiunile tradiţionale cu agenţi în ce priveşte lărgirea accesibilităţii la tehnologie, care face din ce în ce mai dificilă păstrarea identităţilor asumate şi a altor aspecte ale profesiei de ofiţer de caz.

De altfel, potrivit acestora, capacitatea CI de a păstra avantajul în sistemele de culegere de informaţii se va diminua pe măsură ce tehnologia va fi tot mai mult la dispoziţia oricui este interesat şi deţine fondurile

[4] Ivănescu, Lucia „Dennis Blair-şeful efemer al National Intelligence din SUA" publicat pe http://www.independent_al.ro/dosarele_independent/dennis-blair-seful-efemer-al-national-intelligence-din-sua.html.

[5] https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol46no1/html/v46i1a05p.htm.

necesare, context în care, principalul obiectiv al creării şi folosirii sistemelor informative avansate trebuie să fie integrarea informațiilor colectate, care, în cazul în care nu pot fi procesate sau asimilate nu pot fi considerate informații secrete şi prin urmare, devin inutile.

Fiecare agenție îşi elaborează noi tehnologii proprii, în principal în legătură cu domeniul ei de specializare, însă acestea au tendința să fie doar îmbunătățiri ale sistemelor existente, rezultatul fiind un sistem necorespunzător pentru beneficiarii care trebuie să răspundă unor provocări ce sunt într-o permanentă şi rapidă schimbare.

Creşterea cererii de informații secrete a transformat simpla procesare a volumelor imense de date într-o sarcină descurajantă, în condițiile în care instrumentele actuale de procesare a informațiilor au fost proiectate să realizeze analize fundamentale ale unui flux de informații sistematic. Ca urmare a volumului sporit, limitelor de timp şi resurselor umane reduse, aceste instrumente lovesc acum exact în procesele pentru al căror sprijin au fost create.

Pe fondul activării dimensiunii pre-emptive a *intelligence-ului* guvernamental determinat de războiul declarat împotriva terorismului după 9/11, agențiile de informații americane s-au confruntat în scurt timp cu un aflux masiv de informații primare care nu puteau fi procesate, analizate şi exploatate oportun doar cu mijloacele de care dispuneau. În scopul surmontării acestor dificultăți, FBI a apelat din ce în ce mai des la firmele private de *intelligence*, pentru a folosi tehnologia şi experții lor în sprijinul guvernului.

Informațiile şi datele care circulă în prezent cu viteza analizei trebuie să circule de acum cu viteza avertizării. Informațiile specifice care ar putea duce la identificarea şi prinderea unui terorist trebuie să ajungă nestingherite din bazele de date cele mai clasificate şi mai integrate la patrulele care duc la o oprire de rutină în trafic[6].

Autorii clamau necesitatea investițiilor în activitatea de analiză, deoarece cerințele zilnice de a sprijini nevoile imediate ale deciziilor politice *depăşesc capacitățile existente de analiză*.

De exemplu, imagini comerciale din spațiu au oferit recent lumii imaginea unui avion de recunoaştere american parcat pe un aerodrom chinezesc. Nu cu mult timp în urmă, o asemenea imagine ar fi putut veni

[6] https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol46no1/html/v46i1a05p. htm.

numai de la sateliții guvernamentali. În lumea modernă, accesul public la date pertinente prin rețele de ştiri ale mijloacelor de informare, prin Internet şi chiar prin servicii private de informații, este universal şi aproape instantaneu. Drept urmare, atât producătorii cât şi beneficiarii informațiilor sunt tot mai confuzi în încercarea de a face deosebirea între produsele muncii de informații şi analizele şi opiniile din ştiri, şi dintre dezinformare şi minciună[7].

Carmen Medina, fost şef al Centrului pentru Studii de Informații al CIA, afirma, în articolul *Revoluția viitoare în analiza informațiilor: Ce trebuie întreprins atunci când modelele tradiționale nu au dat rezultatele scontate*[8] publicat în 2002, că modelul de analiză a informațiilor adoptat şi utilizat nu reuşea să răspundă schimbărilor rapide în ceea ce priveşte nevoia şi preferințele beneficiarilor. Medina era de părere că agențiile americane se axează insuficient asupra beneficiarului şi îşi concentrază resursele elaborând sinteze tot mai inutile, recomandând *un model revoluționar* care ar transforma analiza concentrată pe *evenimente* zilnice într-o gândire conceptuală previzională care să fie *mai puțin independentă şi neutră* şi mai mult construită pentru a îndeplini nevoile specifice ale beneficiarilor.

Jennifer Sims, Director of Intelligence Studies, Georgetown University susținea că este posibil ca succesul pentru victoriile aduse de serviciile de informații să nu țină doar de culegerea informațiilor *adevărate*, ci de câştigarea unui avantaj decizional asupra unui adversar. Un astfel de avantaj poate scoate din dilemă un guvernant care trebuie să ia decizii şi să-l determine să acționeze. Această abilitate de a uşura alegerea este adevăratul obiectiv al serviciilor de informații."[9]

Crearea avantajului decizional din perspectiva *Viziunii 2015* a CI

Crearea avantajului decizional reprezintă misiunea asumată programatic prin *Viziunea 2015*[10] de către CI în procesul de transformare într-o Organizație Globală şi Integrată de Intelligence, adaptabilă şi capabilă să răspundă adecvat şi eficient provocărilor evoluțiilor mediului de

[7] Ibidem.
[8] https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol46no3/html/v46i3a03p.htm.
[9] „Vision 2015: A Globally Networked and Integrated Intelligence Enterprice", p. 8, publicat pe http://www.dni.gov/Vision_2015.pdf.
[10] http://www.dni.gov/Vision_2015.pdf.

securitate în care dinamica şi complexitatea schimbării generează riscuri mai mari şi un viitor mai puțin predictibil.

Potrivit lui J. M. McConnell – Director al National Intelligence – care preciza în preambulul documentului menționat că misiunea Comunității de Informații este de a crea un avantaj decizional pentru beneficiarii noştri – politicieni, comandanți ai armatei, conducerile serviciilor federale şi oficiali ai serviciilor de informații, aceasta înseamnă că noi colectăm şi analizăm informația pentru a îmbunătăți capacitatea beneficiarilor noştri de a lua decizii, concomitent cu privarea adversarilor noştri de aceste avantaje.

Conform Viziunii 2015, schimbările peisajului de securitate, induse de globalizare şi *era incertitudinii*, reflectate în reducerea timpului de reacție şi comprimarea ciclurilor de decizie, impun proiectarea şi operaționalizarea unui model de *intelligence* orientat către beneficiar, menit să confere abilitatea de a anticipa şi preveni surprizele printr-o vigilență globală ridicată şi previziune strategică.

Necesitatea schimbării paradigmei asupra relației servicii de informații – factori decizionali este generată şi de schimbarea tipologiei beneficiarilor, fiind de aşteptat ca noua generație de guvernanți, nefamiliarizați cu faptul că intelligence-ul este o sursă privilegiată, să dorească ca serviciile de informații să le ofere sprijin „la cerere", personalizat şi să fie tratați ca parteneri – atât ca sursă, cât şi ca beneficiar final.

Translatarea de la modelul actual de informare, centrat pe produs, spre un nou **model interactiv**, care şterge distincția dintre producător şi consumator, implică dezvoltarea unui proiect de informații tip rețea care să permită beneficiarilor să identifice, să acceseze şi să exploateze informațiile de securitate, într-o modalitate sigură şi ajustată nevoilor fiecăruia.

Obiective

Orientarea către beneficiar a informațiilor va impune dezvoltarea capacității organizației de intelligence de a oferi informații obiective, relevante, în timp util şi precise unui palier extins de beneficiari, prin intermediul unor servicii şi produse adaptate fiecăruia în parte.

Din perspectiva reconfigurării relațiilor cu beneficiarii şi a implicării efective a acestora în procesul de intelligence, CI îşi asumă ca obiective:

– folosirea de tehnici sofisticate de depistare a nevoilor beneficiarilor şi de evaluare a performanțelor organizației de intelligence, context în care întrebarea adresată în prezent beneficiarilor *Care sunt prioritățile voastre în materie de informații?* trebuie înlocuită cu *Ce doriți să realizați?* pentru ca

sprijinul acordat acestora să devină mai mult o relație (definită diferit de fiecare beneficiar) decât un eveniment;

– transformarea graduală a produselor analitice în **servicii adaptate**, prin translatarea accentului de la o simplă difuzare pe utilitate, beneficiarii urmând a fi implicați în acest proces prin întrebări *Ce ar fi dacă?*, nu numai prin concluzii de tipul *Ce?*. Pentru realizarea acestui obiectiv este necesar ca analiştii să colecteze date disparate şi să utilizeze metode şi servicii analitice în rețele analitice centrate pe misiune şi destinate obținerii de informații obiective, relevante şi în timp util;

– dezvoltarea unui **angajament față de beneficiar** şi a unui model de management în care „managerii de rețea" să se ocupe doar de anumiți beneficiari, precum şi o delimitare a managementului de rețea în funcție de tipul de beneficiar sau de tipul de problemă de securitate. Pe acest palier se vizează adoptarea unei abordări menite să îi apropie pe profesioniştii în informații de factorii de decizie şi să familiarizeze noii beneficiari cu capacitățile şi limitele organizației.

Misiuni

Acest model integrat – proiectat pentru a promova acuratețea, viteza şi flexibilitatea informării, fără constrângerile legilor organizaționale sau canalelor funcționale – va transforma ciclul tradițional de informații într-o serie dinamică de interacțiuni între cele patru principii ale muncii de informații:

– *Management integrat al misiunii* – integrează şi orchestrează resursele şi expertiza în jurul misiunii, nu al organizației de intelligence sau al domeniului. Misiunilor permanente li se adaugă unele noi care exced securității naționale şi, implicit, informațiilor specifice (epidemii/pandemii, inovații ştiințifice şi tehnologice, dezastre financiare, competiție economică, probleme legate de mediu, interdependență şi securitate energetică, atacuri cibernetice, amenințări privind comerțul global şi infracțiuni transnaționale) a căror îndeplinire va trebui să răspundă provocării generate de estomparea liniilor de demarcație dintre competențele serviciilor de informații interne şi cele externe, precum şi respectarea drepturilor şi libertăților cetățenilor;

– *Culegere de informații adaptată* – realocarea dinamică a senzorilor disparați sau conectați care pot lucra în mod autonom şi în cooperare pentru îmbunătățirea capacității de răspuns, reducerea timpilor de colectare, îmbunătățirea acoperirii şi acurateței prin interferențe şi corelări;

– *Analiza coroborată* – capacitatea de a gestiona şi exploata un volum de informații foarte ridicat şi analişti disparați care să lucreze în

rețele de informații centrate pe o anumită misiune. Va trebui ca analiștii să colaboreze cu experți recunoscuți în domeniul academic, comercial şi de cercetare şi să îşi fundamenteze expertiza pe un acces mai extins la informații din surse deschise, fiind de aşteptat ca beneficiarii să aprecieze în mod deosebit informările sintetice care îmbină expertiza analiştilor de *intelligence* cu relevanța ei pentru agenda politică şi înțelegerea clară şi corectă a situației globale. Precizia analitică şi acuratețea vor reprezenta cerințele minime de aşteptare ale beneficiarilor, iar analizele trebuie să fie clare, transparente şi obiective;

– *Parteneriat strategic* – abilitatea de a extinde CI dincolo de limitele rețelei tradiționale, prin reconceptualizarea modelului actual de parteneriat care să includă aliați şi, conjunctural, parteneri din lumea academică şi industrie.

Interconectivitatea ridicată va spori capacitatea CI de a identifica, monitoriza şi edifica un răspuns în fața unor vulnerabilități sau amenințări care apar la îmbinarea mai multor sisteme (de exemplu, infrastructuri critice de informații, piețe financiare fragile, pandemii etc.), cu potențial de declanşare a unor crize multiple (în mai multe domenii) şi simultane.

Centrarea activității de informații pe o țintă-model concentrică ar trebui să accentueze integrarea misiunii, schimbul rapid de informații şi expertiză, precum şi integrarea resurselor dispersate şi diverse pentru îndeplinirea unor misiuni specifice. Astfel, pentru îmbunătățirea vitezei de culegere şi analiză a informațiilor relevante, este necesară înființarea unor centre integrate de *intelligence*, celule operative (importante pentru reducerea nivelurilor verticale) sau desemnarea unor manageri de misiuni care să gestioneze unitar problematica vizată şi care să acționeze ca interfață între CI şi factorii decizionali responsabili.

Bibliografie

1. *National Intelligence Strategy of the United States of America* (august 2009) publicat pe http://www.odni.gov/reports/2009_NIS.pdf, accesat la 19.07.2010.

2. *SUA nu putea preveni tentativa de atentat de pe 25 decembrie*, publicat pe http://www.evz.ro/detalii/stiri/sua-nu-putea-preveni-tentativa-de-pe-25-decembrie-881358. html, 4 ianuarie 2010, accesat la 19.07.2010.

3. Ivănescu, Lucia, *„Dennis Blair-şeful efemer al National Intelligence din SUA"*, publicat pe *http://www.independent_al.ro/dosarele_independent/dennis-blair-seful-efemer-al-national-intelligence-din-sua.html,* accesat la 19.07.2010.

4. Mazzafro, Joseph M., „IC Vision 2015: Too Little and too Slow!", publicat pe http://www.afcea.org.signal/articles/templates/intel_blog_template.asp? articleid =1673&zoneid0211, accesat la 19.07.2010.

5. Medina, Carmen, „Revoluția viitoare în analiza informațiilor: Ce trebuie întreprins atunci când modelele tradiționale nu au dat rezultatele scontate", în *Studies in intelligence*, Vol. 46, Nr. 3/2002, publicat pe https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol46no3/html/v46i3a03p.htm, accesat la 19.07.2010.

6. Pappas, Aris A., Simon, James M. jr., „Comunitatea informativă: 2001-2015", în *Studies in intelligence*, Vol. 46, Nr. 1/2002, publicat pe https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol46no1/html/v46i1a05p.htm., accesat la 19.07.2010.

7. Sims, Jennifer, Gallucci, Bob, „Why Intelligence-sharing can't always Make us Safer", publicat pe http://www.washingtonpost.com/wp-dyn/content/article/2010/01/07/AR2010010703242.html, 8 ianuarie 2010, accesat la 19.07.2010.

8. Wheaton, Kristan J., „Vision 2015 and The Definition of Intelligence (DNI.gov)", publicat pe http://sourcesandmethods.blogspot.com/2008/07/vision-2015-and-definition-of.html, 23 iulie 2008, accesat la 19.07.2010.

9. http://www.dni.gov/Vision_2015.pdf, accesat la 19.07.2010.

10. https://www.cia.gov, accesat la 19.07.2010.

Corin VÂLCEANU este specialist în domeniul analizei de intelligence, absolvent al cursurilor de masterat Comunicare şi Relații Publice din cadrul Şcolii Naționale de Studii Politice şi Administrative, licențiat în studii economice şi juridice, fiind implicat în pregătirea şi susținerea cursurilor de pregătire pentru analiştii din serviciile de informații.

Ioana BELCIU este analist în domeniul analizei de intelligence, absolventă a Academiei Naționale de Informații *„Mihai Viteazul"*, licențiată a Facultății de Psihologie şi Ştiințele Educației din cadrul Universității Bucureşti. A publicat articole în Psihosociologia & Mass-Media (revistă trimestrială editată de Academia Națională de Informații *„Mihai Viteazul"*).

The Meaning of the SWIFT Provisional Agreement for the EU – US Partnership, with a Focus on Counterterrorism and Data Protection

Ramona Ricarda POPA
Serviciul Român de Informații
e-mail: **ricarda_popa@yahoo.de**

Executive summary:
The SWIFT agreement between the US and the EU is an instrument meant to facilitate the fight against terrorism by sharing data on electronic value transfers. It came into discussion after the 9/11 attacks and the indignation caused by the secret access of some US institutions to personal and financial records of EU citizens. The Agreement represents a challenge to the two great soft powers since its effects go beyond the initially declared cooperation purpose, dealing also with the sensitive issue of protection of personal data, which makes it of direct interest to almost every EU citizen. On a global level, it casts a new light on the transatlantic relationship as it reflects different concepts of state and people security. On a continental level, it shows internal EU divisions of procedural and legal nature as well as a cooperation-deficit between EU institutions, representing a challenge for law makers, security experts, and law enforcement authorities. On individual level, the SWIFT affair certainly raises questions regarding the free exchange of ideas, news, goods and services, etc.

Keywords: SWIFT, counterterrorism, Terrorist Finance Tracking Program, data protection, data manipulation, personal data transfer, electronic value transfer, EU, U.S. Treasury Department, Safe Harbor, transatlantic partnership, security affairs.

1. Introduction

1.1 The factual background

The SWIFT Agreement is an accord between the European Union and the United States of America regarding the processing and transfer of Financial Messaging Data from the EU to the US for the purposes of the

Terrorist Finance Tracking Program[1]. The Agreement has emerged out of the desire of the parties "to prevent and combat terrorism and its financing, in particular by mutual sharing of information, as a means of protecting their respective democratic societies and common values, rights, and freedoms"[2], in the spirit of the transatlantic partnership, based on the UN Security Council Resolution 1373[3]. Its purpose is to ensure that the concerning data "are made available upon request by the U.S. Treasury Department[4] for the purpose of prevention, investigation, detection, or prosecution of terrorism or terrorist financing." (Agreement, § 1.1a) Signed on November 30,2009, the Agreement goes into effect on February 1,2010 for an agreed period of 9 months, and represents an interim solution until a long-term agreement is ratified.

SWIFT is the abbreviation for the cooperative Society for Worldwide Interbank Financial Communications, founded in 1973 with the headquarters near Brussels, Belgium. It is based on Belgian law and has set the international common standards regarding worldwide financial transactions. Likewise, it has established a shared data processing system and worldwide communications network. SWIFT has been providing the proprietary communications platform, products and services that allows to connect and to exchange financial information securely. According to the

[1] It was created by the Bush Administration as a response to 9/11. It is conducted by the CIA, under the supervision of the Treasury Department and based mainly on the SWIFT transaction database, after top officials exerted pressure for the data transfer.

[2] See Agreement text.

[3] Signed September 28, 2001 to enhance international intelligence sharing in the field of counterterrorism, respectively, to impede the movement, organization, as well as fund-raising activities of terrorist groups. It created the SC's Counter Terrorism Committee, to monitor compliance with these provisions.

[4] The Treasury Department is the executive agency responsible for promoting economic prosperity and ensuring the financial security of the US. It operates and maintains systems that are critical to the nation's financial infrastructure, and works with other federal agencies, foreign governments, and international financial institutions to encourage global economic growth, and to predict and prevent economic and financial crises. It performs a critical and far-reaching role in enhancing national security by implementing economic sanctions against foreign threats to the U.S., identifying and targeting the financial support networks of national security threats, and improving the safeguards of our financial systems. Thus, it is the steward of U.S. economic and financial systems, and an influential participant in the global economy. (US Department of Treasury http://www.ustreas.gov/education/duties/)

official site of SWIFT, nowadays, over 8,300 financial institutions and banking organizations, security institutions, and corporate customers in the entire world employ it daily to exchange millions of standardized financial messages, stored for 124 days on a main and a backup computer server. (http://www.swift.com/) This represents about 80% of the worldwide traffic for electronic value transfers, according to the background note of the Justice and Home Affairs Council (p.5). Thus, due to its assignment and possibilities, SWIFT has become the first messaging service for banks issuing international transfers[5].

In June 2006, a series of articles published by The Wall Street Journal[6], The New York Times[7], and The Los Angeles Times[8] disclosed that after the 9/11 attacks, the Treasury Department, the FBI and the CIA had been accessing secretly and systematically the SWIFT database in Virginia, US, without individual court-approved warrants and without the knowledge of the European authorities, to examine the respective transactions[9] – based on a private agreement between SWIFT and the Treasury -, in order to capture al-Qaeda members suspect of having been involved in terrorist bombings. The publications had major consequences upon all 3 involved parties: first, SWIFT became member of Safe Harbor[10] to legalize the transfers, then, starting with December 31, 2009, the computer servers would move out to Switzerland. Finally, after investigations and 2 years of discussions, the SWIFT agreement was signed, to meet the US requirements for access to the data, and to ensure "that designated providers of international financial payment messaging services make available to the

[5] It is known by the customers by the SWIFT-BIC code, which is the SWIFT ID.

[6] It is the most distributed paper in the US, and adopts a more conservative, critical tone. Despite of this, the news tends to be rather liberal. Nonetheless, Gordon Crovitz, a former publisher of the paper, endorses the editors' pursuit for impartiality.

[7] It is the third most distributed daily US newspaper, and the largest metropolitan one, with partly conservative, and partly, but predominantly, liberal bias.

[8] It is the second-largest metropolitan newspaper, and the 4th most distributed in the US. It adopts a liberal tone.

[9] Here one can see the 2 fears of the liberals: government power and mob rule (in this case mass media rule).

[10] Safe Harbor is an agreement employed initially for commercial purposes by economic agents that wanted to use the US as a hub in order to centralize their international data transfers. (Kuner 2009:4)

US Treasury – as administrative authority - financial payment messaging data stored in the EU, necessary for preventing and combating terrorism and its financing". (Preamble, 2nd paragraph) The request is to be executed as a matter of urgency and data may include information about the originator and/or recipient of the transaction, like name, account number, address, national identification number, and other personal data related to financial messages. (§ 4.2) Yet, the SWIFT transfers do not regard US citizens, as the database does not contain information on ordinary transactions that would be made by individuals in the US, such as deposits, withdrawals, checks, or electronic bill payments, according to Stuart Levey, an Under Secretary at the Treasury Department. (Levey, 2006)

The 2006 as well as the 2009 context brought forth a high degree of discontent among the EU representatives, since they regard this development as a US endeavor to achieve its own security goals, and because the US intelligence agencies have now more or less legal access to the personal, financial records of many EU citizens, using different data protection practices than the EU. The ongoing debate has three main critical dimensions, evolving on political-geostrategic, legal-procedural and security level.

1.2 The structural and analytic approach

The subsequent analysis is composed of three interconnected parts, which attempt to answer the question: "what is the impact of the Agreement for the EU-US relationship, in terms of counterterrorism and data protection?" The question is approached by a liberalist understanding of human security as elaborated by UNDP[11], and has takes as a legal frame the EU Data Protection Directive 95/46/EC, the European Convention on Human Rights § 8, the EU Charter of Fundamental Rights § 8, the US Safe Harbor, and the provisional SWIFT Agreement.

The first chapter focuses on the positioning of the two superpowers towards each other as security providers in a globalised world, starting from the utilization of the SWIFT resource. I consider this item of key importance, since the policies of the two entities are highly reflected in both security issues that are discussed in the following chapter. The second part deals with the dilemma of data transfer vs. the principle of respect for

[11] See: New dimensions of human security. In: Human Development Report 1994. Chapter 2. (http://hdr.undp.org/en/reports/global/hdr1994/).

privacy. The last part is concerned with the question of data transfer for an efficient anti-terror fight, the two sections trying to see what impact the agreement has on both data protection and counterterrorism.

According to the UNDP definition, security is no longer a narrow state-centered national issue, but has turned universal, integrative, people-centered, being understood as an all-encompassing concept of human security, since frontiers are no longer barriers, and threats come rather from the actions of millions of people than from aggression by a few nations. (UNDP 1994:24,34) Human security includes highly interdependent components – economic security, food security, health security, environmental security, personal security, community security, and political security – being easier to ensure through prevention (UNDP 1994:22).

I chose a liberalist understanding of human security because it offered more adequate analytical tools than other approaches: in a globalised world the variety of actors are dependant on cooperation to achieve the biggest gains. In international relations liberalism is one of the greatest advocates of interdependence and international cooperation based on a set of common values, in both high and low politics. The theory as it is found in the Oxford Manifesto of 1947 postulates that state preference determines state behavior, every individual having the right to enjoy the essential human liberties, the free exchange of ideas, news, goods and services. Censorship, protective trade barriers, and exchange regulations are rejected. Likewise, debates can be introduced by any actor. (www.liberal-international.org/editorial.asp?ia_id=535)

I applied a qualitative method of analysis, based on a close reading of the most complex press articles I could find on the *SWIFT affair*, both in the US and the EU, in English and German language. The French and Spanish speaking areas have been covered less by articles on this issue. The articles I found have a conservative, liberal or critical stance. Unfortunately I could not find any academic approach to the Swift Agreement until the moment of writing this paper, and only very few on the SWIFT scandal of 2006.

2. The EU-US bilateral relationship in the light of the new agreement

The presence of the SWIFT backup computer server on US territory has given the US security agencies unlimited access to sensitive data, offering them a considerable advantage over other countries in the fight

against terrorism, "a unique and powerful window into the operations of terrorist networks", as Stuart Levey declared. (Lichtblau 2006) Among these are the *link analyses* and their operative employment without individual warrants, a mandatory requirement within the EU. The above mentioned publications, disapproved by the US government, came as a radical bottom-up initiative, rejecting the US state-centric conception of security. Drawing the attention upon the unauthorized employment of sensitive EU resources and the breach against the privacy rights of the EU citizens, they emphasized the interdependency between development, human rights and national security, and called for a new settlement based on open cooperation. By doing this, a valuable top-down systematic prevention instrument was disclosed, striking heavily against a confidential strategy, not only because it taught the potential targets about its existence, jeopardizing ongoing operations and investigations, but also because it placed the US in a difficult position in front of the overseas partner.

The removal of the server from the US was initially seen as another blow to the US counterterrorist policy and thus as a weakening in front of the EU, since it was thought it would go far beyond being a mere change in the construct of this platform with a key role in the field of financial security. It meant restricting the US access to the transaction data because only the servers in the Netherlands and Switzerland[12] would process EU international payment transactions, which in turn meant that the US had to formulate legal, official requests for the records. Moreover, it would have created a certain degree of dependency on the concerned governments, thus decelerating the decision making process and reaction. To avoid this, the US government exerted massive pressure on Brussels, emphasizing the extensive nature of terrorism, based on the drop of the security levels that made the vulnerability against terrorist threats rise, including in Europe. The Secretary of State Hillary Clinton told her European counterparts the fate of the West hung in the balance, whereas US ambassadors "stormed EU governments pulling out all the moral and political stops." (Schlamp, 2009) In this respect, an Agreement would have allowed further access of the US to the SWIFT data, impairing less the usage of this vital tool that has played

[12] International standards and supervisory requirements ask that infrastructure is to be kept geographically separated.

for almost a decade a veiled part in the US national and international counterterrorist surveys and investigations.

After the initial fears were overcome by the US, the SWIFT Agreement turned out to be a tough nut to crack for the EU, as it implied inner European divisions between the EP and the EU Council, at the procedural and legal level. Although an international treaty or agreement requires the unanimous consent of all 27 members, the drafting process took place mainly behind closed doors, the EU Council infringing upon drafting and negotiation procedures, by eluding the EP. This happened even though many countries - especially Germany, Austria, France, and Finland - opposed vehemently to the Agreement, and are presently pushing for its suspension[13].

In this sense, after 2 years of discussions, the swiftly signed Agreement, just before the ratification of the Treaty of Lisbon, reflects the positioning of the two superpowers towards each other. First, it conveys a compromise of the EU towards the US, as well as a sign of trust, in order to keep the common strives against terrorism functioning. Second, it indicates that within the EU, foreign relations with its Western partner take priority to the necessity of solving internal fractures, whereas the US discourse maintained its own policy as a top priority This implies the EU has given in to the US pressure and requirements for the second time in this case, depicting the EU as actor on the international scene.

The SWIFT Agreement shows deficiencies in the internal EU cooperation as well as in the international cooperation realm, because signing the Agreement one or 2 days later, under the Treaty of Lisbon, would have meant harsher negotiating conditions for the US. This would have been based on more strict drafting and negotiating procedures since the EP would have had extensive co-legislative powers, and decision making competences in internal and security affairs, that is, it would have had the veto right. It would have meant a more extensive approach to such a sensitive issue like financial records transfers, since the Lisbon Treaty calls for more precise rules and more competences for the EP on data protection and fundamental rights regarding bank data transfer issues. By this means,

[13] Among them are Cornelia Ernst of Germany, Rui Tavares of Portugal, and Marie-Christine Vergiat of France, who are GUE/NGL MEPs on Parliament's Civil Liberties, Justice and Home Affairs Committee, the Alliance of Liberals and Democrats for Europe, etc.

the content of the Agreement has come to include a series of ill-defined aspects, the entire process shedding an unfavorable light on the EU compliance with democratic principles and upon its capacity for unitary decision making, keeping the EU in a critical position towards the US.

If the disclosure of SWIFT turning from a mere data processor to data controller[14] created in 2006 "legal and political clashes between Europe and the US" (Brand 2006), in 2010 the Agreement officializes this role, turning the EU into a bestower and the US into a beneficiary, with potential impairing consequences for the EU. On the **internal political** level, it cares for a restraint on European sovereignty. On the **financial-banking and data protection** level, it could bring forth monetary fines by banks, if the financial records of the clients are sent to the US government, without the existence of a well founded suspicion of terrorism. On the **security** level, it leaves unsolved the vulnerability for industrial and economic espionage by third parties, as long as the US conclusions based on a comprehensive analysis of financial data can be transferred to third parties.[15] Last, but not least, on the **level of international affair**s it keeps the EU in a position not to disturb in any way the relationship with the US, reflecting the unequal positions of the two involved parties.

3. Meaning for data protection

By accepting an unequal treatment on the basis of citizenship, through the lack of reciprocity, as well as the swift and undemocratic signing process, presuming that its postponing would have maintained the security vacuum, the interim Agreement did not succeed to impose itself against the highly determined US approach in international affairs. As the SWIFT affair depicts, the mere suspicion of a potential terrorist threat sufficed to legitimize protracted state action against the principle of privacy of financial data, recognized as a fundamental right within the EU. Without

[14] A data controller is a natural or legal person which alone or jointly with others determines the purposes and means of the processing of personal data, whereas a data processor is a natural or legal person which processes personal data solely on behalf of the data controller. EU Data Protection Directive § 2(d)-(e). Having this role, SWIFT violated the notification articles of the same directive.

[15] This is an issue discussed also within the Safe Harbor, the US-EU disagreements not having been solved yet.

a specific Congressional authorization (Lichtblau 2006) and without the knowledge of EU privacy commissioners, the US request of financial records corresponds to the infringement of the fundamental rights and the principles of democracy, because legal or institutional barriers to the government's access to private information have been trespassed. Some of the concerned EU bank institutions, who refused to support the US tactics in this respect, namely the European Central Bank, the National Bank of Belgium, the Bank of England and other G-10 banks, knowing about the data gathering, kept silence (Spongenberg 2009), supporting tacitly the US policy and outraging civil society.

The first major consequence of the SWIFT Agreement is that it limits the US access to sensitive EU personal financial data. Since the data would have to be processed and stored in the Netherlands and Switzerland, the US would have to address official requests, "tailored as narrowly as possible", to prevent too much consumer data from being evaluated by law enforcement and intelligence authorities. (Neely 2009) The second major consequence is that it acts upon the privacy[16] of banking data of EU businesses and citizens, because the Agreement actually cares for a shift from the US legislation to the EU one.

On the European continent, the financial personal data are considered human rights according to the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), § 8, and the Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. In the EU, these are protected by the Charter of Fundamental Rights of the EU and the EU Directive 95/46/ED, yet this does not cover the judicial and police cooperation, but it sees that data can only be *processed* with the consent of the data subject. The US does not have a comprehensive data protection system, so that basically an agreement in this sense automatically becomes a challenge and a potential source of tension between the two parties.

By this shift in the legislation field, the Agreement actually opens the way for a transatlantic harmonization of practices and data protection regulations, at higher protection standards, trying to set new rules for the US state behavior vs. state access to privacy. This means that the EU legal

[16] Westin sees privacy as the enforcement of people to determine when, how, and to what extent information about them is communicated to others.

framework takes a step towards gaining a central position in data sharing and that the use of the US governed *Safe Harbor* for security reasons also needs to be re-discussed. The official debates have not reached this point yet, since the EP has not been involved in the signing of the SWIFT Agreement, and the EU Commission, who indicated in 2007 that "onward transfers under Safe Harbor must fulfill the basic requirements of European data protection law" (Kuner 2009:4), has kept out of the signing affair.

On short term, the ongoing divergences around the transfer practices could have a rather hindering effect on the bilateral transatlantic cooperation in the field of data sharing for disclosing terrorist financing, since the legislation switch confronts the EU with two critical dilemmas in 2 fields of utmost importance for both sides:

- Is the transfer of personal financial information appropriate and proportional to the purpose of fighting terrorism, and transparent towards the financial customers?
- What is a too tight data protection and what is a too loose data protection?

Based concretely on the SWIFT Agreement, the first specific critical issues that created discontent refer to:

- the **manipulation standards** for personal financial information regarding the content of the data and their classification level:
    - regarding the **content** of the data, although the Agreement prohibits the onward transfer of data to third parties, broader conclusions based on these data could be passed indirectly to third parties, in the form of conclusions regarding markets, commercial partners, transaction volumes or price calculations and profit margin. Likewise, they could be used for other purposes, i.e. *risk assessment scores or economic profiling*. Financial Times Deutschland goes even further, assessing potential impacts on industrial and economic espionage. Therefore the Agreement is not only a legal consequence to the 'protectionist' call of restraining the US access to EU data, but embodies challenges for more specific limitations, since the "prevention, investigation, detection, or prosecution of terrorism or terrorist financing"[17] is a too wide-ranging

[17] See the Draft Agreement.

formulation to ensure the binding of the data to that purpose. Through this, it raises the proportionality question of the transfer, for how the data is connected to counterterrorist investigations has to be researched and explained first.

- regarding the **classification** level of the data, the Agreement raises the question of common data classification standards regarding EU sensitive and classified personal financial information. Practically, it determined privacy advocates to require that the US comply with the EU data protection standards when processing EU data, because EU beneficiaries should enjoy legal certainty. That means, on the one hand, that the US data protection level should not be lower than those in the EU. On the other hand, it means that a control mechanism should be used to check the compliance with the data protection rules. Under current rules, in the EU, each government is responsible for the application and enforcement of the common EU data privacy law.

- **Legal protection standards** of the data and of the citizens:
  - **The legal authorization** is mentioned only tangentially in terms of a 'central authority', which does not suit the EP demands. The procedures on who decides and how the **decision** is taken regarding the transfer and processing of the data for the purpose of fighting terrorism is too broadly defined.
  - the Agreement still allows an easy access to personal financial data without strong **judicial safeguards**, which raises questions regarding its appropriateness. Not requiring individual search warrants to access financial data violates the principles for privacy and the protection of personal data under the above mentioned EU laws. In this respect, the Agreement calls for more safeguards to prevent broader data searches, determining EU internal disagreements. The fact that the Agreement does not design a role for any data protection body caused Frank Rieger[18] to declare that the

[18] Spokesperson for the Berlin Chaos Computer Club, an organization that advocates online privacy.

Agreement is rather reflecting data imperialism, than an anti-terrorism deal. (Neely 2009)

- The agreement does not legally **protect the citizens against abuse**, since there is no judicial help or protection for "individuals believed to be acting as a "foreign terrorist agent". (Meyer 2006) The Agreement provides for the possibility that "any person who considers his or her personal data to have been processed in breach of this Agreement is entitled to seek effective administrative and judicial redress in accordance with the laws of the EU, its Member States, and the US, respectively" (art.11.3). Yet, there are no further provision regarding how an EU citizen could file a complaint against the US authorities over their handling of their personal data.

  At this point the Agreement reflects a major difference between the EU and US on data protection and privacy, which has produced clashes between the two parties. Whereas the EU follows a socially protective and proactive pattern, the US is rather reactive, being advantaged by the fact that privacy laws are enforced on banks not on banking consortiums like SWIFT.

- The **time limit** of the Agreement does not surpass 2010, whereas the data would be stored for 5 years, which makes the German Federal Criminal Police Office (BKA) doubt the use of the data in the fight against terrorism.

The development in the field of data transfer starting with the passenger name record and the US Customs and Border Protection, up to the SWIFT Agreement, calls for a serious reflection in the area of the data protection policies. This is not only because of the need for common principles and practices in a field in which the EU and the US collide while claiming world leadership. It is also due to the substantial disadvantage in front of the terrorist threat, as the most recent debates have shown: despite the amount of measures for the protection of common rights and values, lawmakers and law enforcers seem to have failed in adapting to the technological challenges.

4. Meaning for the counterterrorist fight

Gilles de Kerchove, the EU Counterterrorism Coordinator, alleges that SWIFT is indispensable for the counterterrorist fight, "one of the most valuable sources of information […] on terrorist financing", as Levey affirms, because it provides a rich *hunting ground* for investigations. As the information can be "mapped and analyzed to detect patterns, shifts in strategy, specific *hotspot* accounts, and locations that have become havens for terrorist activity" (Meyer 2006), the program has pointed to new suspects or "key links in the investigations of al Qaida and other deadly terrorist groups". (Levey, 2006). "Since the Sept. 11 attacks, it has tracked millions of confidential financial transactions handled by SWIFT." (Brand 2006 quotes the U.S. Treasury) "The value of the program has been in tracking lower- and mid-level terrorist operatives and financiers who believe they have not been detected and militant groups, such as Hezbollah, Hamas and Palestinian Islamic Jihad..." (Meyer 2006 quotes Stuart Levey) The SWIFT data has supposedly helped capturing the German 'Sauerland Group'[19], Hambali, the mastermind of the 2002 bombing in Bali, and breaking a terrorist network in the UK[20]; it has helped identify Uzair Paracha, an al Qaeda operative in Pakistan, etc. (Lichtblau 2006)

Nonetheless, the usage of SWIFT data for counterterrorist purposes did not correspond to the original, commercial processing purpose, violating the proportionality principle established by the 95/46/EC Directive. This aspect mirrors the conflicting situation of SWIFT before signing the Agreement: based upon EU legislation, its server in the US had to work under the US legal jurisdiction, being bound to respond to the administrative subpoenas; otherwise it made itself guilty of federal offence. Not infringing US civil rights meant infringing EU fundamental rights. The responsibility for this trespassing bears SWIFT, but also the informed EU financial institutions and banking organizations.

[19] The Group, captured in September 2007, was formed of three Germans converted to Islam and a Turk: Fritz Gelowicz, Daniel Schneider, Attila Selek, Adem Yilmaz. The group was part of the Islamic Jihad Union that has contacts with al Qaida. Their plan was to attack several US facilities in several German cities, by means of car bombings.

[20] Abdulla Ahmed Ali, Tanvir Hussain, and Assad Sarwar conspired to activate bombs disguised as drinks in order to blow up planes flying fron London to US. They were convicted for 30 years; another 4 were found not guilty.

Placing both SWIFT servers under EU legislation for complying with the EU legal framework, may bring about at least a tactical change in the US data collection policy in the field of cutting terrorism financing overseas, since it may induce a deceleration in the analysis based upon SWIFT data. Before the Agreement, TFTP had direct unrestricted access to the data, based on a monthly administrative subpoena[21], without having to seek assistance from foreign banks. This prevented potential time lags or refusals of cooperation. (Meyer 2006) The Agreement changes this situation since it "limits the US authorities' information requests to people with [proven] links to terrorist activity. First, the US authorities must justify their requests with the US Treasury, and then, they must structure them to be as specific as possible, because otherwise, any EU citizen could become object of the US investigators." (Lawton 2009)

This makes indirectly the Agreement require more than an Automated Targeting System[22], and that the various levels of control indeed work as a strainer, otherwise "if a pinpointed request is not possible, SWIFT would provide *all relevant* data - which could include names, addresses and personal identification numbers." (Lawton 2009) Then, the unmanageable amount of the required data would cut the real efficiency of the transfer as part of the preventive policy in anti-terrorist matters. These layers should see that the valuable information be extracted in due time, complying with the EU legal requirements and standards.

Even though after placing the servers under EU jurisdiction the Agreement does not fail to bind the US authorities to inform the EU about possible terrorist threats, the contribution of the US to the EU intelligence agencies may lessen. According to the former French investigating judge commissioned by the EU, Jean-Luis Brugière, before the restrictions the TFTP had generated considerable intelligence to the EU states. (JHA

[21] In the US legal system, the subpoena is a court summon. There are two types: the usual writ for the summoning of witnesses (ad testificandum) or the submission of evidence, as records or documents, before a court or other deliberative body (duces tecum). The administrative subpoena is a non-traditional tool of criminal investigation in the fields of secret service protection, health care fraud, child abuse, controlled substance cases, and Inspector General investigations. (Doyle 2005,2) This method helped bypassing traditional banking privacy protection rules.

[22] This kind of mechanism was used with the transfer of passenger data to the US.

Council, 2009:5) Now the restricting action of the EU may presumably cause a US reduction of intelligence towards the 'data provider'.

This causes many to strengthen their belief that in the field of counterterrorism the Agreement did not produce radical positive changes. German Justice Minister Sabine Leuthheusser-Schnarrenberger and the German Federal Police Agency consider that "granting intelligence agencies access to people's bank accounts doesn't provide any additional security, […] [because] "in terms of combating politically motivated crime, there is no technical requirement or operational interest in a systematic verification of the SWIFT database." (Spiegel online, www.spiegel.de/international/europe/0,1518,674789,00.html)

But what the Agreement actually realizes is that it questions whether there is perhaps also a necessity for a re-evaluation of the counterterrorism legislation to cope with the requested privacy needs while making sure that efficient measures of security can be taken. How can people feel free from fear of terrorist attacks without feeling their privacy is violated by the authorities responsible for security? On short term, this dilemma may restrain the transatlantic cooperation in the field of counterterrorism, which is so much needed to ensure global security, and brings to light that the response to the global threat is not yet global. It could not be at least as long as the discussion is still going on.

5. Conclusion

Even though the agreement is about the transmittal of financial data for the purpose of the counter terrorist fight, it actually directly concerns almost everybody, because it has multifarious legal, procedural, and security consequences and impacts on the privacy and the daily life of EU citizens. The debates around the SWIFT Agreement show that many questions still exist regarding the juridical and political construction of the EU data protection mechanism. They reveal the dilemma that the law makers and those enforcing the law are confronted with when ensuring a high level of security against terrorism while respecting the privacy rights of the citizens and coping with democratic principles. Moreover, they point out that terrorism and counterterrorism are still asymmetric, despite of the global cooperation in security matters. While everyone can fear the occurrence of

cross border threats, the policies to combat them cannot cross the borders of the legal and procedural practices.

In this sense, this interim Agreement is less a basic framework of personal data transfer and more a door for necessary comprehensive improvements in the legislation and practices in this field, to reduce the opposition of the two superpowers. Concerning the EU, it challenges the Commission, the Parliament and the Council to find solutions to the legal problems of the US-based regulation for data protection, and calls for a higher profile as unified actor in front of the unilateral US approach in international and security affairs. It proves that as long as the EU gives in to the US data protection standards and practices despite its clear communitarian laws, it accepts the US to act upon it for "improving regulatory standards"[23]. It induces that the EU accepts the US legislation to undermine the EU one, and the US interests to dominate the EU ones, fetching a blow right in the face of the Union's institutions and democracy. If the final SWIFT Agreement does not embrace this issue, the data protection differences will perhaps continue to dominate the transatlantic agenda.

A first step towards the solution of this problem supposes that the internal issues that concern the Union be clarified so that the EU may act less fractured in the foreign affairs with the US. In this respect, the EU disposes of 2 powerful instruments:

- the Treaty of Lisbon, for it binds the EU Council and Commission to involve the Parliament in all the phases of negotiations, which creates a different juridical context in both, inner and international affairs;
- the civil society, inasmuch as it exercises confidently its role as the second pillar within human security by asking how appropriate, proportional and effective such a data transmittal is as an instrument for identifying terrorist financing and capturing terrorists, and by pressuring the EU to be less submissive in issues like data protection practices.

[23] See the US National Strategy for Homeland Security.

Concerning the overseas partner, the debates encourage an adjustment of the US legislation – in a highly ideal case -, at least with respect to the Privacy Act, or the issue of addressing US courts by EU citizens inasmuch as data protection within the partnership is as important as the counterterrorist fight outside the western alliance. The first mentioned protects the citizens from the inside threats, whereas the second one protects them from the outside perils. This means that if counterterrorism focuses on people, its instruments (read protection in data transfers) should also have citizens as their highest command. As long as the parties infringe upon the fundamental rights and civil liberties of the other[24], they are impeded in their common defense policy and their reciprocal reliance is shadowed. Hence, as the conflicts created by the SWIFT Agreement show, it becomes binding that the partners agree upon common practices, based on highly commended principles, in order to be strong against others.

Even though one cannot really talk about its contribution to the fight against terrorism, an Agreement for financial data transfer has been necessary in the context of the SWIFT architectural changes. With all its advantages or breaches, it displays the common endeavors to master without delay asymmetric threats, as well as the EU efforts to turn the transatlantic partnership for combating terrorism as smooth as possible, trying for the time being to keep away from the public the sensitive subject regarding the US engagement with the EU security issues.

[24] Another example is the violation of the EU Directive 95/46/ED in the case of the transfer of the passenger data.

6. Bibliography

1. Brand, Constant, „Belgian PM: Data Transfer Broke Rules", in *The Washington Post*, 28.09.2006, El. Ed http://www.washingtonpost.com/wp-dyn/content/article/2006/09/28/AR2006092800585.html.

2. Dahl-Eriksen, „Tor: Human Security: A New Concept which Adds New Dimensions to Human Rights Discussions?", in *Human Security Journal* Volume 5, Winter 2007, El. Ed. Accessed 24.01.2010 http://www.peacecenter.sciences-po.fr/journal/issue5pdf/4.Eriksen.pdf.

3. Doyle, Charles, „Administrative Subpoenas and National Security Letters" in *Criminal and Foreign Intelligence Investigations*, Background and Proposed Adjustments. CRS Report for Congress. April 15, 2005, El. Ed. Accessed 22.01.2010 www.fas.org/sgp/crs/natsec/RL32880.pdf.

4. European Digital Rights: A new SWIFT agreement under negotiation between EU and USA. In: EDRi-gram Nr. 7.17. 09.09.2009. El. Ed. http://www.edri.org/edri-gram/number7.17/swift-european-parliament

5. *European Parliament: Resolution of 17 September 2009 on the envisaged international agreement to make available to the United States Treasury Department financial payment messaging data to prevent and combat terrorism and terrorist financing*, El. Ed. Accessed 24.01.2010 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2009 -0016+0+DOC+XML+V0//EN

6. Financial Times Deutschland: „Datenstriptease erbost Wirtschaft", in *Financial Times Deutschland*. 30.11.2009 http://www.ftd.de/politik/deutschland/:swift-abkommen-datenstriptease-erbost-wirtschaft/50044462.html?page=2

7. Gellman, Barton/Blustein Paul/Linzer, Dafna: Bank Records Secretly Tapped.Administration Began Using Global Database Shortly After 2001 Attacks, in *Washington Post*, June 23, 2006. El. Ed. Accessed 22.01.2010 http://www.washingtonpost.com/wp-dyn/content/article/2006/06/23/AR2006062300167.html.

8. Justice and Home Affairs Council: BACKGROUND Note. Brussels, 27.11.2009, El Ed. Accessed 25.01.2010 http://blog.tech-and-law.com/2009/12/eu-transfer-of-financial-messages-data.html.

9. Kuner, Christopher, „Onward Transfers of Personal Data Under the U.S. Safe Harbor Framework", in *Privacy & Security Law*, 17.08.2009, El. Ed. Accessed 22.01.2010 http://www.hunton.com/files/tbl_s47Details/FileUpload265/2639/Kuner_Onward_Transfers_8.09.pdf.

10. Lawton, Michael, „EU approves data-sharing SWIFT agreement with US authorities", in *DW-World.de*. 30.11.2009, El. Ed. http://www.dw-world.de/dw/article/0,,4952263,00.html.

11. Levey, Stuart Levey, „Statement of Under Secretary Stuart Levey on the Terrorist Finance Tracking Program", 23.06.2006, in *The Press Room of the US Treasury Department*, El. Ed. http://www.treas.gov/press/releases/js4334.htm.

12. *Liberal International*, „The Oxford Manifesto of 1947", accessed 24.01.2010, www.liberal-international.org/editorial.asp?ia_id=535.

13. Lichtblau, Eric / Risen, James, „Bank Data Is Sifted by U.S. in Secret to Block Terror", in *The New York Times*, June 23, 2006, El. Ed. accessed 22.01.2010 http://www.nytimes.com/2006/06/23/washington/23intel.html?_r=1&hp&ex=1151121600&en=18f9ed2cf37511d5&ei=5094&partner=homepage.

14. López Aguilar, Juan Fernando, „SWIFT: European bank data transfers must comply with European standards, say MEPs", press release in *European Parliament site*. 03.09.2009, http://www.europarl.europa.eu/news/expert/infopress_page/019-60174-246-09-36-902-20090903ipr60173-03-09-2009-2009-false/default_en.htm.

15. Meyer, Josh / Miller, Greg, „U.S. Secretly Tracks Global Bank Data. The Treasury Dept. program, begun after the Sept. 11 attacks, attempts to monitor terrorist financing but raises privacy concerns", in *L.A. Times*, June 23, 2006, El. Ed. accessed 22.01.2010 http://articles.latimes.com/2006/jun/23/nation/na-swift23?pg=3.

16. Neely, Brett, „EU to share consumers' financial data with US", in *Deutsche Welle-World.de*, 13.11.2009, El. Ed. http://www.dw-world.de/dw/article/0,,4887522,00.html.

17. *Official Journal of the European Union*, „Processing of EU originating Personal Data by United States Treasury Department for Counter Terrorism Purposes – 'SWIFT'. Terrorist Finance Tracking Program – Representations of the United States Department of the Treasury (2007/C 166/09)", El Ed. accessed 24.01.2010 http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_166/c_16620070720en 00180025.pdf.

18. Schlamp, Hans-Jürgen, „Spying on Terrorist Cash Flows. EU to Allow US Access to Bank Transaction Data", in *Spiegel online International*, 27.11.2009 http://www.spiegel.de/international/europe/0,1518,663846,00.html.

19. Spiegel Online: Not So SWIFT. European Parliament to Reject Bank Data Agreement with US. 29.01.2010, El. Ed. Accessed 29.01.2010. http://www.spiegel.de/international/europe/0,1518,674789,00.html.

20. Spongenberg, Helena, „European Central Bank knew about US data access", in *EUobserver*, 29.06.2006, El. Ed. http://euobserver.com/9/21984.

21. UNDP, „New dimensions of human security", in *Human Development Report 1994*, Chpt. 2, El. Ed. accessed January 23, 2010. http://hdr.undp.org/en/reports/global/hdr1994/.

22. Vermeulen, Mathias, „EU approves data-sharing SWIFT agreement with US authorities", in *The Lift. Legal Issues in the Fight Against Terrorism*, 30.11.2009 http://legalift.wordpress.com/2009/11/30/eu-approves-data-sharing-swift-agreement-with-us-authorities/.

Ramona Ricarda POPA a absolvit în 2002 limba şi literatura germană şi engleză, la Universitatea Lucian Blaga din Sibiu. În anul 2003 a absolvit Academia Națională de Informații *„Mihai Viteazul"*, Bucureşti, iar în perioada 2007-2009 a participat la un curs de cercetare în domeniul păcii şi al conflictelor la Marburg (Germania). Până în prezent a realizat mai multe studii în domeniu, cu accent pe transformările sociale şi politice în perioadele de tranziție după conflicte sângeroase.

INSTRUCȚIUNI PENTRU AUTORI

Misiune şi conținut. *Revista Română de Studii de Intelligence (RRSI) este dedicată studiilor de intelligence şi disciplinelor ştiințifice conexe, cu scopul de a facilita crearea unui forum de dezbatere pentru mediile profesional, academic, politic şi public.*

RRSI este o publicație nepartizană şi nonprofit care nu pledează în favoarea sau împotriva vreunei poziții, responsabilitatea pentru ideile prezentate aparținând în exclusivitate autorilor.

Politica de evaluare*. RRSI acceptă doar editoriale, articole şi recenzii care nu au fost anterior publicate.*

Editorii şi redactorii RRSI selectează materialele transmise de autori şi, acolo unde este cazul, le ameliorează prin dialog constructiv, doar cu acceptul acestora din urmă, asigurând astfel corectitudinea şi valoarea ştiințifică a materialelor ce urmează a fi publicate. Evaluarea calității academice a materialelor se face în anonimat ("blind review"), corespondența dintre evaluatori şi autori realizându-se doar prin intermediul e-mailului ani@sri.ro. RRSI garantează că lucrările nu sunt respinse/modificate pentru că ideile exprimate sunt contrarii altor studii publicate anterior sau pozițiilor evaluatorilor, ci doar în cazul în care nu fac dovada cercetării ştiințifice.

RRSI asigură confidențialitatea pentru materialele respinse de la publicare, precum şi pentru modificările aduse acestora.

Pregătirea materialelor pentru publicare

1. Forma de prezentare a lucrării

Articolele propuse spre publicare în RRSI se prezintă atât în format fizic, cât şi în format electronic pe adresa Academiei Naționale de Informații „Mihai Viteazul": Şos. Odăi nr. 20, sector 1, Bucureşti, ani@sri.ro.

Textul trebuie redactat cu caractere Times New Roman de mărimea 12, dublu spațiat. Prima pagină trebuie să conțină titlul lucrării şi afilierea autorului (nume şi prenume, titlu ştiințific, apartenența la o instituție/asociație/organizație, precum şi adresa de e-mail).

Articolul va fi însoțit de un abstract (de până la 100 de cuvinte) şi de cuvinte-cheie (keywords), ambele într-o limbă de circulație internațională.

Toate referințele bibliografice trebuie precizate (parentetic, note de subsol etc.).

Autorii sunt responsabili pentru obținerea oricărei permisiuni referitoare atât la publicarea unor materiale din alte surse, cât şi la respectarea oricăror restricții sau proceduri care țin de locurile de muncă unde activează ori au activat.

Odată publicat, materialul intră în proprietatea RRSI, iar fiecare autor primeşte câte un exemplar al numărului RRSI în care i-a fost publicată contribuția.

Aranjarea în formatul de carte tipărită a textului, figurilor şi tabelelor se face, de regulă, de către personalul de specialitate al Editurii Academiei Naționale de Informații „Mihai Viteazul".

Pentru citate se folosesc ghilimele („ – pentru deschidere şi " – pentru închidere).

Figurile se numerotează. Titlul figurii se scrie cu un corp mai mic cu 2 pt decât textul de bază, imediat sub aceasta, fără spații, după care se dă explicația figurii, respectiv a graficului şi se precizează sursa, dacă este cazul.

Tabelele dintr-o lucrare trebuie să aibă o prezentare unitară. Se recomandă ca fiecare să fie numerotat şi să aibă un titlu. Titlul se scrie drept şi centrat deasupra tabelului. Numerotarea tabelului se face deasupra titlului. Titlul tabelului se scrie cu un corp mai mic decât textul de bază. Dacă există tabele care cuprind note, acestea se vor scrie imediat după tabel, nu la piciorul paginii şi nici în interiorul tabelului.

În cazul referințelor bibliografice din text, ordinea datelor este următoarea: numele şi prenumele autorului, titlul, volumul/ediția, editura, localitatea, anul, locul citat. Dacă lucrarea nu are autor, se trec trei steluțe liniare (***) sau numele instituției sub egida căreia a apărut lucrarea.

2. Referințe bibliografice

Bibliografia se plasează la sfârşitul articolului, după anexe.

De regulă, lucrările se scriu în ordinea alfabetică a numelor autorilor, numerotându-se cu cifre arabe urmate de punct; când sunt doi sau mai mulți autori pentru o lucrare, regula privitoare la ordinea alfabetică este valabilă doar pentru primul nume.

Titlul lucrării se scrie exact cum este tipărit în publicația citată, cu mențiunea că în cazul limbii române ortografia trebuie actualizată conform normelor Academiei Române.

De regulă, ordinea datelor este următoarea: numele şi prenumele autorului, titlul lucrării, volumul/ediția, editura, localitatea, anul.